opentext™

OpenText™ Intelligent Capture

Administration Guide

This guide explains the concepts, software, and procedures required to manage the Intelligent Capture system.

ECPCORE220300-AON-EN-01

OpenText™ Intelligent Capture
Administration Guide
ECPCORE220300-AON-EN-01
Rev.: 2022-June-13

This documentation has been created for OpenText™ Intelligent Capture CE 22.3.
It is also valid for subsequent software releases unless OpenText has made newer documentation available with the product, on an OpenText website, or by any other means.

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111
Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440
Fax: +1-519-888-0677
Support: https://support.opentext.com
For more information, visit https://www.opentext.com

Copyright © 2022 Open Text. All Rights Reserved.

Trademarks owned by Open Text.

Adobe and Adobe PDF Library are trademarks or registered trademarks of Adobe Systems Inc. in the U.S. and other countries.

One or more patents may cover this product. For more information, please visit https://www.opentext.com/patents.

Disclaimer

No Warranties and Limitation of Liability

Every effort has been made to ensure the accuracy of the features and techniques presented in this publication. However, Open Text Corporation and its affiliates accept no responsibility and offer no warranty whether expressed or implied, for the accuracy of this publication.

Table of Contents

Chapter 1

Before You Begin

As the Intelligent Capture administrator, you will need to understand the following:

- Security configuration
- Licensing
- ScaleServer technology
- Deployment in development, test, and production environments
- Intelligent Capture Administrator
- Intelligent Capture system performance
- System data protection
- Database tables and custom reports design

Chapter 2

Understanding Security Configuration

The information in this section explains security configuration settings available in Intelligent Capture, secure deployment and usage settings, secure maintenance, and physical security controls. This information is required to ensure secure operation of an Intelligent Capture System. This information is presented in the following topics:

- "Intelligent Capture Security Overview" on page 19 describes the components of Intelligent Capture that require security considerations.
- "Access Control Settings" on page 20 describes settings available in Intelligent Capture to ensure a secure operation of the Intelligent Capture System.
- "Communication Security Settings" on page 24, "Data Security Settings" on page 33, "Secure Serviceability Settings" on page 35, "Security Alert System Settings" on page 36, and "Other Security Considerations" on page 36 describe how to deploy and use Intelligent Capture securely.
- "Secure Maintenance" on page 38 describes how to perform secure maintenance of Intelligent Capture.
- "Physical Security Controls" on page 38 describes controls to protect Intelligent Capture components against unauthorized physical access and physical tampering.

2.1 Intelligent Capture Security Overview

Intelligent Capture consists of several components and third-party providers that have security considerations:

- Microsoft SQL Server provides the infrastructure for the Intelligent Capture Database. The Intelligent Capture Database is an optional component that stores batch metadata that is used to configure and monitor the system and to produce reports and logs.
- Intelligent Capture Server communicates with the Intelligent Capture Database and with client modules, and stores batch data.
- Intelligent Capture REST Service is a Web application that runs on IIS and communicates with Intelligent Capture REST clients, the Module Server, and the Intelligent Capture Server.
- Intelligent Capture Web Client is a Web application that runs on IIS and communicates with Intelligent Capture REST Service.
- The Module Server is a Windows Service that communicates with the Intelligent Capture REST Service.
- Intelligent Capture Administrator provides central administration, configuration, and reporting for all Intelligent Capture components.

- Intelligent Capture client modules perform tasks as directed by the Intelligent Capture Servers to which they are connected. Individual modules are grouped into a functioning document capture system by customer-defined processes.
- Web Services Hosting provides hosting services between the WS Input module and third-party web services consumers.

2.2 Access Control Settings

Access control settings enable the protection of resources against unauthorized access.

2.2.1 Access Methods

Each Intelligent Capture component accesses other Intelligent Capture components through defined pathways.

2.2.1.1 Intelligent Capture Database Access Methods

The Intelligent Capture Database is an optional component which is required to enable functionality such as reporting and ScaleServer functionality. The database is hosted by Microsoft SQL Server and accessed by other Intelligent Capture components using *TCP/IP*. The Intelligent Capture Database can be configured to use any unused port and can use a named or unnamed SQL Server instance. The default port is listed in "Port Usage" on page 24.

When installing the Intelligent Capture Database components, a login ID that has at least the SQL Server `dbcreator` role is required.

For upgrading the Intelligent Capture Database components, a login ID that is the SQL Server database owner is required,

The Intelligent Capture Database requires SQL Server or Windows authentication. Specify a valid SQL Server or Windows login ID and password for the components that connect to the Intelligent Capture Database.

Caution

Do not use a system administration account in production environments for Data Access Layer (*DAL*) registration. Using an account with full permissions is a security risk. Instead, create a specific SQL Server user account with the following required permissions:

- **Connect**
- **Execute**
- **Update**
- **Insert**
- **Select**

- **Delete**

2.2.1.2 Intelligent Capture Server Access Methods

The Intelligent Capture Server is a native Microsoft Windows program. It normally runs as a Windows service. Access to the Intelligent Capture Server takes place over *TCP/IP* and the access can be configured to use any unused port. The default port is listed in "Port Usage" on page 24. Communication occurs among an Intelligent Capture Server, other Intelligent Capture Servers in a ScaleServer group, and all other Intelligent Capture components.

Authentication between an Intelligent Capture Server and the Intelligent Capture Database is configured when the database and server components are installed as explained in the *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*. After installation, if the Intelligent Capture Database credentials change, the credentials registered in each Intelligent Capture Server must be updated by running the `DalConfig.exe` utility on each Intelligent Capture Server machine. Instructions for running `DalConfig.exe` are provided in "Resolving SQL Server Database Connectivity Issues and Maintaining Database Access Credentials" on page 517.

Intelligent Capture components connect to one or more Intelligent Capture Servers by using authentication methods described in "Authentication Configuration" on page 22. These components are granted permission to run and perform other functions by using access control methods described in "User Authorization" on page 23 and "Component Authorization" on page 24.

Most Intelligent Capture client modules are able to connect to multiple Intelligent Capture Servers that have been configured as a ScaleServer group. In this configuration, modules establish connections to multiple Intelligent Capture Servers by using the host name or IP address of each of the Intelligent Capture Server machines. For more information on all the modules and which modules are ScaleServer-compatible, see *OpenText Intelligent Capture - Module Reference (ECPCORE-CMD)*.

2.2.1.3 Web Services Hosting Access Methods

Intelligent Capture Web Services requires the use of Web Services Hosting and Web Services Coordinator, both of which are installed by the Intelligent Capture client setup program. Both Web Services Hosting and Web Services Coordinator are Windows services, but are not configured to start automatically by default. Customers who want to use the WS Input module must start the Web Services Hosting service and the Web Services Coordinator service manually or configure it to start automatically.

Web Services Hosting uses *TCP/IP* to communicate with the Web Services Coordinator and third-party web service consumers. The Web Services Coordinator communicates directly with the Intelligent Capture Database. Ports used for these communication channels are listed in "Port Usage" on page 24.

2.2.2 User Authentication

User authentication settings control the process of verifying the user accessing Intelligent Capture.

2.2.2.1 Default User Accounts

Intelligent Capture does not have default user accounts. It uses Microsoft Windows user accounts for authentication and authorization. Except when installed on a single machine for development or demonstration purposes, these user accounts must be domain accounts. These accounts can use any of the authentication security providers used by Microsoft Windows: NTLM, Kerberos, or Negotiate.

2.2.2.2 Administrator Role

During server installation, users can add the credentials of a user to add to the Intelligent Capture **Administrator** role. This user does not have to be a Windows Administrator on the server machine, or any other machine. When the Intelligent Capture Server starts, this user is added to the Intelligent Capture Administrator role and is granted all the permissions to start and use all features of any Intelligent Capture component, including Intelligent Capture Administrator and all client modules.

Information about configuring Intelligent Capture roles and permissions is provided in "User Authorization" on page 23.

2.2.2.3 Authentication Configuration

Intelligent Capture authentication configuration is accomplished by configuring Microsoft Windows domain user accounts with user names, passwords, and appropriate access rights. Modules and other components that run as services can be configured to run under specific machine accounts.

Access to Intelligent Capture is controlled by setting the permissions for user roles and by assigning individual user to those roles, as explained in "User Authorization" on page 23 and "Component Authorization" on page 24.

Intelligent Capture imposes no requirements on user name or password complexity, change intervals, or scope of required periodic changes. All such requirements and restrictions must be implemented and enforced within the Windows user domain.

In a multiple-domain environment, create trusts between the different domains so that cross-domain authentication can succeed. The minimum trust relationship is "Nontransitive One-Way External Trust" from the domain with clients that must authenticate to the domain that has servers which must perform the authentication.

The *`SecurityPackage`* parameter specified in each machine's `settings.ini` file configures the method of secure communication to be used with the Intelligent Capture Server. Options include `Negotiate`, `NTLM`, and `Kerberos`. The default setting is `Negotiate`, which enables the client and server to negotiate either Kerberos or NTLM as the authentication protocol.

Before implementing the Kerberos security package, the Intelligent Capture client must configure a service principal name (*SPN*) using the guidelines described at http://msdn.microsoft.com/en-us/library/aa378747(VS.85).aspx.

2.2.2.4 User Actions Performed without Authentication

No user actions are possible from Intelligent Capture client or administrative modules without successful authentication.

2.2.3 User Authorization

User authorization settings control rights or permissions that are granted to a user to access a resource managed by Intelligent Capture.

After a user is authenticated, the Intelligent Capture Server checks user authorization to determine which permissions to grant to the user. User permissions are granted and revoked by assigning permissions to roles and by assigning Windows domain users or groups to those roles.

Intelligent Capture includes a number of predefined roles; however, by default no users are assigned to any roles except the default Administrators role described under "Administrator Role" on page 22. The predefined roles can be used "as is" or can be modified, and new roles can be added as needed. Roles are defined, assigned, and managed in the **Licensing / Security** pane of the Intelligent Capture Administrator by clicking **View Roles** under **Security**. "Understanding Permissions" on page 134 describes Intelligent Capture roles and permissions.

Access Control Lists (*ACL*) further define access for users or groups to modules, batches, departments, or processes. For more information, see "Managing Security" on page 130.

2.2.4 Component Access Control

Component access control settings define control over access to Intelligent Capture by external and internal systems or components.

2.2.4.1 Component Authentication

Within an Intelligent Capture system, Intelligent Capture Servers authenticate with the Intelligent Capture Database by using either SQL Server or Windows authentication.

The SQL Server hosting the Intelligent Capture Database must be configured with an appropriate account as described in *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*. Then, when each Intelligent Capture Server is installed, the credentials of this SQL Server or Windows account must be specified.

During installation of the Intelligent Capture Server and the Module Server, the installation program offers to configure the Windows Firewall (if running) to open the ports required to pass network traffic to and from the Intelligent Capture

Database. Customers can choose to use this automatic configuration, or bypass this step and configure the firewall manually. If a firewall other than the Windows Firewall is being used, it must be configured to pass traffic on the ports listed in "Port Usage" on page 24.

2.2.4.2 Component Authorization

Within an Intelligent Capture system, Intelligent Capture Servers are authorized to function by activating and by using software security keys. The security key establishes the Server ID. Activating an Intelligent Capture Server authorizes the server to function. To enable immediate operation during the time it takes to obtain activation codes, Intelligent Capture Servers function for a predefined grace period. When that grace period expires, minimal functionality is maintained to enable Intelligent Capture Administrator to connect to the server for the purposes of establishing a valid activation.

Individual Intelligent Capture components (modules) are authorized to function according to module and connection licenses that are stored on the Intelligent Capture Servers to which they connect. Various types of licenses are available to handle various production, demonstration, and development scenarios. Licenses can specify the maximum number of simultaneous server connections, the maximum number of pages that can be processed per unit of time, and other restrictions. License feature codes for certain components can restrict or allow certain module features to function.

Licenses are installed by using the **Licensing / Security** pane of the Intelligent Capture Administrator. Instructions for managing Intelligent Capture licenses are provided in "Understanding License Types" on page 39.

2.3 Communication Security Settings

Communication security settings enable the establishment of secure communication channels among Intelligent Capture components as well as between Intelligent Capture components and external systems or components.

2.3.1 Port Usage

The following table lists the default ports used by various Intelligent Capture components.

Table 2-1: Intelligent Capture Port Usage

Component	Service	Protocol	Port	Description
Microsoft SQL Server	SQL Server(MSSQLSERVER)	*TCP/IP*	1433	Default port; can be changed during SQL Server installation.

Component	Service	Protocol	Port	Description
Intelligent Capture Server	InputAccel Server	*TCP/IP*	10099	Default port for Intelligent Capture Server-Client communication. Can be changed during Intelligent Capture Server and Client installation.
Web Services Hosting	Web Services Hosting	*TCP/IP*	40571	Enables the Web Services Coordinator to communicate with Web Services Hosting through .NET Remoting. The included utility `portreserve.exe` enables administrators to reserve any unused port through which Web Service Hosting can accept *HTTP* connections.
Web Services Coordinator	Web Services Coordinator	*TCP/IP*	12007	Enables the Intelligent Capture Administrator and the WS Input module to communicate with the Web Services Coordinator.
Standard Import module (Email)	None	*TCP/IP*	110	Default port for *POP3* mail servers. Specify the actual port to use during setup in the **Profile** tab.

Component	Service	Protocol	Port	Description
			995	Default port for *POP3 SSL* mail servers. Specify the actual port to use during setup in the **Profile** tab.
			143	Default port for *IMAP4* mail servers. Specify the actual port to use during setup in the **Profile** tab.
			993	Default port for IMAP/SSL mail servers. Specify the actual port to use during setup in the **Profile** tab or **Email Connection** settings.
			587	Default port for *SSL SMTP* email. Specify the actual port to use during setup in the **Profile** or **Email Connection** settings.
			25	Default port for non-*SSL SMTP* email. Specify the actual port to use during setup in the **Profile** and **E-mail Forwarding** tabs.

Component	Service	Protocol	Port	Description
			80	Default port for Exchange WebDav to connect to an Exchange server using HTTP. Specify the actual port to use during setup in the **Profile** tab or **Email Connection** settings.
			443	Default port for Exchange WebDav to connect to an Exchange server using HTTPS. Specify the actual port to use during setup in the **Profile** tab or **Email Connection** settings.
			80	Default port for Exchange Web Services to connect to an Exchange server using HTTP. Specify the actual port to use during setup in the **Profile** tab or **Email Connection** settings.

Component	Service	Protocol	Port	Description
			443	Default port for Exchange Web Services to connect to an Exchange server using HTTPS. Specify the actual port to use during setup in the **Profile** tab and **Email Connection** settings.
Module Server OCR Engine	None	TCP/IP	10092	Default port.
Archive Export module	None	*TCP/IP*	Not applicable	Use the included `SLDRegistration.exe` to discover and register information about the host, port, and credentials of the target SAP system.
IBM CSSAP Export module	None	*TCP/IP*	Not applicable	Port that the module uses to export to the CommonStore server. Must be specified in the **General** tab of the **Definition Properties** window during setup. Can vary by batch if specified in an IA Value.

Component	Service	Protocol	Port	Description
Export for OpenText Content Server module	None	*TCP/IP*	2099	Default port that the module uses for non-secure connections to the Content Server server. Different ports can be specified in the **Content Server Logon** window when starting the module for production. Information on establishing secure connections is provided in the *OpenText Export for OpenText Content Server Guide*.
Custom export modules not specifically listed	Depends on module	*TCP/IP*	Not applicable	Command-line arguments for starting the module in production mode enable a server port to be specified for the target repository. The specified port must match the port on which the repository server is listening. Each module guide provides information on the available command line arguments.

2.3.2 Network Encryption

You can encrypt data transferred between client modules and the Intelligent Capture Server.

Also, the *Documentum Advanced Export module* login credentials, which are stored for establishing dynamic repository connections in production mode, are stored using protected IA Values. A protected IA Value is encrypted and accessible only by the user who created it or by a user who is a member of a role that has been granted access to protected IA Values. Protected IA Values are encrypted using Microsoft Cryptography to prevent a network sniffer from intercepting them.

Note: However, Intelligent Capture does not provide built-in communications encryption or security for network communication among locally networked Intelligent Capture components (other than the aforementioned); that is, such network communication takes place in clear text. Any needed security must be provisioned by using the appropriate security providers.

2.3.3 Intelligent Capture REST Service, Intelligent Capture Web Client, and Module Server Security

Intelligent Capture REST Service and Intelligent Capture Web Client are hosted on IIS and the required IIS features are enabled by the Intelligent Capture installer. The Module Server is hosted as a Windows service.

For more information, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

IIS settings

Intelligent Capture REST Service and Intelligent Capture Web Client must be configured to use Secure Sockets Layer (*SSL*) to ensure that user credentials and data traffic are encrypted between the hosts and their clients.

Intelligent Capture REST Service and Intelligent Capture Web Client's Application Pool identity must be configured as follows:

- Enable `Read/write/delete/create` access to the shared data folder on the file system with the shared data folder.
- Add the identity to the following Windows groups on the Web server machine:
  - `IIS_IUSRS`

    This group grants access to all the necessary resources on the computer for proper functioning of IIS.
  - `Performance Log Users`

    Intelligent CaptureREST Service works with performance counters for special tracing and reporting purposes.

- Add the identity to the Intelligent Capture `Administrators` role so that it has the necessary permissions on the Intelligent Capture Server.
- For Intelligent Capture REST Service and Intelligent Capture Web Client, configure the SSL certificate and HTTPS binding by adding these bindings in **IIS Management Console** in **Actions** > **Bindings**.

User for Connecting to the Intelligent Capture Server

The user to be used to connect to the Intelligent Capture Server must be a member of the Intelligent Capture `Administrators` role. This user is specified in the Intelligent Capture REST Service Configuration tool. If `*` was specified for this user, then the user is the Intelligent Capture REST Service's Application Pool identity.

Shared data folder

Configuration information for all Intelligent Capture REST Service and Intelligent Capture Web Client websites in the Intelligent Capture system are stored in a shared data folder.

The Intelligent Capture Server user password used to connect from the Intelligent Capture REST Service is encrypted and stored in a file in the shared data folder.

User authentication

User authentication can be configured through one of the following mechanisms:

- Windows authentication
- A custom Intelligent Capture REST Service authentication plug-in

2.3.4 Web Component Security

For the components hosted by IIS (see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*), configure IIS to use Secure Sockets Layer (*SSL*) to ensure that user credentials and data traffic are encrypted between the hosts and their clients.

Access to these components is controlled by several security providers, including the web server that is hosting the component, Windows user permissions (*ACL*s), Intelligent Capture licensing, and Intelligent Capture Administrator-assigned user roles.

Security settings for Microsoft IIS 7.0 require enabling of these role service security settings that are not installed by default:

- Basic Authentication
- Windows Authentication
- IIS Client Certificate Mapping Authentication

Security settings for Microsoft IIS 7.5 require enabling the following role service settings that are not installed by default:

- Application Development
  - *ASP.NET* (requires enabling of the following three settings)
  - .NET Extensibility
  - *ISAPI* Extensions
  - *ISAPI* Filters
- Security
  - Basic Authentication
  - Windows Authentication
  - IIS Client Certificate Mapping Authentication
- IIS 6 Management Compatibility
  - IIS 6 Metabase Compatibility
  - IIS 6 WMI Compatibility
  - IIS 6 Scripting Tools
  - IIS 6 Management Console

2.3.5 Web Services Security

The Web Services Hosting component can accept an *SSL* certificate by using a utility such as `HttpCfg.exe` supplied with Microsoft Windows Server editions to assign a certificate to a port. After implementation, the *HTTP* driver receives SSL connections on this port and uses the installed certificate to authenticate the server and to establish a secure connection. A simple user name and password combination is then used to authenticate the third-party client system. Because different validation providers are used by the web services consumer client, the Web Services subsystem has no predetermined authentication techniques. However, the client-side scripting functionality of the WS Input module can access incoming parameters, perform validation, and then process or deny the call.

More information about the Web Services *API* can be found in the *OpenText Intelligent Capture - Scripting Guide (ECPCORE-PSC)*.

The Web Services Coordinator component is a Windows service that is installed as part of the Web Services client component installation. It processes asynchronous web service requests and pairs them with responses, even when those responses can arrive hours after the requests are made. These responses are forwarded to the WS Input module. In systems where data security is a concern, the Web Services Coordinator should be installed on a secured server machine.

Note: All components of the Web Services subsystem run as services only. After installation, they do not start automatically, but must be started manually

or be configured to start automatically by using the Service Properties for each service within the Microsoft Management Console.

2.4 Data Security Settings

Data security settings enable definition of controls to prevent data permanently stored by Intelligent Capture to be disclosed in an unauthorized manner.

Within an Intelligent Capture system, data is permanently stored in the Intelligent Capture Database and on one or more Intelligent Capture Servers.

The data that is stored in the Intelligent Capture Database is accessible only to users who have SQL Server administrative access or who know the Intelligent Capture Database *SQL* credentials. These credentials are managed by Microsoft SQL Server administration tools.

The data that is stored on the Intelligent Capture Servers is directly accessible to users who have credentials that enable access to the Intelligent Capture Server installation folder (`C:\IAS` by default).

Note: The Intelligent Capture Server fully supports locating its `IAS` root directory on an *NTFS* file system, and uses the built-in NTFS security system (access control lists) to implement its own security. Alternatively, the Intelligent Capture Server main directory can be located on a non-NTFS file system, such as is used in many Network Attached Storage (*NAS*) and Storage Area Network (*SAN*) devices. However, when installed on a non-NTFS file system, *ACL*-based security is not supported. Due to the known performance issues, *NAS* is supported for low volume environments only.

The data that is stored on the Intelligent Capture Servers is also indirectly accessible to users who have been assigned to roles that have administrative permissions. Roles are defined and users are assigned to roles by using the **Licensing / Security** pane in the Intelligent Capture Administrator. Information about managing roles and permissions is provided in the topic *Managing Users and Groups*.

When images are edited or displayed in ScanPlus and RescanPlus, the images are downloaded from Intelligent Capture Server and might be cached locally. Large scanned or imported images might be cached locally. You can configure whether these images are to be cached locally.

2.4.1 Encryption of Data

Data stored by the Intelligent Capture Database and the Intelligent Capture Servers is not encrypted by the Intelligent Capture system with the following exceptions:

- SQL credentials: The Intelligent Capture Database *SQL* login credentials are stored in the Intelligent Capture Database in an encrypted form.
- Temporary batch staging files: These temporary files can be encrypted. For more information, see "Managing Client-Server and Batch Staging File Data Encryption" on page 139.

For Intelligent Capture REST Services, including Intelligent Capture Web Client, user session files, that is, scanned pages and imported images uploaded and downloaded by users, are stored and encrypted in the shared data folder. Design-time metadata is not encrypted. Because client modules do not accept encrypted files, these files are decrypted when they are passed to client modules and encrypted when they are passed back to Intelligent Capture REST Services.

By default, encryption is enabled. To disable or enable encryption, see "Installing Intelligent Capture Web Client and Intelligent Capture REST Service" in the *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

2.4.2 Web Services Subsystem Data Integrity

The Web Services subsystem uses *SSL* for authentication and secure communication between the web services sever and client. Instructions on configuring, installing, and binding an *SSL* certificate to a given *HTTP* port can be found in the *OpenText Intelligent Capture - General Import/Export Modules Guide (ECPCORE-CIO)*. The certificate must be installed on the machine that runs the Web Services Hosting component.

The WS Output module can interact with external web services that use *SSL* and therefore use *SSL* certificates. In these cases, the client (the WS Output module) must trust this certificate to authenticate the server (the external web service). This trust can be established in either of the following ways:

- The server certificate is installed into the client's trusted certificates storage.
- The server certificate is signed by a trusted vendor, and the client has the vendor's certificate installed in trusted storage. In this case, the client can download the server's certificate and verify its signature. If the certificate is properly signed by a trusted vendor, then the client will trust the server certificate.

Communication between client and server is handled through an *SSL* connection, using *HTTPS* instead of *HTTP*. After the server is authenticated, a secure connection is established and the client is authenticated using a standard user name and password. No additional encryption is required for credentials, because the *SSL* connection is already encrypted. This configuration enables you to securely store and transfer the client-side user name and password as parameters in a web call.

2.4.3 Data Erasure

Intelligent Capture performs document capture in batches corresponding to customer-defined parameters and then processes and exports the data from those batches into external systems for long-term storage. Intelligent Capture is designed to store batch data for only a short time—a few hours or perhaps a few days depending on the customer's business needs.

Batch data is stored in two places: the batches subfolder of the Intelligent Capture Server installation folder (`C:\IAS`, by default) holds batch documents and some related batch data, and the Intelligent Capture Database holds metadata, logs, values for reports, and audit data.

- Batches are typically deleted from the Intelligent Capture Server, either manually or by an automated activity, some period of time after their data has been exported and verified. The batch deletion facilities built into Intelligent Capture use standard Windows file system deletion *API*s. No secure deletion facility is provided. Customers must take any necessary precautions to restrict access to batch data during its lifecycle and to ensure it is deleted in a prudent manner consistent with the need for confidentiality.
- A subset of batch data stored in the Intelligent Capture Database. This data is removed automatically when the Intelligent Capture Server is restarted, after which data for active batches is rebuilt. This data is also removed automatically when batches are deleted from the Intelligent Capture Server.

2.4.4 FIPS Compliance

When installed and configured according to the information in the *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*, Intelligent Capture is compliant with the requirements of the Federal Information Processing Standard (*FIPS*), which provides guidelines for security and computer interoperability.

2.5 Secure Serviceability Settings

An Intelligent Capture system does not have specific serviceability settings that enable a third party to access the system. There are no hidden accounts or passwords that provide access outside the control of the customer's secure configuration. If it becomes necessary to enable an outside party to access a secured Intelligent Capture system, the customer must grant access by adding a specific account and configuring the necessary roles and permissions, and should then revoke that access when the service has been completed.

2.6 Security Alert System Settings

Intelligent Capture has no built-in alert system; however, third-party systems can be used to enable alerts to be sent to key personnel when specific events occur. If a third-party alert system is used, consult the related documentation to understand how to configure the necessary alerts.

2.7 Other Security Considerations

The topics in this section describe security considerations that are not covered in other sections.

2.7.1 Running Intelligent Capture in a Hardened Environment

The Intelligent Capture infrastructure is build entirely on Microsoft products. Microsoft publishes documentation about running its server products in a secure, or hardened, environment. Hardening machines means establishing security policies, applying all of the latest operating system security patches, disabling unneeded services, enabling firewalls, blocking unused ports, and configuring an *IT* infrastructure to block unwanted access.

Intelligent Capture is intended to run in a hardened environment and has been tested with some common, but not all possible, hardened configurations and components.

2.7.2 Running Intelligent Capture with Minimum Permissions

Good security practice includes setting up machines to run their applications with the minimum possible permissions. In particular, the Intelligent Capture Server is designed to run under a least-privileged user account (*LUA*) that is automatically configured and provisioned by the Intelligent Capture Server installation program. For more information on which permissions are needed by each Intelligent Capture component, see*OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

2.7.3 .NET Remoting and NAT Devices

.NET Remoting connections cannot be established with a client or server behind a network address translation (*NAT*) device. Because .NET Remoting uses *TCP* connections to communicate between clients and servers in the Web Services subsystem, some components (including Web Services Hosting, Web Services Coordinator, and the WS Input module) cannot communicate if any of these components is behind a *NAT*.

2.8 Secure Deployment Settings

The following table lists secure deployment settings that can be used within an Intelligent Capture system.

Table 2-2: Secure Deployment Settings

Default setting	Secure deployment settings	Pros of secure deployment settings	Cons of secure deployment settings	How to configure secure deployment settings
Encryption is provided for network communication between client modules and the Intelligent Capture Server.	For best possible security between client and server, employ encryption of network traffic.	Encryption provides high level of protection for the communication between client and server by avoiding the tampering, spoofing, and "man-in-the-middle" type of attacks.	Impact on performance	For client modules, you can specify encryption using Intelligent Capture Administrator. Intelligent Capture uses the encryption providers that are available on the operating system and machine. Make sure that the encryption provider is registered on both the server a client machines.
Login credentials.	Clients on the local network: Configure one of the following Windows authentication security providers: *NTLM* or Kerberos. Clients connecting remotely: Configure *HTTP* connections using *SSL*.	Prevent interception of Windows and Intelligent Capture credentials.	None	Consult Microsoft documentation to determine how to enable authentication security and to enable *SSL* in remote connections.

2.9 Secure Maintenance

The following topics describe how to maintain security after an Intelligent Capture system is deployed and in use.

2.9.1 Security Patch Management

The following table lists the major components on which Intelligent Capture depends and who is responsible for applying security patches.

Table 2-3: Security Patch Management

Third-party Component	Frequency of Patch	OpenText Responsibility (Y/N)	Customer Responsibility (Y/N)	How to Apply Patch
Microsoft Windows OS	Monthly	N	Y	See the information provided by the patch vendor.
Microsoft SQL Server	As released	N	Y	
Microsoft Internet Explorer	As released	N	Y	

2.9.2 Malware Detection

Malware detection should follow the same guidelines and requirements as used for other client/server products in the enterprise. In general, appropriate malware detection software should be installed and regularly updated with new signatures on all machines that are exposed to interactions on a public network.

Note: Malware detection should normally not be installed on the Intelligent Capture Servers, as these machines should be locked down from Internet threats. Using malware detection software on Intelligent Capture Servers will significantly reduce their performance.

2.10 Physical Security Controls

Physical security controls enable the protection of resources against unauthorized physical access and physical tampering. Intelligent Capture Server machines, the Intelligent Capture Database host, and client machines that run unattended modules should be installed in a secure server facility on server-class equipment, using the same considerations for power, cooling, backup, and physical access as used for other critical components of your enterprise network.

Chapter 3

Understanding License Types

Intelligent Capture provides different types of licensing, depending on processing needs. License types include daily, group, periodic, service bureau, and attended client licenses. If you are unsure about your licensing level and the features it includes, contact OpenText Global Technical Services at My Support (https://support.opentext.com).

3.1 Daily Licenses

A daily license allows a specified number of pages to be processed per day. Each night at midnight (the Intelligent Capture Server time), the number of pages processed is reset to zero; and the system can then process up to (but not exceed) the specified number of pages until the next day when the count is set back to zero again.

The total amount of pages that can be processed per day is determined differently for individual modules and the Intelligent Capture Server:

Module Daily Licensing

The number of pages that an individual module is licensed to process per day equals the number of pages allowed in the license multiplied by the number of module connections allowed (Pages x Connections).

Server Daily Licensing

The total number of pages that the Intelligent Capture Server is licensed to process per day equals the total number of pages that can enter the system in one day, regardless of how many modules are connected to the server.

Related Topics

"Centralized Licensing" on page 101

"Page Count Sharing and Transfer" on page 48

"Importing License Codes from a License File" on page 124

"Viewing or Modifying License Code Settings" on page 125

3.2 Group Licenses

A group license pools page counts and connections of various modules that are members of the group. Individual modules reference the group license to determine the number of pages they can process and the number of module instances that can connect to the Intelligent Capture Server.

With group licenses, page counts are not reset every night. Instead, the modules in the group can continue processing until the specified page limit or "Valid Until" date is reached, whichever comes first. After the limit is reached, the license becomes invalid and a new license must be issued.

Note: Group licenses have an "Enter By" date. If the license is not installed on or before this date, the Intelligent Capture Server will consider the license invalid and a new license must be issued. Customers with new keyless installations requiring activation can request an extension to their "Enter By" date from OpenText Global Technical Services at My Support (https://support.opentext.com).

Related Topics

"Centralized Licensing" on page 101

"Page Count Sharing and Transfer" on page 48

"Importing License Codes from a License File" on page 124

3.3 Periodic Licenses

A periodic license is a type of group license. It is generated in a manner similar to most non-daily licenses except that its page count is reset to zero on a regular basis, usually monthly or annually. This is usually referred to as the expiration, or "rollover" date. If you are unsure about your licensing level and the features it includes, contact OpenText Global Technical Services at My Support (https://support.opentext.com).

After the rollover date is reached, the number of pages processed is reset to zero; and the system can then process up to the given amount of pages until the next period end is reached and the count is reset to zero again. No new license needs to be created.

Related Topics

"Centralized Licensing" on page 101

"Page Count Sharing and Transfer" on page 48

"Importing License Codes from a License File" on page 124

"Viewing or Modifying License Code Settings" on page 125

3.4 Service Bureau Licenses

The service bureau license package is a special type of group license designed for customers who perform contract information capture and require licensing based on their contract size. This allows the customer to purchase licensing to process a specified number of pages with a designated group of modules. Every page processed by every module is counted against the group license page count. This license does not renew automatically. When the licensed number of pages is exhausted, a new license must be purchased if additional processing is needed.

Related Topics

"Centralized Licensing" on page 101

"Page Count Sharing and Transfer" on page 48

"Importing License Codes from a License File" on page 124

"Viewing or Modifying License Code Settings" on page 125

3.5 Attended Client Licenses

The attended client license package is a special type of connection-based group license for clients. When a daily or periodic Intelligent Capture Server license is purchased, it is typically bundled with an attended client package and one export module of the customer's choice. In previous releases, the attended client license was called a "universal" license. If you are unsure about your licensing level and the features it includes, contact OpenText Global Technical Services at My Support (https://support.opentext.com).

Intelligent Capture Server connections are controlled through the attended client license. The server includes one connection that all attended client modules must share. For each attended client license, you may connect one attended client module. Although only one of the attended client modules is allowed to connect to the Intelligent Capture Server at any one time, the Intelligent Capture Server can accept up to 19 more connections from the non-attended client modules combined.

The attended client license comes with a standard set of Intelligent Capture modules, all of which are licensed under a non-daily group license. It is also possible to buy additional licenses outside of the predefined module set. For example, the ScanPlus module license must be purchased separately, since its license is based on the type of scanner being used and the features it supports. Custom export modules are also frequently licensed outside of the standard attended client license. These additional modules usually have an unlimited page count and are licensed on a daily basis. Page counts track the number of pages that enter the system, regardless of which or how many modules process the page. Module page counts, therefore, are set to "Unlimited" with this type of license.

Related Topics

"Centralized Licensing" on page 101

"Page Count Sharing and Transfer" on page 48

"Importing License Codes from a License File" on page 124

"Viewing or Modifying License Code Settings" on page 125

3.6 Server Licenses

ScaleServer technology uses a combination of licensing, server configuration parameters, and technology in the Intelligent Capture Servers themselves. To configure a ScaleServer group, you must obtain server and client licenses that enable the ScaleServer technology.

Certain licensing levels include ScaleServer licensing, and with other licensing levels ScaleServer licensing is an option. If you are unsure about your licensing level and the features it includes, contact OpenText Global Technical Services at My Support (https://support.opentext.com).

Table 3-1: Server Feature Codes that Enable ScaleServer Technology

ClusterBase	Feature Code
1	F
2	E
3	EF
4	D
5	DF
6	DE
7	DEF
8	C

Additional server feature codes enable the use of specific Intelligent Capture Server functionality.

Table 3-2: Additional Server Feature Codes

Feature Code	Description
Q	Enables support for identity obscuring. This feature code ensures that user names are hidden in all reports and logs.

Feature Code	Description
R	Enables support for using reporting features. All licences contain this feature code.
S	Enables support for side-by-side installation. Users need this license if Intelligent Capture Servers are installed in an Active/Active clustering environment.
W	License to use the Intelligent Capture REST Services (including Intelligent Capture Web Client) and PixTools for Mobile. It enables creating a batch on the Intelligent Capture Server using the Intelligent Capture REST service. **Note:** Unlicensed usage of the PixTools for Mobile is exclusively for application development and test purposes. Production use or connection to an Intelligent Capture Server through the Intelligent Capture REST Service for batch submission purposes requires an PixTools for Mobile license. If you are not currently licensed for the PixTools for Mobile, contact OpenText Global Technical Services at My Support (https://support.opentext.com).

Related Topics

"Centralized Licensing" on page 101

"Page Count Sharing and Transfer" on page 48

"Importing License Codes from a License File" on page 124

"Viewing or Modifying License Code Settings" on page 125

3.7 Intelligent Capture REST Services Licenses

Intelligent Capture REST Service client (including Intelligent Capture Web Client) and Module Server licensing is managed through the Intelligent Capture Web Client Licensing page.

To log in to the Intelligent Capture Web Client Licensing page, in your browser, set your browser's language option to the language as instructed by your administrator, navigate to the Intelligent Capture Web Client URL that your administrator provided, and log in as a user in the Administrator group and then select **<***your_avatar_user_name***>** > **Licensing**.

Notes

- For operating system and browser requirements, see the *Intelligent Capture Release Notes* (available in My Support (https://support.opentext.com/)).
- JavaScript must be enabled in your browser.

For more information about the Intelligent Capture Web Client Licensing page, see *OpenText Intelligent Capture - Web Client Licensing Guide (ECPCORE-ARE)*.

Using an Intelligent Capture REST Service client in conjunction with Intelligent Capture Server requires feature code `W`. For more information, see "Server Licenses" on page 42.

3.8 Client Module Licenses and Feature Codes

Each Intelligent Capture client module that you want to use must have licenses that specify the required feature code. Some modules have module-specific feature codes, and others apply to all Intelligent Capture client modules. If you are unsure about your licensing level and the features it includes, contact OpenText Global Technical Services at My Support (https://support.opentext.com).

Note: Module feature codes are integral to the module license codes. You cannot arbitrarily change feature codes.

Client Module Feature Codes

The following codes apply to all Intelligent Capture client modules. Feature code `X` and feature code `Y` are mutually exclusive.

Table 3-3: Client Module Feature Codes

Feature Code	Description
X	Indicates that the Intelligent Capture client module may connect to an Intelligent Capture Server in a ScaleServer group. Each client module also must be ScaleServer-compatible.
Y	Indicates that the Intelligent Capture Server will only accept connections from the module when it is running on the same computer as the Intelligent Capture Server. This can be useful when creating a low-volume production system on a single workstation, or more commonly for testing and troubleshooting purposes.

Completion, Intelligent Capture Designer, and Extraction Module Feature Codes

Table 3-4: Feature Codes

Feature code	Description
A	Enables Advanced Recognition.

ScanPlus and RescanPlus Feature Codes

These codes support scanner features in ScanPlus and RescanPlus.

Table 3-5: ScanPlus and RescanPlus Feature Codes

Feature code	Description
A	Module can be used with ISIS Level 1 scanner drivers. Level 1 scanners are typically simplex scanners with throughput of less than 20 pages per minute, no grayscale, no document feeder, limited page sizes.
B	Module can be used with ISIS Level 1 and 2 scanner drivers. Level 2 scanners are typically duplex scanners with throughput between 20 and 50 pages per minute, grayscale, document feeder, page sizes up to 11 x 17 inches.
C	Module can be used with ISIS Level 1, 2, and 3 scanner drivers. Level 3 scanners are higher-speed models with throughput between 50 and 90 pages per minute, document feeder, image processing, barcode recognition, endorser/ imprinter, and may include book and microfilm scanners and multistream capabilities.
D	Enables support for ISIS Level 1, 2, 3, and most production level scanners. Also allows use of scanner drivers that do not have defined levels.

NuanceOCR Module Feature Codes

Table 3-6: NuanceOCR Module Feature Codes

Feature code	Description
A	Enables *RER*, providing two engines that work together to perform handprint recognition.
B	Enables *OMR*, providing optical mark recognition.

Advanced Recognition Modules and Features

Advanced Recognition modules and features include:

- Classification module
- Identification module
- Collector module
- Auto-Learning Supervisor service
- Advanced Recognition development tools and accessories

Feature codes for these modules and features include:

Table 3-7: Feature Codes for Advanced Recognition Modules and Features

Feature code	Description
A	Limited to 50 Templates per project (otherwise unlimited)
B	Array field
C	Free Form
D	Western OCR engine
E	General-Use OCR engine
G	1D barcode engine
H:	Generating statistics
I	Text Matching
K, L, M	Any of these feature codes will allow the maximum characters per second with Advanced OCR/ICR engine zonal license. The feature codes are: • K, L, or M: 400 maximum characters per second

Feature code	Description
N, O, P	Any of these feature codes will allow the maximum pages per hour with Advanced OCR/ICR engine with full page license. The features codes are: • N, O, or P: 3600 maximum pages per hour

Related Topics

"Centralized Licensing" on page 101

"Page Count Sharing and Transfer" on page 48

"Importing License Codes from a License File" on page 124

"Viewing or Modifying License Code Settings" on page 125

3.9 Disaster Recovery Licenses

Certain licensing levels include Disaster Recovery licensing, and with other licensing levels Disaster Recovery licensing is an option. If you are unsure about your licensing level and the features it includes, contact OpenText Global Technical Services at My Support (https://support.opentext.com).

Related Topics

"Centralized Licensing" on page 101

"Page Count Sharing and Transfer" on page 48

"Importing License Codes from a License File" on page 124

3.10 Calculating Page Counts

A server license decrements page count when a page enters the system. A page is defined as a single-sided image, which is scanned or imported into an Intelligent Capture Server by modules such as ScanPlus, Standard Import, WS Input, Ricoh GlobalScan Plug-in, or any other module that can add a page for processing. For every page scanned or imported in simplex mode, one page is counted. For every page scanned or imported in duplex mode, two pages are counted. Each single-sided page is counted once when it enters an Intelligent Capture system.

Notes

- If a page is not associated with a template and no data is extracted from that page when the Extraction module retrieves a task, then that page is not counted against the extraction license page counts.

- Independent of licensing, the WS Output module has a maximum allowed number of pages limit. When this limit is reached, WS Output stops processing tasks, but no error message is displayed. The Intelligent Capture Server log rule (`AllServerWarnings`) logs all warnings to the Intelligent Capture Database. This rule is on by default so all Intelligent Capture Server warning messages regarding running out of page counts are logged to tbl_AuditErrorLog.

Related Topics

"Centralized Licensing" on page 101

"Page Count Sharing and Transfer" on page 48

"Importing License Codes from a License File" on page 124

"Viewing or Modifying License Code Settings" on page 125

3.11 Page Count Sharing and Transfer

Intelligent Capture Servers in a ScaleServer group communicate amongst themselves to facilitate page count sharing. When a specific Intelligent Capture Server in a ScaleServer group needs to process additional pages (due to a request from a client module) and has run out of licensed volume, it requests the pages from other servers in the group.

The quantity of pages a server can borrow is determined by the server parameter `PagesToBorrow`, and the default value of this parameter is 1000. For more information, see "Intelligent Capture Server Parameters" on page 341.

The decision of which server to borrow pages from is based on the available page volume of each Intelligent Capture Server in the ScaleServer group. Also, a server cannot lend more than half of its available volume to the other servers in the ScaleServer group. The transfer of pages from one server to another is final and pages are not returned to the lending server.

The following is a summary of the events surrounding the page sharing and transfer feature:

- A request to create new pages comes from a client module. This request is always directed to a specific Intelligent Capture Server.
- If the server has sufficient pages to satisfy the request, the request is handled by that Intelligent Capture Server. Page sharing or transfer is not required because the server can handle the request to create new pages.
- If the server does not have sufficient pages to satisfy the request, it requests to borrow pages from another server in the ScaleServer group. If there are no other servers with pages to share, then the request from the client is denied and a corresponding error message is returned.
- When a server decides it must borrow pages from another server, the determination of which server to borrow from is based on volume information

that is communicated between the servers in a ScaleServer group. If the borrow request is denied, other servers are queried in turn until the request is either satisfied or no servers are left to query. If the request cannot be satisfied, the server returns an error to the client. If the request is successful, the pages are transferred between servers and the client request is successful. The page sharing operation is performed automatically without impacting client modules.

Notes

- Page count sharing applies to both the server license and licenses used by client modules. Client modules can share page count between different servers having the same license in a ScaleServer group.
- As a server approaches its licensed page count limit, messages are sent to attended modules which display when the user logs in to the module or as batches are created. Also the server logs warnings to the Intelligent Capture Administrator, the Windows Event Log and the `debug.out` so that users can plan on getting more pages licensed.

Related Topics

"Centralized Licensing" on page 101

"Calculating Page Counts" on page 47

"Importing License Codes from a License File" on page 124

"Viewing or Modifying License Code Settings" on page 125

3.12 Monitoring Licenses

Administrators need to know when module licensing is nearing a critical point. Critical points happen when any of the following occur:

- Available module page count is nearing zero
- Available server page count is nearing zero
- Valid Until date is approaching
- Not enough module copies available
- Not enough Intelligent Capture Server connections available

The Intelligent Capture Administrator provides the **Module Licenses** window to monitor Intelligent Capture licenses. Various columns display the pages used and pages available, as well as the percentage of available pages and the percentage of total number of licensed copies of each module used. By monitoring this window, you can determine whether you have adequate licenses and be aware of approximately how long until your licensed page count is used.

When the licensed number of Intelligent Capture Server connections have been consumed, the Intelligent Capture Server refuses connections from additional

modules. When operators are using attended modules, the issue is obvious; however, for unattended modules and modules running as services, you may not immediately be aware of the problem until batches do not complete as expected.

When a license nears a point where it will no longer enable a module to process pages (typically, when its available page count is nearing zero), the Intelligent Capture Server sends appropriate messages to the client modules. However, only attended modules display these messages. Unattended modules and modules running as services cannot display messages of any type.

To determine whether a licensing issue is preventing modules from connecting to an Intelligent Capture Server or, after connection, from processing pages, use the Intelligent Capture Administrator to examine the **Logs** pane in the **Reports / Logs** panel.

Note: The server logs a license warning or error message to the Windows event log. Administrators can configure the Windows event log to send emails when licensing warning messages are added to the log.

Chapter 4

Understanding ScaleServer Technology

ScaleServer is the technology that combines multiple Intelligent Capture Servers into a single information capture system. This provides scalability when processing volume increases beyond the capacity of a single server. ScaleServer technology enables distribution of capture processing among Intelligent Capture Servers.

4.1 Overview of ScaleServer Technology

A ScaleServer group of Intelligent Capture Servers consists of two or more individual Intelligent Capture Servers connected to the same network, and licensed and configured to work together as a single information capture system.

To understand why ScaleServer technology is important, consider how a single-server Intelligent Capture system captures documents in comparison to the ScaleServer capture model:

The Single-Server Capture Model

Without ScaleServer technology, a single Intelligent Capture Server creates batches and sends tasks from those batches to each Intelligent Capture client module, as specified by instructions encoded in the batch. As each module completes its work, it sends the resulting data back to the Intelligent Capture Server where it waits until the appropriate module signals that it is available to perform the next step of the document capture operation.

In this asynchronous, task-at-a-time environment, multiple copies of duplicate modules can run on multiple client workstations providing scalability, redundancy, and high peak throughput.

This single-server model provides a robust information capture system on the client side, but leaves the server side of the system dependent on just one Intelligent Capture Server. This single Intelligent Capture Server must remain on line and must handle both the storage requirements and processing requirements of the entire information capture workload because, without ScaleServer technology, there is no way to expand the server side of an Intelligent Capture system. If the hardware or software of the Intelligent Capture Server fails, or if a server needs to be intentionally taken offline to perform backups, maintenance, or upgrades, then the entire work flow must come to a stop.

The ScaleServer Capture Model

With ScaleServer technology, multiple Intelligent Capture Servers work together, sharing the work load in a single information capture system. Each server manages its own batches and each client machine requests tasks from all available servers.

When a module finishes with a task, it sends the task back to the Intelligent Capture Server that "owns" it.

Multiple Intelligent Capture Servers that are connected using ScaleServer technology provide many benefits. Here are just a few:

- High Availability: An Intelligent Capture system that uses multiple servers can continue operating when a server fails or is intentionally taken offline for maintenance or upgrades. However, batches are tied to individual servers, so if a server goes down, processing of a batch on that server is suspended until the server comes back online. This will not disrupt any other work being processed.
- Increased productivity: With tasks being sent to client workstations from multiple Intelligent Capture Servers, module wait time between arriving tasks can be minimized providing a higher duty cycle for unattended modules and less idle time for attended-module operators.
- Increased scalability: Additional servers can be brought online as needed to handle increasing page volume, without stopping the system.

Related Topics

"Adding and Connecting ScaleServer Groups" on page 128

"Viewing or Modifying ScaleServer Settings" on page 130

"Viewing ScaleServer Groups" on page 126

"Intelligent Capture Permissions List" on page 381

4.2 ScaleServer Functionality and Benefits

ScaleServer technology uses several techniques to ensure maximum productivity from your multi-server information capture system. This section discusses the following points related to ScaleServer functionality:

- "Ensures Existing Processes and Batches are Unique within the ScaleServer Group" on page 53
- "Ensures New Processes and Batches are Unique" on page 53
- "Ensures that Batch Values are Unique" on page 53
- "Enables Modules to Connect to Multiple Servers" on page 53
- "Requeues Incomplete Tasks when a Server Reappears" on page 54
- "Operates Transparently in Run All Batches Mode" on page 54
- "Operates Transparently in Run Single Batch and Open Batch Modes" on page 54

  "Handles Licenses in a Reasonable Manner" on page 54
- "Handles ScaleServer Connections Dynamically" on page 56

Ensures Existing Processes and Batches are Unique within the ScaleServer Group

Each time an Intelligent Capture Server in a ScaleServer group is started, the server performs a self-check for process and batch integrity. An existing process or batch can only exist on one server, so the server does a check to ensure that existing processes and batches are unique within the ScaleServer group. The ScaleServer process and batch identification system not only ensures processes and batches are unique, it also provides a mechanism to ensure that tasks from each batch are returned to the Intelligent Capture Server that "owns" them.

Note: The batch ID is unique across multiple Intelligent Capture Servers within a ScaleServer group, but the batch name need not be unique.

Ensures New Processes and Batches are Unique

All new processes and batches are created on a single Intelligent Capture Server. When a new process is created, it must be installed on one Intelligent Capture Server, set up as needed, and then copied to other Intelligent Capture Servers in the ScaleServer group. The process is then consistent and available across all servers in the group to create new batches on each Intelligent Capture Server.

The Intelligent Capture Administrator module has commands that facilitate copying a process easily to all servers in a ScaleServer group. When a process is copied, the process ID is changed on each server. Even though the processes contain the same contents, but the servers recognize the processes as different.

You cannot have multiple copies of a batch because, unlike processes, batches contain data that must exist on a single server at a time. However, the Intelligent Capture Administrator module enables moving batches from one server to another.

Ensures that Batch Values are Unique

Batch values apply only to the tasks included in the current batch. Batch values include step settings, nodal data, file values, and permissions. These values, and the batch itself, can only reside on a single Intelligent Capture Server in a ScaleServer group. When that server is not online, this data is not available to any of the client modules.

Enables Modules to Connect to Multiple Servers

Within an established ScaleServer group, ScaleServer-compatible modules running in production mode can connect to all or any subset of the Intelligent Capture Servers in the group. To determine if a module is ScaleServer-compatible, see "Appendix—Intelligent Capture Client Modules" on page 569 table.

Note: When an Intelligent Capture Server is removed from a ScaleServer group, the client modules connected to that Intelligent Capture Server will require approximately two minutes to disconnect from the Intelligent Capture Server.

Non-ScaleServer-compatible modules can continue to be used in a ScaleServer group by connecting to one Intelligent Capture Server at a time.

Requeues Incomplete Tasks when a Server Reappears

If a specific server in a ScaleServer group disconnects while processing a task, the task remains unfinished. When the server reconnects, it will resubmit the unfinished task for processing. Thus, an operator might see a task represented because it was not fully processed the first time it was submitted to the module. In this case, the operator should continue processing the task until it completes.

Operates Transparently in Run All Batches Mode

Most Intelligent Capture operators run modules in Run All Batches mode. In this mode, the module receives tasks from all connected servers in a ScaleServer group as soon as tasks are available. The order in which a module receives tasks is determined by the priority setting of the batch from amongst all of the batches on the server from which the task is being sent. That is, the priorities of all batches are not shared amongst all servers in a ScaleServer group. For example, if a client module receives several tasks simultaneously from different servers in the ScaleServer group, then the sequence in which these tasks are processed no longer depends on the individual priority of each task.

Modules continue to receive tasks as long as at least one Intelligent Capture Server is connected and has tasks available for processing. If all servers disconnect (or if the only server disconnects when the module is started with the `-autoreconnect` command line parameter), then the module silently waits for tasks until after a server reconnects and tasks become available.

Operates Transparently in Run Single Batch and Open Batch Modes

In Single Batch mode, operators select the batch to process, and then automatically receive tasks from that batch alone. In Open Batch mode, operators select from among all batches regardless of whether the batches include an instance of the module being used.

In either Run Single Batch or Open Batch mode, the Open Batch window displays a list of batch names only. If it is important for operators to be able to identify the particular server that owns a batch, then use a batch naming convention that identifies the host server.

Handles Licenses in a Reasonable Manner

ScaleServer technology changes the way module connections work when modules connect to multiple Intelligent Capture Servers. When a module connects to a

ScaleServer group, it makes a physical connection to each server specified at login. With ScaleServer connection sharing, only one connection license is consumed by all the module's physical connections. Servers communicate with each other to establish which server, if any, has licensed the connection. The server that has licensed the connection is called the “licensing server”. When any module except for ScanPlus connects to a server that is not the licensing server, a connection license is borrowed from the licensing server, thus preventing the connection from consuming an additional connection license for the module. Hence, a single client module can connect to all servers in a group while consuming only one connection license.

Note: In a ScaleServer group, a ScanPlus module cannot borrow a feature code license from another server within the same ScaleServer group; that is, a ScanPlus module consumes feature code licenses only from the same machine to which it connected. Therefore, make sure that each ScanPlus module connects first to a server that has the appropriate feature code and that the server has enough licenses to accommodate all ScanPlus modules (with their required feature codes) that are to connect to that server. Furthermore, make sure to use the most restrictive feature code that is available for a scanner. For example, for an ISIS Level 3 scanner, use feature code C instead of D; reserve feature code D for a scanner driver that does not have a defined ISIS level.

In the event that the licensing server becomes unavailable, other servers in the group will choose a different server to be the licensing server for the connection, consuming a connection license. This switch occurs for each connection licensed by the server that has become unavailable. In the event that no new connection license is available, other servers in the ScaleServer group will assume that the license is valid until the original licensing server is back online. Then, the other servers in the ScaleServer group will request a connection license from the newly restored server and it will again become the licensing server for this connection. If the server is unable to provide a new connection license when coming back online, the connection will be unlicensed and no further tasks will be sent to the connection.

The following points summarize connection count sharing for license handling:

- When a module connects to a ScaleServer group, only a single connection is consumed per machine running a module, even though the module can connect to multiple servers.
- The module connection to any Intelligent Capture Server in a ScaleServer group succeeds if any of the Intelligent Capture Servers in the group has a valid connection license.
- When a module connects to a ScaleServer group, the first connected Intelligent Capture Server queries the other Intelligent Capture Servers in the group to check if a connection license for that module is already consumed. If found, then it does not consume a connection license for that module. If not found, then it tries to consume the connection license locally if available. If it does not have any valid connection license locally, then it will query all the other Intelligent Capture Servers in the ScaleServer group to see if they have a valid connection license and if so, “borrow” it.

Handles ScaleServer Connections Dynamically

Bringing additional Intelligent Capture Servers online without stopping the entire document capture system keeps both modules and their operators working productively at all times. For more information on adding servers to a ScaleServer group, see"Adding and Connecting ScaleServer Groups" on page 128.

Enables Page Count Sharing

A page is defined as a single-sided image, which is scanned or imported into an Intelligent Capture Server. Each single-sided page is counted once when it enters an Intelligent Capture system. For more information, see"Page Count Sharing and Transfer" on page 48.

Note: Page count sharing applies to both the server license and licenses used by client modules. Client modules can share page count between different servers having the same license in a ScaleServer group.

Examples

If you have two Intelligent Capture Servers (each one has a license for 7.5 million pages) and four module licenses (two from each server) in a ScaleServer group, then the following conditions apply:

- When both servers are running, you can connect up to four Scan clients because you have a total of four module licenses. Furthermore, all four Scan clients are logged into the ScaleServer group, and therefore are connected to both servers simultaneously.
- When one server goes down, then the following conditions apply:
  - Even though the server that supplied two of the licenses is down, all four of the running Scan clients remain operational; that is, the four Scan clients still remain connected to the operational server and can still create batches on it. A client is not disconnected even when its licensing server goes down because in connection count sharing, the client has already consumed a connection count from a license.
  - However, if a user closes one of the four clients and then tries to restart it, then the client cannot log in again because the two licenses available from the operational server are in use.
  - Only two ScanPlus clients can reconnect to the server because each server has two ScanPlus licenses only.
  - You cannot process more than 7.5 million pages because an operational server cannot borrow pages from a non-operational server.

Related Topics

"Adding and Connecting ScaleServer Groups" on page 128

"Viewing or Modifying ScaleServer Settings" on page 130

"Viewing ScaleServer Groups" on page 126

"Intelligent Capture Permissions List" on page 381

Chapter 5

Understanding Intelligent Capture Multiple Language Implementation

Intelligent Capture supports multiple languages within an Intelligent Capture deployment, thereby enabling global document processing. Multiple language support enables Intelligent Capture batches and tasks to process data in multiple languages and use multiple locale settings.

5.1 Prerequisites for Intelligent Capture Multiple Language Implementation

Intelligent Capture multiple language feature has the following prerequisites:

- On a single machine, the locale (specified in the **Regional Options** setting) and code page settings (specified in **Language for non-Unicode Programs** setting) must match; that is, the locale settings and code page must be for the same location. This requirement applies to all Intelligent Capture Server machines and client module machines.
- All machines that run CaptureFlow Designer or Process Developer must use the same code page. If a process contains characters from languages not included in the system code page, define a custom data-only MDF to hold variables for all literal text containing those characters. For more information, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)* or *OpenText Intelligent Capture - Scripting Guide (ECPCORE-PSC)*.

Related Topics

"Intelligent Capture Multiple Language Capabilities" on page 60

"Intelligent Capture Multiple Language Limitations" on page 61

5.2 Intelligent Capture Multiple Language Capabilities

Intelligent Capture multiple language feature includes the following capabilities:

- Intelligent Capture Servers and client modules can run on any supported Windows operating system using single-byte or double-byte code pages. This capability is an enhancement over the Intelligent Capture 6.0 SP3 implementation which only supported a single-byte code page.

  Note: Code page is set per client or server machine.

- Intelligent Capture Servers and client modules can use different code page and locale formatting options. Locale formatting determines the formatting and display of IA Values for items such as dates, numbers, and currency. Locale formatting is always performed using the locale of the account used to run the Intelligent Capture Server or client modules. These values must be read in the same locale to be interpreted correctly.
- The nine localization languages for Intelligent Capture are used to control the User Interface (*UI*) language displayed to the user. For details on how to set the UI language for each Intelligent Capture component, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.
- The *UI* language that Intelligent Capture components use is independent of the languages that can be part of a batch, task, or page. For example, a French customer may set the *UI* language for all client modules to French, but may have French and Chinese data in batches and tasks.
- Batches and tasks can contain data in multiple languages and characters from different code pages.
- Pages can contain data in multiple languages and characters from different codepages provided that the client modules can support it.

  Note: Multiple language is best supported when using only Intelligent Capture client modules from 7.0 versions. It is recommended to upgrade all modules if you require the multiple language feature.

Related Topics

"Intelligent Capture Multiple Language Limitations" on page 61

"Multiple Language Implementation: Use Cases" on page 62

5.3 Intelligent Capture Multiple Language Limitations

Intelligent Capture multiple language feature has the following limitations:

- Client modules listed as "New in 6.x" and "New in 7.0" in table and the Copy and Multi modules which was were available prior to Intelligent Capture 6.0 do not have any limitations.
- Client modules listed as "Available Prior to 6.0" (except for the Copy and Multi modules) in the table have the following limitations:
  - Modules are code page based. These modules can use any code-page but are restricted to using only a single code-page.
  - Batches can contain multiple languages, but care must be taken to ensure that only tasks containing languages in the module's code page are routed to the module. This can be accomplished using Dynamic Step Departments or Task-level routing. See use cases 2 and 3 for examples.
  - Some modules do not support multi-byte (Asian character support) code pages. These modules include:
    - Global 360 Export
    - Timer
- Supporting multiple languages on a page is subject to the capabilities of the individual client modules. For example, NuanceOCR supports recognition of multiple European languages at a time. However, it can recognize only one Asian language at a time. If another Asian language is required, then users must run a different instance of the module for the other Asian language. A mix of Asian and European languages (other than English) is not supported.
- Custom modules may not support multiple-language or Asian languages. Users should verify whether any custom modules they use can process data from multiple code pages and whether any Asian language is supported.
- Formware and ClaimPack are limited to using single-byte code pages. Also, they have only been tested on an English operating system and with English locale formatting options.

Related Topics

"Intelligent Capture Multiple Language Capabilities" on page 60

"Multiple Language Implementation: Use Cases" on page 62

5.4 Multiple Language Implementation: Use Cases

These use cases help understand the multiple language implementation in Intelligent Capture.

1. A customer wants to use English, French, German, Spanish, Italian, and Brazilian Portuguese (languages supported by the 1252 code page) in their batches/tasks/pages using 7.0 client modules. Each client module will process all tasks regardless of language.

   Implementation strategy for client modules:

   - Install, setup, and run 7.0 client modules. Set the code page and locale formatting for dates and numbers to a language supported by the 1252 code page on all client machines. Set the UI language appropriately for each client machine. All date/time/numbers will be formatted using the locale specified by the account used to run the client machine that is processing the batch.

2. A customer wants to use English, French, German, Spanish, Italian, and Brazilian Portuguese (code page 1252) in their batches/tasks/pages using Intelligent Capture 7.0 client modules. They require different operators to run Completion for each different language.

   Implementation strategy for client modules: Implementation is similar to use case 1, with a few changes:

   - Install multiple Completion applications on different client machines.
   - For one Completion client machine, set the code page and locale formatting for dates and numbers to French and specify the UI language as French. For a second Completion machine, set the code page and locale formatting for dates and numbers to Italian and specify the UI language as Italian. Do this for each Completion machine so that there are Completion modules that will run in each of the required languages.
   - Design a process using departments to route tasks to the Completion module instances running in different languages. This might be done with Step-level departments, or at the task level with `IATaskRouting`.
   - Identify the language of your batch or task while it is being processed. Depending on your data, there are different ways that you may identify the language of a batch/task/page. You might use barcodes or patchcodes to identify the language; separate documents by language prior to scanning; or use a module such as Classification to detect distinguishing characteristics on forms of each language, etc. The important point is to identify the language of a document and set either a Step department or IATaskRouting value accordingly for the Completion step.
   - Have each Completion operator start the module with the department for the language in which they will process tasks. Each Completion operator will only receive tasks that match the language of the department they specify.

3. A customer wants to use French (code page 1252) and Russian (code page 1251) in their batches/tasks/pages using a mix of client modules available prior to 6.0 and 7.0 client modules.

   Implementation strategy for client modules:

   - Set up at least two client machines, one set to French Locale and UI and the second set to Russian Locale and UI. Make any changes to the default Locale formatting settings on each machine.
   - For all client modules available prior to 6.0, install a set of the required modules on each client machine. For client modules new in 7.0, there are no restrictions. They can be installed on any of the client machines.
   - Design a process using Step departments or `IATaskRouting` to route tasks to the appropriate language client for processing. Your process must contain logic to set the correct routing (see Use Case 2 for ideas). The Step department or `IATaskRouting` value must be explicitly set in the process for each step that is language-dependent (all modules available prior to 6.0). Also, if using an OCR module, consider whether you need two steps of the module--one to recognize French and one to recognize Russian characters.
   - Start client module instances with departments set appropriately for the language in which they will process. Each module started in this way will only receive tasks that match the department, and therefore the language they specify.

4. A customer wants to use only French language (codepage 1252) in batches but with a mix of Intelligent Capture 6.0 SP3 client modules and 7.0 client modules.

   Implementation strategy for client modules:

   - Make sure that 6.0 SP3 client modules have the code page and locale formatting for dates and numbers set to French.
   - The 7.0 Intelligent Capture Servers must be installed on machines set to the same locale as the 6.0 SP3 client modules since 6.0 SP3 client modules must have the same codepage and locale as Intelligent Capture Server.
   - 7.0 client modules can be installed, either replacing all the SP3 clients on a machine, or on machines in addition to the ones running the SP3 modules.

     Note: Within a single machine, all clients must be of the same version. You cannot install 7.0 and SP3 modules on the same machine.

5. A customer wants to upgrade from Intelligent Capture 6.0 SP3 and start using Korean in their batches.

   Implementation strategy for client modules:

   - Since 6.0 SP3 does not support Asian languages, the customer must upgrade all their client modules to 7.0.
   - Change the locale of some or all of their machines to Korean.
   - Follow suggestions in Use Case 3 to process in a mixed locale environment.

Related Topics

"Intelligent Capture Multiple Language Capabilities" on page 60

"Intelligent Capture Multiple Language Limitations" on page 61

Chapter 6

Understanding Deployment Between Development, Test, and Production Environments

You use the utilities in this section to deploy Intelligent Capture configuration items between development, test, and production environments in an automated manner that allows for backup, rollback, and logging.

6.1 Intelligent Capture Deployment Profile Configuration

`CaptivaDeploymentUI.exe` is an editor for Intelligent Capture deployment profiles. You use it to create a deployment profile or edit an existing one, and then run the deployment profile from a source Intelligent Capture environment to a target environment. A deployment profile (an XML file) specifies individual Intelligent Capture configuration items, their deployment backup and rollback actions, and a log folder. Each deployment profile can be saved in a user-specified file and reused later.

For security purposes, connections and user credentials to the source and target environments must be specified for each individual deployment; that is, they are not persisted in any file.

Note: By default, `CaptivaDeploymentUI.exe` is located in `C:\Program Files (x86)\InputAccel\Client\binnt\`

`CaptivaDeploymentUI.exe` runs `CaptivaDeploymentCmd.exe` for actual deployment. After your deployment profiles are created, you can run `CaptivaDeploymentCmd.exe` manually or through a batch file, instead of running it through `CaptivaDeploymentUI.exe`.

`CaptivaDeploymentCmd.exe` runs the following utilities for individual deployment items:

- `IAMigrate.exe`

  Deploys database objects.

- `Iaadminutil.exe`

  Deploys licenses, IA Server configuration, scale server groups, module setup values, process setup, and process ACLs (including process ACLs for new batches).

- `DeploymentUtility.exe`

  Deploys DCC configuration items.

- `BatchCopyCmd.exe`

  Deploys processes.

- `QuickModuleHost.exe -modulename:ObjectCopy`

  Deploys global scanner configuration items.

  For more information, see "QuickModuleHost.exe ObjectCopy" on page 78.

Notes

- Alternatively, you might use each of these utilities individually, for example, if you have only a few or one-off changes.
- Any command-line value that has spaces must be enclosed within double quotes.
- Each utility has command-line help.
- By default, these utilities are located in `C:\Program Files (x86)\InputAccel\Client\binnt\`.
- For `BatchCopyCmd.exe` and `DeploymentUtility.exe`, if you cannot connect to a server using its IP address, then add its IP address to the `hosts` file.

To deploy a profile:

1. Create a profile or load an existing profile.

   - To create a profile, first specify at least one deployment item and click **Save**.

     Note: A new deployment profile must be saved before you can run it.

   - To load an existing deployment profile to reuse or edit it, click the **...** button to the right of **Deployment profile** and select the profile file.

2. Add deployment items by clicking **Add Item**, selecting an item type, and specifying its value.

   For more information, see:

   "Database Configuration Item Values" on page 68

   "DCC Configuration Item Values" on page 70

   "Other Configuration Item Values" on page 73

3. Specify the following options:

   - **Backup** and **Location**

     See "Backup" on page 68.

   - **Rollback on error**

     See "Rollback on Error" on page 67.

   - **Log folder**

4. To run a deployment, click **Run**, specify connection info for the source and target environments, and then click **Run**, again.

Caution

- To avoid data loss, wait at least five minutes after deployment completes before starting Intelligent Capture Administrator.

Notes

- You are prompted to connect to servers when you run the profile.
- Depending on the type of objects being deployed, some of the connection fields might be disabled. For example, if only database objects are being deployed, then only the database connection fields are enabled.
- If you cannot connect to a server using its IP address, then add its IP address to the `hosts` file.
- Both the source and target servers must be licensed.
- Depending on the volume of deployment data and network connection speed, the deployment may take from a few seconds to several minutes. When deployment is done, a dialog is posted with a brief summary of deployment results. Make sure to check the log file for any errors.

6.1.1 Rollback on Error

None	Do not roll back if an error occurs and continue deployment execution.
RollbackAllAndStop	Roll back all changes on the first error and terminate execution. The rollback is performed in the reverse order.
RollbackCurrentAndStop	On the first error, roll back data for the current item and terminate execution.
RollbackCurrentAndContinue	Only roll back changes for which errors occurred and continue deployment execution with the next item.

6.1.2 Backup

All	Data for every deployment item in the target environment is backed up before the data from the source environment is deployed. Exceptions are License, ProcessAcl, and ProcessNewBatchAcl.
Selected	Data is backed up only for those deployment items for which the corresponding **Backup** check box is selected.
Backup location	Under this root backup folder, another folder is created for the specific deployment runtime session. The folder name schema is: `CaptivaDeployment<YYYYMDHHMMSS>` For instance, if a deployment was started at 10:15:27 am on August 30, 2016, the corresponding folder name would be `CaptivaDeployment2016830101527`. When there are deployment items that need to be backed up and if the specified folder does not already exist, then it is created.

6.1.3 Database Configuration Item Values

For the **Value** field, specify one of the following values:

- Empty

  All objects of the item type are to be deployed.

- Only one object name

  Only the specified object is deployed (for example, if the Department item's value contains `HR`, then only the `HR` department is deployed). If you want to deploy multiple objects of a certain type (but not all of that type's objects), then add a separate deployment item for each object.

Notes

- If any database configuration item is specified in the deployment profile, then an external database must exist in both the source and target servers.
- Any configuration item value that has spaces must be enclosed within double quotes.
- If a configuration item cannot be backed up, then the **Backup** option is disabled for it.

Item Type	Item Value Syntax	Item Description
AllDbObjects	Empty	Includes the complete scope of items handled by `IAMigrate.exe`, which includes all of the items in this table.
Department	Empty or one object name	A database object related to a department (that is, department names and associated ACLs).
Module	Empty or one object name	A database object related to modules (that is, module names and associated ACLs).
PurgeDef	Empty or one object name	A database object related to purge definitions (that is, purge definitions, localized text, purge stored procedures).
PurgeCfg	Empty or one object name	A database object related to configured purges (that is, configured purges and related purge definitions).
ReportDef	Empty or one object name	A database object related to report definitions (that is, report definitions, report samples, localized text).
ReportCfg	Empty or one object name	A database object related to configured reports (that is, configured reports and related report definitions).

Item Type	Item Value Syntax	Item Description
Role	Empty or one object name	A database object related to roles (that is, roles, associated permissions, localized text). **Notes** • The association between roles and user accounts is not distributed. To add user accounts to roles through a command-line interface, use `iaadminutil.exe -set_role_users`. • Changes to role names cannot be deployed. To update role names, you must update them manually in each Intelligent Capture environment by using Intelligent Capture Administrator.
Rule	Empty or one object name	Database objects related to Log Rules (that is, log rules, rule data definitions, filter definitions, sink definitions, sink DLL definitions, localized text).

6.1.4 DCC Configuration Item Values

For the **Value** field, specify one of the following values:

- Empty

  All objects of the item type are to be deployed.

- Only one object name

  Only the specified object is deployed (for example, if the **DocumentType** item's value contains `InvoiceAR`, then only the `InvoiceAR` document type is deployed). If you want to deploy multiple objects of a certain type (but not all of that type's objects), then add a separate deployment item for each object.

- Filter expression

  In case of the update of existing items, the content of most of the DCC items can be filtered.

For both new and updated items, individual configuration item values can be replaced with the content read from a file.

To filter which individual configuration items should be deployed for a particular object, use the `SCOPE` keyword. For example, to specify to only deploy values of the configuration items *`ProcessName`*, *`BatchNameSchema`*, and *`ScriptTag`* for the *`EmailImportProfile`* named *`emailProf1`*:

```
emailProf1,SCOPE,ProcessName,BatchNameSchema,ScriptTag
```

To replace a source value with a value contained in a file, use the `REPLACE` keyword. For example, to specify that during the deployment of `GlobalOptions` item, the value of the *`DeploymentFiles`* should be read from the file, `C:\DeploymentData\GlobalOptions\DeploymentFiles.txt`:

```
REPLACE,DeploymentFiles,C:\DeploymentData\GlobalOptions\DeploymentFiles.txt
```

Both `SCOPE` and `REPLACE` may reference multiple config items. If `SCOPE` is used, then `REPLACE` must reference only `SCOPE` values. For example, in the deployment of the EmailImportProfile named emailProf1, the value for the ScriptTag can be read from a file, `C:\DeploymentData\example\ScriptTag.txt`:

```
emailProf1,SCOPE,ProcessName,BatchNameSchema,ScriptTag,REPLACE,ScriptTag,C:
\DeploymentData\example\ScriptTag.txt
```

Notes

- The following item types cannot be filtered and replaced: *`DocumentResource`*, *`DocumentTypes`*, *`ExportProfile`*, *`ImageProcessing`*, *`NamedQuery`*, *`OcrProfile`*, *`AXConnection`*, *`CmisConnection`*, *`DqlConnection`*, *`EmailConnection`*, *`FileDirectoryConnection`*, *`OdbcConnection`*.
- Any configuration item value that has spaces must be enclosed within double quotes.
- If a configuration item cannot be backed up, then the **Backup** option is disabled for it.

Item Type	Item Value Syntax	Item Description
DccAll	Empty	Includes all of the items handled by `DeploymentUtility.exe`, which includes all of the items in this section. **DccAll** does not deploy XPPs.
AXConnection	Empty, one object name, or a filter expression	ApplicationXtender connection
CmisConnection	Empty, one object name, or a filter expression	CMIS repository connection

Item Type	Item Value Syntax	Item Description
CustomFiles	One file name	A file of any file type, including a script DLL
CustomStyle	Empty	Custom styles
DesktopShortCutKeys	Empty	Intelligent Capture Desktop Shortcuts
DocumentResource	Empty or one object name	• Custom OCR engine definitions used in a Recognition Project • Bitmap images used in document types as background images on the form **Note:** These items are displayed on the Intelligent Capture Designer **Deployment** tab under **Document Resources**.
DocumentTypes	Empty or one object name	Document type
DqlConnection	Empty, one object name, or a filter expression	Documentum connection
EmailConnection	Empty, one object name, or a filter expression	Email connection
EmailImportProfile	Empty, one object name, or a filter expression	Email import profile
ExportProfile	Empty or one object name	Export profile
FileDirectoryConnection	Empty, one object name, or a filter expression	File system connection
FileImportProfile	Empty, one object name, or a filter expression	File system import profile
GlobalOptions	Empty	GlobalOptions
ImageConversion	Empty, one object name, or a filter expression.	Image conversion profile
ImageProcessing	Empty or one object name	Image processing profile.
NamedQuery	Empty or one object name	Query.
OdbcConnection	Empty, one object name, or a filter expression	Database connection.
OcrProfile	Empty or one object name	Standard OCR profile

Item Type	Item Value Syntax	Item Description
ScanImportProfile	Empty, one object name, or a filter expression	Distributed Capture import profile.
SystemStyle	Empty	System Styles.

6.1.5 Other Configuration Item Values

Notes

- Any configuration item value that has spaces must be enclosed within double quotes.
- If a configuration item cannot be backed up, then the **Backup** option is disabled for it.
- DPPs cannot be deployed. Use Dispatcher Manager to deploy them.
- If no processes exist in the target server, then the following configuration items must be deployed as follows:
  1. ProcessIap must be specified before *`ProcessAcl`*, *`ProcessSetup`*, *`ProcessStepSetup`*.
  2. *`ProcessSetup`* must be specified before *`processStepSetup`* and *`CustomScript`*.

Item Type	Item Value Syntax	Item Description
License	License file	The license file to install. Does not support backup and rollback actions. **Note:** Uses `iaadminutil.exe -licfile`.
ProcessIap	`<process_name>, <overwrite_flag(true or false)>`	Deploys an IAP process file and all related CodeBehind DLL's. Example: `InvoiceARExport,true` On rollback the IAP is deleted, if it did not exist before, or is overwritten with its previous instance. **Note:** Uses `BatchCopyCmd.exe`.

Item Type	Item Value Syntax	Item Description
ProcessAcl	Process name	Deploys ACLs for the process. Does not support backup and rollback actions. **Note:** Uses `iaadminutil.exe -copy_proc_acl`.
ProcessNewBatchAcl	Process name	Deploys process ACLs defined for the new batches. Does not support backup and rollback actions. **Note:** Uses `iaadminutil.exe -copy_proc_acl_new_batch`.
ProcessSetup	Process name	Deploys setup of the process. For this deployment to be successful, the target environment must have a process by the same name, and the target process step types (modules) must match the source process step types. If the target process has a different number of steps or the steps are of different types, then deployment fails. The setup is deployed by matching step names, and the steps with different names are skipped without posting an error. **Note:** Uses `iaadminutil.exe` with options: `-exportprocsetup` and `-importprocsetup`.

Item Type	Item Value Syntax	Item Description

ProcessStepSetup	`<process_name>,<process_step>`
	`[,<list>]`
	
	where:
	
	`<list>` is the list of pairs:
	
	`[<value_name>,<full_path_to_file_`
	`with_value_data>]`
		Deploys setup of the specified process step.
		
		To replace a value of one or several step configuration items, specify their names and files containing the replacement values. This functionality is intended for purposes of using predefined values for individual configuration items that cannot be transferred between environments. For instance, Documentum Export "Definitions" value should not be transferred from Test into Production environment. To keep this value from being overwritten during deployment, perform the following procedure:
		
		1. From a process with a Documentum Export step (DCTM) configured with the Defintions value, export DCTM step setup into a file:
		
		`iaadminutil.exe -s <IAShost> -u account -p pwd -exportprocstepsetup SrcProcessName DCTM C:\Captiva\Config\DCTM\SrcProcessName_DCTM_setup.txt`
		
		2. Open the file with the exported data (`SrcProcessName_DCTM_setup.txt`) in a text editor and delete all values except the value following the text "Definitions="
		
		3. Save this modified file:
		
		`C:\Captiva\Config\DCTM\DefinitionsVal.txt`
		
		4. Configure the deployment profile with an item ProcessStepSetup and Value:
		
		`ProcessWithDctmStep,DctmStep,Definitions, C:`

Item Type	Item Value Syntax	Item Description
		`\Captiva\Config\DCTM \DefinitionsVal.txt`
ScaleServerLink	`<scale_server_group_name>, <IAS_server_id>`	Deploys ScaleServer group participation. Only one IAS server may be specified per deployment item. If several servers are put into a group, add a separate deployment item for each server. **Note:** Uses `iaadminutil.exe` with options: `-get_scaleserver`, `-add_scaleserver`, and `-remove_scaleserver` (for rollback).
CustomScript	`<module_name>,<script_name>, <C-sharp_flag(0 or 1)>`	Deploys custom script binaries for legacy modules like ScanPlus. Example: `ScanPlus,ScanPlusScript1.dll ,0` **Note:** Uses `iaadminutil.exe` with options: `-download_script`, `-upload_script`, and `-delete_script`.

Item Type	Item Value Syntax	Item Description

ScanConfig	`<scan_config_name>; <comma-separated_list_of_items>; <optional_state_file>`	Deploys scanner configuration used by ScanPlus.
		
		Example:
		
		`ScannerConfig1;; C:\Captiva\Config\Scanner\State1.txt`
		
		To deploy all configuration items from source into the target environment and not replace the State value, do not specify any items, except the config name:
		
		`<scan_config_name>;;`
		
		If the target environment already has a previous version of the configuration and only several items needs to be updated, list them in the second token, for example:
		
		`ScannerConfig1;State,Tag4;`
		
		If the value of the State item is replaced with a content from a special file, specify this file in the third token, for example:
		
		`ScannerConfig1;Tag4; C:\Captiva\Config\Scanner\State1.txt`
		
		Note: Uses `QuickModuleHost.exe -modulename:ObjectCopy -byname`.

6.1.6 QuickModuleHost.exe ObjectCopy

You use the `QuickModuleHost.exe` ObjectCopy module to deploy ScanPlus and RescanPlus global scanner settings.

Example:

```
QuickModuleHost.exe -login:user1,pswd@server1 -modulename:ObjectCopy
-scopemodule:ScanPlus -write:C\temp\spt3.xml -overwrite -items:state
-byname -statefile:c:\temp\importState1.txt -silent:TestScannerConfig4
```

Notes

- To display command-line help, execute the following:

  ```
  QuickModuleHost.exe -login:<username>,<password>@<servername> -modulename:ObjectCopy
  ```

- `-scopemodule:<module>`

  Module to update. Valid values are the following:

  `ScanPlus`

  `RScanpls`

- `-read`

  Specifies a file into which to download the configuration specified by *`-silent`*. By default (that is, without any file specified), `ScannerConfigurations.xml` is created in the same directory in which `QuickModuleHost.exe` is running. Can be specified with *`-overwrite`*. Cannot be specified with *`-write`*.

- `-write`

  Specifies a file that contains the configuration for upload. Can be specified with *`-overwrite`*. Cannot be specified with `-read`.

- `-overwrite`

  Specify *`-overwrite`* with *`-read`* or *`-write`* to overwrite a file or configuration as follows:

  – When *`-read`* is specified and a file with the same name and path exists, then it is overwritten.

  – When *`-write`* is specified and a configuration with the same name exists, then it is overwritten.

- `-items:<config_names>`

  A comma-separated list of individual configuration items to be updated in the target environment.

- `-statefile:<file_name>`

  A file that contains a replacement value for the State config item specified in `-items`.

- `-byname`

You should specify the *-byname* parameter, so that the write configuration is identified by its name instead of its internal ID because the internal ID might change between deployments. That is, if you delete the original configuration and then consequently reuse the same name, a different ID is generated; consequently, the corresponding configuration would not be updated on the target servers because the internal IDs are different.

6.2 Data Migration from a Test Environment to a Production Environment

In an Intelligent Capture environment with the Intelligent Capture Database installed, all configurations and settings are stored in the Intelligent Capture Database. In an environment with no database installed, all configurations and settings are stored in the `IADBConfig.data` file.

Configuration settings stored in the Intelligent Capture Database or in the `IADBConfig.data` file can be migrated from a test environment to a production environment. Configurations and settings are moved from a test environment to a production environment using the IAMigrate application (`IAMigrate.exe`). `IAMigrate.exe` is located in `C:\Program Files (x86)\InputAccel\Client\binnt` by default:

Caution

- To avoid data loss, wait at least five minutes after `IAMigrate.exe` completes before starting Intelligent Capture Administrator.

6.2.1 IAMigrate Application Requirements:

- `IAMigrate.exe` does not export data from, or import data to, an Intelligent Capture Database that is at a version previous to the 6.5 version. To export data from an existing Intelligent Capture 6.0 or Intelligent Capture 6.0 Service Pack test database, the database must first be upgraded to the 7.0 version. The version of `IAMigrate.exe` shipped with Intelligent Capture 7.0 is only compatible Intelligent Capture Database, version 7.0.
- The `IAMigrate.exe` file can be run from any location as long as the `InputAccel DataAccess.dll` and `Emc.InputAccel.Core.dll` files are in the same location.
- `IAMigrate.exe` must be run from a Windows command prompt.
- Test and production databases or `IADBConfig.data` files must be the same version.
- `IAMigrate.exe` must have access to the appropriate database or `IADBConfig.data` file: either the source for export of data, or the target for import of data. When migrating from a SQL database, the machine on which `IAMigrate.exe` runs must have network access to the SQL Server containing the database.
- None of the Intelligent Capture components must be connected to the database during the migration process. In other words, there cannot be any processing

that involves reading from or writing to database when the data is being migrated.

- It is important to fully backup the production database or `IADBConfig.data` file before attempting any import operations. `IAMigrate.exe` does not include any restore or rollback functionality. `IADBConfig.data` can be backed up by making a copy of the file. Intelligent Capture Databases need to be backed up using SQL Server Management Studio backup functionality.

6.2.2 Intelligent Capture Objects Migrated When Using the IAMigrate Application

Only configurations and settings are migrated from the test to production environment. Note that some of the objects pertaining to reporting tables are not migrated if data is stored in an `IADBConfig.data` file instead of the Intelligent Capture Database. This is because reporting capability is not available when a database is not installed.

Intelligent Capture objects and tables that are migrated from the Intelligent Capture Database include:

- `Departments`
- `Modules`
- `ModuleValues`
- `ModuleFiles`
- `LogRules`
- `PurgeDefinitions`
- `ReportDefintions`
- `ConfiguredPurges`
- `ConfiguredReports`
- `PurgeStoredProcedures`
- `ReportsStoredProcedures`
- `ValueAttribute`
- `ReportSamples`
- `ServerConfig` items

Intelligent Capture objects and tables that are migrated from the IADBConfig.data file include:

- `Departments`
- `Modules`
- `ModuleValues`

- `ModuleFiles`
- `Roles`
- `LogRules`
- `PurgeDefinitions`
- `ConfiguredPurges`
- `ValueAttribute`
- `ServerConfig` items

Note: Changes to role names cannot be deployed. To update role names, you must update them manually in each Intelligent Capture environment by using Intelligent Capture Administrator.

Configuration and settings data not migrated include:

- Batch information
- Process information
- IA Values
- Audit and Error logs
- Permissions and Identities
- Module attributes
- Intelligent Capture Server and ScaleServer group information

The following sections provide more detail about how to use the `IAMigrate.exe` application:

6.2.3 Understanding the Export and Import Modes of the IAMigrate Application

The `IAMigrate.exe` runs in two modes: export mode or import mode. Export mode exports data from the test environment, while import mode imports the exported data to a production environment. To understand more about these two modes, review the following sections:

6.2.3.1 Export Mode of the IAMigrate Application

Exporting data from the test environment is the first step in the migration process. When running in export mode, `IAMigrate.exe` exports the contents of the specified Intelligent Capture Database tables or `IADBConfig.data` file to *XML* files. The *XML* files are created in a directory named `IAMigrate_XML`, located in `EMC\InputAccel` folder in `ProgramData` (`C:\ProgramData\EMC\InputAccel`, by default). These *XML* files must not be changed in any way.

During the export operation, two other files are generated: `IADB_Export.log` and `IADB_ImportControlFilter.csv`. These files are created in a directory named `IAMigrate_Logs`, located in `EMC\InputAccel` folder in `ProgramData` (`C:\ProgramData\EMC\InputAccel`, by default):

- The `IADB_Export.log` file lists the record type, and a unique identifier value for each individual record in each table exported.
- The `IADB_ImportControlFilter.csv` file lists each Intelligent Capture object type, along with a unique identifier value for each object exported, one object per line. Each line includes a numeric control value that controls the import or update behavior of that object to the production environment. Objects can be imported or not imported, updated or not updated to the production environment.

Note: `IAMigrate.exe` can be run multiple times in export mode. The *XML* files are replaced each time, but up to five previous versions of the *LOG* and *CSV* files are preserved.

6.2.3.2 Import Mode of the IAMigrate Application

Import mode of the `IAMigrate.exe` imports data from the test environment to the production database based on the control values set in the `IADB_ImportControlFilter.csv` file. Import mode is always run after running the `IAMigrate.exe` in export mode.

When run in import mode, the `IAMigrate.exe` application reads the `IADB_ImportControlFilter.csv` and associated *XML* files, loads data from the exported *XML* files, and imports Intelligent Capture Objects into the production environment according to their individual control file values in `IADB_ImportControlFilter.csv`. During import, the `IADB_Import.log` is created in the `IAMigrate_Logs` subdirectory.

Running `IAMigrate.exe` in import mode includes a preview option , which allows viewing of Intelligent Capture Objects before the import operation is confirmed. In preview mode the `IADB_ImportPreview.log` file is generated.

Note: Import mode only imports the data to the production environment without validating any of the settings.

Modifying the Import Behavior of Intelligent Capture Objects

Intelligent Capture objects are imported (imported or updated) based on their control value attribute specified in the `IADB_ImportControlFilter.csv` file that is generated when you run the IAMigrate application in export mode. The control values in this file can be modified to specify the import behavior for individual objects, but not be modified otherwise. Use a text editor capable of handling UTF-8 encoded files, and be cautious not to alter the file format or object names.

Control values:

- *0*: Do not import or update this object. If the control value = 0, the object and any related child objects are skipped. All server configuration (`ServerConfig`) items have a default control value = 0.
- *1*: Import but do not update. If the control value = 1 and the object exists in the production database, then the object and all related child objects in the production database are skipped. However, the object is imported if it does not exist in the production database.
- *3*: Import and update. If the control value = 3, a new object is added to the production database if it does not exist, and an existing object is updated. All items except the `ServerConfig` items have a default control value = 3.

Note: If an individual entry for an object cannot be read, the default behavior is to set the control flag value = 0 for that object

Exceptions:

- Some `ServerConfig` items must not be imported, because they require specific settings on the Intelligent Capture Server host machine, such as directory locations, *IP* addresses, or ports. Importing invalid or incompatible `ServerConfig` items can result in a corrupted production database, or in Intelligent Capture Server failures.
- If the test database or `IADBConfig.data` file contains `ServerConfig` items for only one Server ID, import of `ServerConfig` items is allowed. In this case any `ServerConfig` items flagged for import are duplicated for each Server ID in the production environment. If the test database or `IADBConfig.data` file contains `ServerConfig` items for more than one Server IDs, the `IAMigrate.exe` logs a message, but does not allow import of any `ServerConfig` items.

6.2.4 Migrating Data from a Test Database to a Production Database

Note: This section discusses the process of migrating data from a test database to a production database. This process is applicable only if your environment contains an Intelligent Capture Database.

The `IAMigrate.exe` application accepts arguments from the command line. These arguments can be specified in any order:

Arguments to migrate data from the Intelligent Capture Database

Use these arguments to migrate data from the Intelligent Capture Database. These options apply only if you have installed an Intelligent Capture Database and want to migrate data to another Intelligent Capture Database.

- `-help`: Display the application usage message.
- `-silent`: Do not display any user prompts.
- `-mssql`: Export or import from the Intelligent Capture Database. This argument is required.
- `-export`: Export objects from the test database to XML files.
- `-import`: Import objects from XML files to the production database.
- `-objtype`: The types of objects to import/export. All objects of the specified type are imported/exported. To import a specific object only, specify it in `-objname`.
- `-objname`: The name of the object to import. The corresponding type of object must be specified in `-objtype`.
- `-preview`: Preview import operations, without committing changes to the production database. The `-preview` option only works when used with the `-import` argument. It allows all of the import operations to be simulated and logged, without actually committing the changes to the production database.
- `-dbserver <test or production database server name>`: Name of the database server.
- `-dbname <test or production database name>`: Name of the database.
- `-username <username>`: Database user account login name.
- `-password <user password>`: Database user account password.

Note: The database login arguments (`-dbserver`, `-dbname`, `-username`, `-password`), each one followed by a valid value, are required. The `IAMigrate.exe` does not run if these four arguments and values are not specified.

Notes

- Either the `-import` or `-export` arguments must always be specified.

- As a best practice, it is recommended that you first implement, validate, and optimize the configurations and settings in a test database. When done, deploy the settings to a production database.

To migrate configuration data and settings from a test to production database:

1. Review the requirements to run the IAMigrate application.
2. Open a command window and point to `IAMigrate.exe`.
3. Ensure the `IAMigrate.exe` has access to the test database from which the data is exported.
4. Export configuration and settings from the test environment using the following command-line argument:

   `-mssql -export -dbserver <<test database server>> -dbname <<test database name>> -username <<username>> -password <<password>>`

   `IAMigrate.exe` creates one *XML* file for each table exported and a *CSV* file for the entire export operation. For details on the files created, see "Export Mode of the IAMigrate Application" on page 82 .
5. Open the `IADB_ImportControlFilter.csv` file located in the `IAMigrate_Logs` folder using a text editor capable of handling UTF-8 encoded files.
6. Update the control values in the `IADB_ImportControlFilter.csv` file based on how you want the objects imported in the production database. See "Import Mode of the IAMigrate Application" on page 82. By default, all objects except for server configuration items, have a control value of 3 which indicates an import and update. Server configuration items have a control value of 0 which means that the item is not imported or updated. Be cautious not to alter the file format or object names. Save the *CSV* file after making changes.
7. Preview the values that are imported using the following command-line argument:

   `-mssql -import -preview -dbserver <<production database server>> -dbname <<production database name>> -username <<username>> -password <<password>>`

   The preview option enables you to review the import values without committing any of the changes to the production database.
8. After reviewing the import values, commit the exported configuration and settings to the production database using the following command-line argument:

   `-mssql -import -dbserver <<production database server>> -dbname <<production database name>> -username <<username>> -password <<password>>`

   The test database data is now moved to the production database.

Note: The `IAMigrate.exe` does not run unless a successful database login has occurred.

6.2.5 Migrating Data from an IADBConfig.data File

Note: This section discusses the process of migrating data from the `IADBConfig.data` file. This process is applicable only if the current Intelligent Capture installation excludes the Intelligent Capture Database.

Arguments to migrate data from the IADBConfig.data file

Use these arguments to migrate data from the `IADBConfig.data` file. These options apply only if your environment does not include the database installation.

- `-help`: Display the application usage message.
- `-silent`: Do not display any user prompts.
- `-nodb`: Export or import from the `IADBConfig.data` file when a database is not installed.
- `-nodbpath`: location of the `IADBConfig.data` file, for example `C:\IAS`.
- `-export`: Export objects from the test database to XML files.
- `-import`: Import objects from XML files to the production database.
- `-objtype`: The types of objects to import/export. All objects of the specified type are imported/exported. To import a specific object only, specify it in `-objname`.
- `-objname`: The name of the object to import. The corresponding type of object must be specified in `-objtype`.
- `-preview`: Preview import operations, without committing changes to the production database. The `-preview` option only works when used with the `-import` argument. It allows all of the import operations to be simulated and logged, without actually committing the changes to the production database.

Note: Either the `-import` or `-export` arguments must always be specified.

To migrate configuration data and settings from a test IADBConfig.data file to production IADBConfig.data file:

1. Review the requirements to run the IAMigrate application.
2. Open a command window and point to `IAMigrate.exe`.
3. Make sure that the `IAMigrate.exe` has access to the `IADBConfig.data` file from which the data is exported.
4. Export configuration and settings from the test environment using the following command-line argument:

   `-export -nodb -nodbpath <<location of IADBConfig.data>>`

   `IAMigrate.exe` creates one *XML* file for each table exported and a *CSV* file for the entire export operation. For the details on the files created, see "Export Mode of the IAMigrate Application" on page 82 .

5. Open the `IADB_ImportControlFilter.csv` file located in the `IAMigrate_Logs` folder using a text editor capable of handling UTF-8 encoded files.
6. Update the control values in the `IADB_ImportControlFilter.csv` file based on how you want the objects imported in the production database. See "Import Mode of the IAMigrate Application" on page 82. By default, all objects except for server configuration items, have a control value of 3 which indicates an import and update. Server configuration items have a control value of 0 which means that the item is not imported or updated. Be cautious not to alter the file format or object names. Save the *CSV* file after making changes.
7. Preview the values that are imported using the following command-line argument:

   `-import -preview -nodb -nodbpath <<location of IADBConfig.data>>`

   The preview option enables you to review the import values without committing any of the changes to the production database.
8. After reviewing the import values, commit the exported configuration and settings to the production database using the following command-line argument:

   `-import -nodb -nodbpath <<location of IADBConfig.data>>`

   The test database data is now moved to the production database.

Note: The `IAMigrate.exe` does not run unless a successful database login has occurred.

6.2.6 Migrating Data from the Internal Database to Intelligent Capture Database

Customers who initially install Intelligent Capture without a database may later need the additional reporting functionality, scalability with ScaleServer functionality, or improved performance that is available with the Intelligent Capture Database. If they choose to make the change, users can use the `IAMigrate.exe` to facilitate the conversion. `IAMigrate.exe` enables users to move configuration data from `IADBConfig.data` to MS SQL Intelligent Capture Database) while retaining existing user data and settings.

Notes

- For the conversion to be successful, the Intelligent Capture Server machine, domain, and environment must be the same. The only changes allowed are the database type and the location of the database.
- Objects such as server configuration items, identities, roles, permissions, licenses can be migrated as long the server machine, domain, and environment remain the same.
- Users switching from one machine or domain to another should use the standard test-to-production migration to move their data, and avoid the potential issues with machine or domain-specific values.

Intelligent Capture objects and tables that are migrated from the Internal Database to Intelligent Capture Database include:

- `Departments`
- `Modules`
- `ModuleValues`
- `ModuleValueScreenRes`
- `ModuleFiles`
- `Role`
- `RoleIdentity`
- `RolePermission`
- `Permission`
- `Identity`
- `LogRules`
- `ValueAttribute`
- `PurgeDefinitions`
- `ConfiguredPurges`
- `ServerConfig` items

To convert from using the IADBConfig.data file to using the Intelligent Capture Database:

1. Install the Intelligent Capture Database using the Intelligent Capture Database installer. For instructions on installing the database, adding user accounts, and ensuring access to the database from the Intelligent Capture Server machine, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.
2. Stop the Intelligent Capture Server.
3. On the Intelligent Capture Server machine, open a command window and point to `IAMigrate.exe`.
4. Make sure that the `IAMigrate.exe` has access to the `IADBConfig.data` file.
5. Export configuration and settings from `IADBConfig.data` using the following command-line argument:

   `-convert -export -nodb -nodbpath <<location of IADBConfig.data>>`
6. Preview the values that are imported using the following command-line argument:

   `-mssql -import -convert -preview -dbserver <<production database server>> -dbname <<production database name>> -username <<username>> -password <<password>>`

The preview option enables you to review the import values without committing any of the changes to the production database.

7. After reviewing the import values, commit the exported configuration and settings to the production database using the following command-line argument:

   ```
   -mssql -import -convert -dbserver <<production database server>>
    -dbname <<production database name>> -username <<username>>
    -password <<password>>
   ```

8. Ensure connectivity between the server and the Intelligent Capture Database. Run DalConfig.exe from the `binnt` directory where the Intelligent Capture Server is installed. In the **Data Access Layer Configuration** window, select the following:

   1. **Database Type**: MSSQL Server.
   2. **Data Store ID**: InputAccel Database.
   3. **Data Source (Server)**: Type the name of the SQL Server to which you want to connect.
   4. **Catalog**: Type the name of the Intelligent Capture Database on the SQL Server. The default name for the Intelligent Capture Database is **IADB**; however, it may have been renamed.
   5. **User** and **Password**: Type the credentials for the newly created SQL database.
   6. **Test Connection**: Click to test the connection between the server and the database.
   7. **Save**: Click to save the new settings.

9. To indicate that the Intelligent Capture Server is now using the MS SQL Intelligent Capture Database, change the `ExternalDatabase` value in the `HKEY_LOCAL_MACHINE\SOFTWARE\InputAccel\Server` key as follows:

   ```
   "ExternalDatabase"="1"
   ```

10. Restart the server. The server will now connect to and use the Intelligent Capture Database.

Chapter 7

Getting Started with Intelligent Capture Administrator

Intelligent Capture Administrator is an administration tool for Intelligent Capture. This section discusses the various tools provided by Intelligent CaptureAdministrator to administer Intelligent Capture.

The *Using Intelligent Capture Administrator* section is designed to present users with conceptual information about the Intelligent CaptureAdministrator module, as well as step-by-step instructions on how to use the module. The topics within this section cover basic overview information, introducing the features and functions of the module.

7.1 Understanding Intelligent Capture Administrator

Intelligent Capture Administrator is an administration tool for Intelligent Capture that enables administrative personnel to monitor, edit, adjust, and respond to most Intelligent Capture administrative needs. Intelligent Capture Administrator centralizes and consolidates many activities, including the following key administrator activities:

- Server administration
  - Licensing, configuring, monitoring, and controlling all Intelligent Capture Servers within your organization
  - Licensing, establishing, and monitoring ScaleServer groups of Intelligent Capture Servers
- Client module license administration
- User administration
- Client administration
- Reporting, logging, and performance monitoring administration
- Configuring access control through a system of users, groups, permissions, and access control lists
- Web Services configuration and administration

Related Topics

"Monitoring Intelligent Capture" on page 96

"Centralized Settings Configuration" on page 100

"Centralized Licensing" on page 101

"Centralized Logging" on page 101

"Flexible Reports" on page 102

"Performance Monitoring" on page 103

"Robust Security and Access Control" on page 103

"Web Services" on page 104

7.1.1 Intelligent Capture Administrator Component Interactions and User interface Language

The Intelligent Capture Administrator interacts with your Intelligent Capture system on several levels to enable it to perform all necessary administrative tasks. Many of the components work behind the scenes, but result in the high availability of up-to-date, useful information.

Table 7-1: Intelligent Capture Administrator Interaction with Intelligent Capture Components

Component	Intelligent Capture Administrator Interaction
Intelligent Capture Servers	Performs all Intelligent Capture Server administrative access: • Activate Intelligent Capture Servers and install and manage licenses. • Add and remove individual Intelligent Capture Servers. • Create, modify, and remove ScaleServer groups. • List Intelligent Capture Servers per ScaleServer group. • Manage Intelligent Capture Server settings.
Processes and batches	Performs all process and batch administration and control: • Install and manage processes on selected Intelligent Capture Servers. • Create new batches. • Define process and batch step settings. • Monitor batch status and batch traffic.

Component	Intelligent Capture Administrator Interaction
Modules	Performs administrative tasks related to Intelligent Capture modules: • Add new modules so they can be recognized by the system. • Display module task processing status. • List batches and processes to which the module is assigned, as well as open connections to the module.
Database	The Intelligent Capture Database is an optional install component. If installed, the following additional features are available within Intelligent Capture: • Enables reporting and logging functionality. The database stores statistical data for use in reports, enabling reports to be generated without requiring an Intelligent Capture Server to load batches to retrieve the data for the reports. • Enables ScaleServer support. • Web Services support. The database manages call and task queues for the Web Services modules, and enables features such as load balancing, asynchronous task handling, and free-form interactions with third-party systems.
Security	Interacts with the Security subsystem to implement the level of security required by the organization, and includes features that control access to various parts of the Intelligent Capture Administrator itself, including: • Manage server and module license codes. • Facilitate Intelligent Capture Server activation. • Define user roles and permissions.

Component	Intelligent Capture Administrator Interaction
Logging	Configures the logging subsystem to capture meaningful, real-time data: • Define log view filters. • Create custom log rules. • Create data definitions that define additional data to pass with the log. • Define filters to limit the type of data that is logged. • Create sink definitions to specify the log file destination: database, file, or Windows event log. **Note:** Most logging functionality is available only if the Intelligent Capture Database is installed. If the database is not installed, only error and warning logs are available and can be configured.
Reports	Configures the database (if installed) to generate meaningful, customizable reports: • Define report definitions that specify a stored procedure for gathering report data. • Select and generate reports. • Configure automatic purging of old reports. • View and manage purge definitions. • Integrate with Crystal Reports to design, display, and print custom reports.
Auditing	Provides pre-configured reports for key auditing activities: • File audit trail report: captures information regarding the viewing and modifying of data captured by the Intelligent Capture system, including when a document was created, modified, viewed, and deleted. • Module audit trail report: records information, including a date and time stamp, for each module that created, accessed, processed, modified, or deleted an image or a batch, in compliance with *FDA* 21 *CFR* Part 11 regulations.

Related Topics

"Intelligent Capture Administrator Layout" on page 95

"Monitoring Intelligent Capture" on page 96

7.1.2 Intelligent Capture Administrator Layout

After logging in with a valid user name, password, Intelligent Capture Server, and domain name, the main **Intelligent Capture Administrator** window opens (Figure 7-1). The **Intelligent Capture Administrator** window consists of three main areas:

- Navigation panel: Displays a column of navigation options.
- Subnavigation panel: Displays a list of links related to the selected main navigation option.
- Main activity pane: Displays the activity that has been selected in the navigation panel. The main activity pane may be further subdivided into separate sections. Many of these sections contain one or more lists of detailed information about the selected activity.

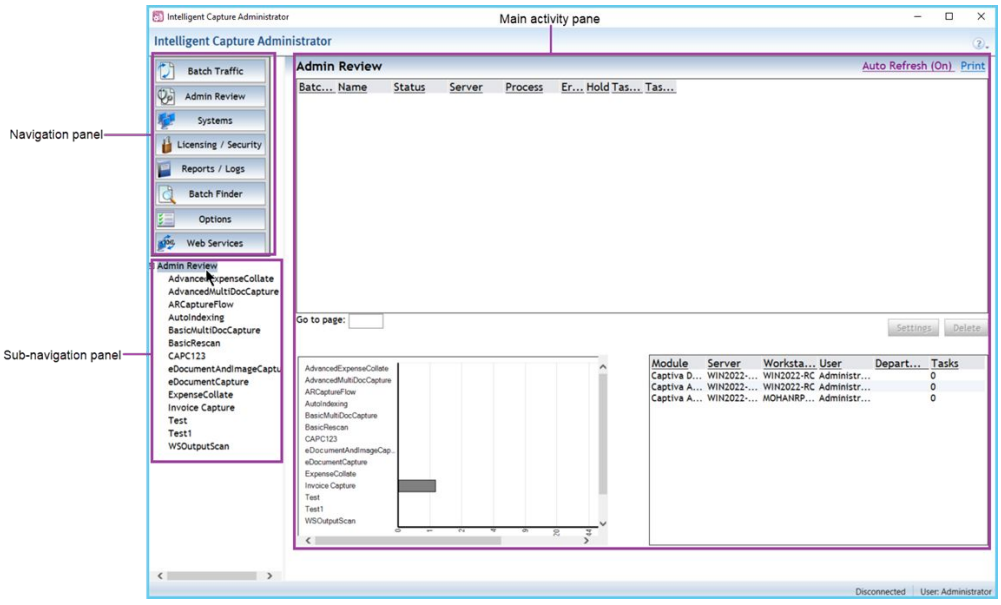

Figure 7-1: Intelligent Capture Administrator— main window

The default activity that is displayed by the Intelligent Capture Administrator immediately after logging on is defined in the **Default Settings** and **Custom Settings** panes; therefore, the initial appearance of the Intelligent Capture Administrator may vary from user to user. The factory default activity is **Batch Traffic**.

Notes

- The Intelligent Capture Administrator does not have a traditional menu bar. Most commands and options are located in context menus that are accessed by right-clicking an item (for example: process, batch) in the main activity pane.
- Use the Navigation and Sub navigation panels to move around in Intelligent Capture Administrator.

Related Topics

"Intelligent Capture Permissions List" on page 381

"Monitoring Intelligent Capture" on page 96

7.2 Monitoring Intelligent Capture

Intelligent Capture Administrator provides monitoring of information and metrics related to all aspects of running an Intelligent Capture installation. The following table describes each of the main activities that the Intelligent Capture Administrator can perform and provides links to topics that contain more detailed information:

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 7-2: Intelligent Capture Administrator Activities

Component	Description
Batch Traffic	Initially displays a list of all batches that exist in all connected Intelligent Capture Servers together with a list of all installed processes and modules that are used as steps in those processes. In addition, it displays a bar graph showing the task count for each module step in each process. By selecting an individual process from the list of links at the bottom of the navigation panel, the **Batch Traffic** pane changes to display information about only those batches that have been created from the selected process.
Admin Review	A variation on the **Batch Traffic** pane, the **Admin Review** pane displays a quick status of all batches that either are on hold or have errors, enabling an administrator to quickly locate trouble spots in their work centers. By selecting an individual process from the list of links at the bottom of the navigation panel, the **Admin Review** pane changes to display the status of only those batches that were created from the selected process.

Component	Description
Systems	Displays links to view and manage system settings, including: • **Servers**: Adds, displays, and deletes Intelligent Capture Servers. • **ScaleServer Groups**: Adds, displays, and deletes ScaleServer groups. • **Processes**: Installs, displays, and deletes processes and defines their module steps by running them in setup mode. **Note:** Some menu items are disabled for Intelligent Capture Designer processes because of their multi-file structure. Instead you should use Intelligent Capture Designer because it has extensive functionality for deploying and maintaining its processes on Intelligent Capture Servers. • **Modules**: Adds, displays, and deletes modules and displays all batches and processes that use a selected module. • **Monitor**: – Lists the client modules that are currently processing batches on the Intelligent Capture Server. – Selecting a module displays batches (in any batch status) that have tasks in the Ready state for the module. You can also right-click a module to select the applicable actions, such as viewing its settings. **Note:** The available actions are a subset of those for modules in the **Modules** pane. – In the **Batches ready and waiting** table, you can select multiple batches and then right-click to select the applicable actions, such as changing batch priority. **Note:** The available actions are the same as those for batches in the **Modules** pane. • **Connections**: Displays all active module connections together with a list of batches that contain steps of a selected module.

Component	Description
	• **Departments**: Adds, displays, and deletes departments.
Licensing / Security	Defines all aspects of Intelligent Capture security, including: • **License Codes**: Adds and displays license codes and enables removal of expired licenses. • **Module Licenses**: Displays licensing details for each module license that has been installed. • **Server Activations**: Facilitates installing activation files for each server in your enterprise and activating these servers. • **Roles**: Defines user roles, assigns them permissions, and adds and removes domain users and groups to or from these roles.
Reports / Logs	Manages the reporting and logging capabilities of the Intelligent Capture system, including: • **Reports**: Adds and displays reports. • **Report Definitions**: Defines new reports and manages existing report definitions. • **Purges**: Adds and displays purges. • **Purge Definitions**: Defines new purges and manages existing purge definitions. • **Logs**: Displays logged events. • **Log View Filters**: Adds new log viewing filters and manages existing log filters. • **Log Rules**: Defines the rules about what to log, when to log it, and where to log it.
Batch Finder	Performs simple and advanced searches and filtering to help find batches, and enables users to save search and filter definitions for future use. Advanced searches can find batches based on batch properties such as name, description, server, process, status, priority, batch creation date, and IA Values within the batch data.

Component	Description
Options	Defines global and user options for the Intelligent Capture Administrator. **Global Options** define all instances of the Intelligent Capture Administrator running on any workstation. **User Options** override **Global Options** and apply only to the logged-in user. Options specify the starting page, the number of rows to display in each table, and the maximum number of batches to retrieve at one time, as well as how often to refresh the data displayed in each of the screens. Options also define the workstations you want to monitor, default logging events, the location of the local tool directory, and whether to run modules using restricted or unrestricted mode.
Web Services	Manages web services for Intelligent Capture, enabling you to add, view, and remove web services and web service hostings, and define web services global options, including *SQL* server connections and network options for the Web Services subsystem. **Note:** The **Web services** options are unavailable unless the Web Services components have been installed.
Help	Displays help about the current activity.

Related Topics

"Intelligent Capture Permissions List" on page 381

"Intelligent Capture Administrator Component Interactions and User interface Language" on page 92

7.3 Centralized Settings Configuration

The Intelligent Capture Server stores all Intelligent Capture configuration data. This data is accessed by client workstations, the Web Services subsystem, one or more Intelligent Capture Administrator instances, and any other components that have a need for this information. The types of configuration settings stored include:

- License codes for all Intelligent Capture Servers.
- Logging rules that are used to capture errors, audit data, and other values for use in various displays and reports.
- Settings for modules that are run as services.
- Settings for ScaleServer groups.
- Module settings that are not task based; that is, settings that are not associated with *IPP*s.
- User settings such as window sizes, position, and layout, enabling these settings to be applied to any workstation an operator chooses to use.
- Web Services subsystem configuration, such as the hostings list, the registered web services list, the process name for each web service method that starts a new batch, and security settings for hostings.

Related Topics

"Managing Intelligent Capture Licenses" on page 122

"Managing ScaleServer Groups" on page 126

"Managing Processes" on page 153

"Viewing All Batches in the System" on page 166

"Monitoring Intelligent Capture" on page 96

"Understanding Logs" on page 206

"Understanding Log Rules" on page 215

"Understanding Report Definitions" on page 232

7.4 Centralized Licensing

Intelligent Capture licensing is based on date ranges, page counts per day, and other factors, and is customized for the needs of each customer. Large enterprises may have multiple Intelligent Capture Servers, either operating independently or as members of ScaleServer groups.

Page counts are maintained within each Intelligent Capture Server. Intelligent Capture Servers within the same ScaleServer group can share page counts from each of their licenses, enabling automatic load balancing. For example, if one Intelligent Capture Server has used all of its licensed page count for the day, other Intelligent Capture Servers within the same ScaleServer group can credit some of their available page count to it so that all servers can continue working.

Related Topics

"Managing Intelligent Capture Licenses" on page 122

"Managing ScaleServer Groups" on page 126

7.5 Centralized Logging

Intelligent Capture features a comprehensive logging and instrumentation subsystem that not only provides critical information within the Intelligent Capture Administrator, but also forms the basis for several other Intelligent Capture features, such as reports. Some logging events are preconfigured so that critical system data is always captured. Other logging events can be customer-configured using logging rules.

Logs can be viewed directly within the Intelligent Capture Administrator, and log data can be included in reports. Because logs can contain a lot of data, log filters can be defined to limit the amount of information display to areas of interest. In addition, logs can be written to various locations by creating logging sink definitions. For example, log data can be written to a file, to a database, or to the Windows Event Log.

Note: The Intelligent Capture logging subsystem cannot log client module events until a client module successfully connects to an Intelligent Capture Server. Therefore, errors that occur when a client module is not connected are instead written directly to the Windows Event Log. For example, if an invalid department name is specified, the client log in does not complete; therefore, the Intelligent Capture logging system cannot log the error. Instead, the client module writes the error to the Windows Event Log.

Related Topics

"Understanding Logs" on page 206

"Understanding Log View Filters" on page 212

"Understanding Log Rules" on page 215

7.6 Flexible Reports

Accurate and timely information is important to any enterprise datacenter. If installed, the Intelligent CaptureDatabase records information from key operational areas and makes it available for use in reports. The report information recorded by the Intelligent Capture Database includes:

- Detailed processing information, including information about interactions between modules and individual pages.
- Module performance metrics, such as page recognition times, module processing times, and times associated with automated processes.
- Operator metrics, including operator performance information such as characters typed, fields indexed, pages processed, and so forth.
- Events that have been logged by the centralized logging facility.
- Custom data that has been designated by the customer.
- Custom reports created for custom modules.

In addition to gathering data for reports, the Intelligent Capture reporting features include the ability to display a number of preconfigured reports and to define custom reports. Because reports are based on data that was captured and saved in real time while batches were being processed, the reports can be generated and displayed without actually asking the Intelligent Capture Server to load the batches.

Note: The Intelligent Capture Database supports installation on a case sensitive SQL Server. The Intelligent Capture Database, however, is case insensitive. This means that upper and lower case characters are not differentiated and instead are treated the same way when performing searches or using the reports functionality in Intelligent Capture.

Related Topics

"Understanding Report Definitions" on page 232

"Understanding Purging" on page 246

7.7 Performance Monitoring

Enterprise document capture operations demand high availability and maximum performance from every component. Administrators need to be aware of performance at multiple levels, including overall system health and performance, individual module performance, and operator performance. This information should lead easily to the identification of bottlenecks in the capture workflow.

Intelligent Capture facilitates performance monitoring through a series of reports covering batches, documents within batches, and pages within documents. Each item of data can be reconciled against activity throughout the system down to the individual node level. Performance reports can be exported to formats compatible with popular spreadsheet programs for further analysis. Intelligent Capture also includes performance counters that can be used to monitor the Intelligent Capture system performance.

Depending on how the performance monitoring feature is licensed, user performance statistics are either stored and displayed with actual user identification or with generic user identification, enabling Intelligent Capture to operate within the data gathering regulations of the locale in which it is being used.

Related Topics

"Monitoring Intelligent Capture" on page 96

"Robust Security and Access Control" on page 103

7.8 Robust Security and Access Control

Intelligent Capture features a robust security system with multiple levels of access control. Each user is identified through a unique user ID and password in the Intelligent Capture system. When identified, users are assigned roles that give them access only to those system features they need to use. Access control is defined in Intelligent Capture Administrator by a user who has permission to define user roles. Even within the Intelligent Capture Administrator itself, administrator access can be limited to just those features that each category of administrator needs to access. In addition, operators can be assigned to roles that limit which processes and batches they can access.

In addition to user roles, the following features ensure that data within the Intelligent Capture system remains secure:

- The Intelligent Capture Server runs in a secure mode such that its folder need not be shared, preventing unauthorized access to files that are stored on the server.
- The Intelligent Capture Administrator and other attended modules automatically disconnect after a time delay to prevent unauthorized viewing of images and data in cases where a workstation is left unattended without logging out. When the module window is again accessed after the timeout period, it requires the user to enter login information before allowing access to the module.

- All Intelligent Capture data stored in files on Intelligent Capture Servers or client workstations, as well as data communicated over a network (including the Internet) can be encrypted to prevent unauthorized access. Encryption is accomplished by using the encryption capabilities of the underlying platform (Encrypting File Systems, Secure Sockets Layer, *IPSec*, and other encryption standards).
- All modules new in Intelligent Capture 6.0 and later are designed and tested to meet the requirements of the Health Insurance Portability and Accountability Act (*HIPPA*) of 1996, which requires that patient data remain secure throughout its lifecycle.

Related Topics

"Managing Users and Groups" on page 142

"Configuring Roles" on page 131

"Configuring the Access Control List" on page 138

7.9 Web Services

Intelligent Capture Web Services is a set of components that enables the Intelligent Capture system to be either a consumer or a provider of web services, or both. The Intelligent Capture Web Services subsystem includes the components described in the following table.

Note: The Web Services Hosting service and Web Services Coordinator service are used only with the Web Services Input module. The Web Services Output module functions on its own, without these additional components.

Table 7-3: Web Services Components

Component	Description
Web Services Hosting	Provides an Intelligent Capture-specific web server that acts as a web services provider, receiving and processing requests for the Web Services Input module. It extracts input parameters in *XML* format and transmits them to the Web Services Coordinator, and then waits to receive output parameters from the Web Services Coordinator to send in response to the caller. Web Services Hosting is a Windows service that is installed during the Client Components phase of the installation process, as described in the *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

Component	Description
Web Services Coordinator	Manages web service hostings by storing request parameters until response parameters are available, enabling a scalable, asynchronous web services implementation. It uses the Intelligent Capture Database to store the requests and responses. The Web Services Coordinator uses the Client to connect to the Intelligent Capture Server. The recommended connectivity is through integrated security. The Web Services Coordinator matches up requests and responses by using configuration data and Correlation ID mapping, enabling Web Services Input to start processing tasks only when both the module is triggered and all necessary web service responses have been received. The Web Services Coordinator also enables the possibility of using multiple Web Services Hosting instances, some of which can be isolated from the public network by a firewall, while others are configured for public Internet access. The Web Services Coordinator uses .NET Remoting to communicate with Web Services Hosting, the Web Services Input module, and the Intelligent Capture Administrator. Web Services Coordinator is a Windows service that is installed during the Client Components phase of the installation process, as described in the *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.
Intelligent Capture Database	Provides a storage location for web service request parameters that are stored by the Web Services Coordinator until response parameters are available. Maintains a web services call queue and a web services task queue that facilitate web call-task synchronization. The Intelligent Capture Database is defined within Microsoft SQL Server during the database installation process, as described in the *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

Component	Description
Web Services Input module	An Intelligent Capture module that serves as a web services provider, processing *SOA* requests from external web service consumers. The Web Services Input module can process requests from any web service clients that make use of Microsoft WSE 3.0, JAX-WS 2.0, or Apache Axis2. A Web Services Input module step can be included as the first module in a process, in which case it creates new batches based on a specified process name, or it can be included as a later step, in which case it can insert new data and files into an existing batch. The module provides mapping for simple parameters (single values, structures, and arrays), and it implements client-side scripting to process more complex parameters. The Web Services Input module is installed during the Client Components phase of the installation process, as described in the *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*. The Web Services Input module is fully described in the *OpenText Intelligent Capture - General Import/Export Modules Guide (ECPCORE-CIO)*.

Component	Description
Web Services Output module	An Intelligent Capture module that serves as a web services consumer, using Internet protocols to access the functionality of external *SOA* participants (web services providers). By using connection information that is specified during module setup, the Web Services Output module generates a proxy that can communicate with an external web service. By using mapping information specified during module setup, the module converts data stored in IA Values into parameters that are meaningful to the external web service client. The Web Services Output module also has a client-side scripting interface to enable more complex operations that are not part of the built-in functionality. The Web Services Output module is installed during the Client Components phase of the installation process, as described in the *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*. The Web Services Output module is fully described in the *OpenText Intelligent Capture - General Import/Export Modules Guide (ECPCORE-CIO)*.

Intelligent Capture Web Services enable external systems to interact with Intelligent Capture workflows and enables Intelligent Capture to interact with the workflows of external systems. As well, external systems can use only the specific capabilities of individual Intelligent Capture modules. For example, you can create a process that consists of a Web Services Input step, a processing module step (for example, NuanceOCR), and a Web Services Output step. The Web Services Input step receives data and files from the external system, creates a new batch based on an associated process, then initiates processing with the specific Intelligent Capture module. After processing completes, the Web Services Output step sends the results back to the external system.

Related Topics

"Intelligent Capture Permissions List" on page 381

"Managing Web Services and Hosting" on page 251

Chapter 8

Configuring Intelligent Capture Administrator

Before using the Intelligent Capture Administrator, configure it to meet business requirements. For more information on installing the application, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

8.1 Setting Up Intelligent Capture Administrator

Topics in this section include important tasks to perform after successfully installing the product. Use these concepts and tasks to configure the environment.

There are a number of default and user configuration options in Intelligent Capture Administrator. These configuration options specify the users' preference of the startup window to view when logged in to Intelligent Capture Administrator and other settings. These configurations are stored for each user and displayed when users login to Intelligent Capture Administrator.

8.1.1 Logging In to Intelligent Capture Administrator

To log in to Intelligent Capture Administrator:

1. Select **Start** > **All Programs** > **OpenText Intelligent Capture** > **Intelligent Capture Administrator**.

   Note: Make sure the Intelligent Capture Server is running.

2. As the module starts, it displays a **Login** window. Enter a **Server** name.
3. Enter your Windows login credentials. The **User** drop down list contains the name of the current logged in user, followed by a list of known domains. If the domain is not specified, it is assumed you are using the same domain as the current logged in user.
4. Click **Login**.

Related Topics

"Specifying Intelligent Capture Administrator Default Settings" on page 110

"Setting Preferences for Your Work Environment" on page 111

8.1.2 Specifying Intelligent Capture Administrator Default Settings

Intelligent Capture Administrator settings enable administrators to set options that apply to the Intelligent Capture Administrator application. In addition, individual users can override the **Default Settings** by specifying **Custom Settings**.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To set Intelligent Capture Administrator default settings:

1. In the **Intelligent Capture Administrator** window, select **Options** from the navigation panel to display the **Options** pane.
2. Click **Default Settings** to display the **Default Settings** pane.
3. In the **Display Options** section:
   - **Start page**: Select the default pane that displays when the user logs in to Intelligent Capture Administrator.
   - **Maximum number of rows in table lists**: Select the number of rows to display in each table.
   - **Maximum number of batches**: Select the maximum number of batches to display.
   - **Maximum number of logs**: Select the maximum number of logs saved in the system.
   - **Show Internal Steps**: Select to display internal steps (`IABatchCreationMerge`, `ENDDone`, `Gateway` and `GatewayEndBlock`) in all applicable panes (for example, the **Steps** pane in **Batch Settings**).

     Note: Some steps, such as `ENDDelete`, should always be visible.
4. In **Page Refresh Rates**, specify the **Current Refresh Rate** in seconds for the listed **Intelligent Capture Administrator** windows and panes.

   Note: **Page Refresh Rates** automatically refresh the pane. If auto refresh occurs while performing administrative tasks on one of the pane, any work being performed can be disrupted. When performing administrative tasks on one of these pane, use the **Auto Refresh** link on the particular pane to turn off auto refresh. When finished, click the link again to switch auto refresh back on. Note that the specified **Auto Refresh** setting is session-wide and is not maintained between sessions.
5. In **Module Setup Options**, select a setup options:
   - **Restricted (does not consume a license)**: Use to setup the module without using a license. In this mode the module is restricted from getting or setting nodal data.

- **Unrestricted**: Use to setup a module using a license.

6. Click the appropriate option to continue:

   - **Apply Recommended Settings**: Use to restore the settings to the default settings.
   - **OK**: Use to save the displayed settings.
   - **Cancel**: Use to discard the changes and return to the previous window.

Related Topics

"Logging In to Intelligent Capture Administrator" on page 109

"Setting Preferences for Your Work Environment" on page 111

"Intelligent Capture Permissions List" on page 381

8.1.3 Setting Preferences for Your Work Environment

Users can specify their individual options for their Intelligent Capture Administrator session. These options override the **Default Settings**. These settings are specific to your work environment.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To set Intelligent Capture Administrator custom settings:

1. In the **Intelligent Capture Administrator** window, select **Options** from the navigation panel to display the **Options** pane.
2. Select **My Preferences** to display the **My Preferences** pane and set the user preferences for your work environment.
3. In the **Display Options** section:

   - **Start page**: Select the default pane that displays when the user logs in to Intelligent Capture Administrator.
   - **Maximum number of rows in table lists**: Select the number of rows to display in each table.
   - **Maximum number of batches**: Select the maximum number of batches to display.
   - **Maximum number of logs**: Select the maximum number of logs saved in the system.
   - **Show Internal Steps**: Select to display internal steps, such as `IABatchCreationMerge`, in all applicable panes (for example, the **Steps** pane in **Batch Settings**).

     Note: Some steps, such as `ENDDelete` should always be visible.

4. In the **Page Refresh Rates** select the **Screen Name** and specify the **Current Refresh Rate** if changing the value from the **Default Refresh Rate**.

   Note: Page Refresh Rates automatically refresh the pane. If auto refresh occurs while performing administrative tasks on one of the pane, any work being performed can be disrupted. When performing administrative tasks on one of these pane, use the **Auto Refresh** link on the particular pane to turn off auto refresh. When finished, click the link again to switch auto refresh back on.

5. In **Module Setup Options**, select a setup options:

   - **Restricted (does not consume a license)**: Use to setup the module without using a license. In this mode the module is restricted from getting or setting nodal data.
   - **Unrestricted**: Use to setup a module using a license.

6. Click the appropriate button to continue:

   - **Apply Recommended Settings**: Restores the recommended "factory" settings.
   - **Apply Default Settings**: Discards any custom settings and restores the default settings.
   - **OK**: Save the displayed settings.

Related Topics

"Logging In to Intelligent Capture Administrator" on page 109

"Specifying Intelligent Capture Administrator Default Settings" on page 110

"Intelligent Capture Permissions List" on page 381

8.2 Customizing Information Tables Using the Column Manager

Intelligent Capture Administrator displays information in tables. Users can configure these tables to display or hide columns and change the column positions.

Caution

When the columns are rearranged, resized, or otherwise modified, the default settings are no longer available.

To customize table columns using the Column Manager:

1. In the **Intelligent Capture Administrator** window, navigate to any of the panes that display information in tables, for instance select **Licensing / Security** >

View License Codes to display the **License Codes** pane. This pane contains information about all license codes in the system.

2. Right-click the column header to display the **Intelligent Capture Administrator Column Manager**.

   Note: The column manager functionality is only available when the header row text is *bold*, underlined, and displayed in a gray background.

3. In the **Column Manager** window:

   - Select the columns to display from the **Hidden Columns** list box and click **>>** to move the selected items to the **Visible Columns** list box. After setting the column configuration for a table, only the selected columns are displayed in the window or pane in the order specified.
   - Select items from the **Visible Columns** list box and click **Up** or **Down** to position the selected item within the list box.

4. Click **OK** to save the settings.

Note: Some columns may contain no data and may be blank for all the rows in the table.

Related Topics

"Specifying Intelligent Capture Administrator Default Settings" on page 110

"Setting Preferences for Your Work Environment" on page 111

Chapter 9

Managing Intelligent Capture Using the Intelligent Capture Administrator

After Intelligent Capture Administrator has been configured, administrators will follow the topics in this section to use and maintain the application.

9.1 Managing Intelligent Capture Servers

You can add registered Intelligent Capture Servers to the Intelligent Capture Administrator and then activate the servers. Activated servers can then be managed and monitored. For more information on installing and configuring Intelligent Capture Servers, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

9.1.1 Viewing the List of Intelligent Capture Servers

You can view the list of all Intelligent Capture Servers registered in the system.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view the list of Intelligent Capture Servers:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel.
2. Click **View Servers**. The **Servers** pane displays the list of all registered Intelligent Capture Servers in the system.
3. Click **Add** to add and connect a new Intelligent Capture Server to administer in Intelligent Capture Administrator.
4. To delete Intelligent Capture Servers, select the relevant servers from the list and click **Delete**.
5. Select an Intelligent Capture Server from the list and click **Settings** to view the server settings and parameters.

Note: Viewing and editing server settings is only available in Intelligent Capture Administrator 7.5 and later.

Related Topics

"Adding and Connecting Intelligent Capture Servers" on page 116

"Activating Intelligent Capture Servers" on page 117

"Intelligent Capture Permissions List" on page 381

9.1.2 Adding and Connecting Intelligent Capture Servers

Intelligent Capture Servers must be added to the system through Intelligent Capture Administrator. Intelligent Capture Servers that are successfully added and then activated can be monitored using Intelligent Capture Administrator.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To add and connect Intelligent Capture Servers:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Servers**. The **Servers** pane displays the list of all registered Intelligent Capture Servers in the system.
3. Click **Add**. The **Add Server** window displays.
4. Specify the connection information of the Intelligent Capture Server in the **Server address** field. This is the *IP* address or the *FQDN* (Fully Qualified Domain Name) of the Intelligent Capture Server.
5. Set the **Service name** of the Intelligent Capture Server.
6. Specify the**TCP/IP port** of the Intelligent Capture Server.
7. Click **OK**. The Intelligent Capture Server is added to the system.

   You can now activate the Intelligent Capture Server and then install license codes on the activated Intelligent Capture Server.

Related Topics

"Centralized Settings Configuration" on page 100

"Activating Intelligent Capture Servers" on page 117

"Systems" on page 274

"Servers" on page 275

"Intelligent Capture Permissions List" on page 381

9.1.3 Setting Intelligent Capture Server Protocols

1. Select one of the following:
   - For a standalone server:

     Systems > **Servers** > <*server_name*> > **Server Settings**
   - For ScaleServer group:

     Systems > **ScaleServer Groups** > <*ScaleServer_name*> > **ScaleServer Group - <***name***> Settings**
2. Specify the following properties:

Table 9-1: Server Communications

TCP/IP protocol	**TCP/IP** and **Port**	Specify that the Intelligent Capture Server is to use the TCP/IP protocol and the TCP/IP port number.
	IPv4 and **IPv4 Address**	Select for the Intelligent Capture Server to use IPv4 and specify its address.
	IPv6 and **IPv6 Address**	Select for the Intelligent Capture Server to use IPv6 and specify its address.
HTTP/HTTPS protocol	**HTTP(S)** and **Server host URI**	Select for the Intelligent Capture Server to use the HTTP/HTTPS protocol and specify its URI.

9.1.4 Activating Intelligent Capture Servers

Intelligent Capture Server that are added to Intelligent Capture Administrator have to be activated to enable batch processing tasks. In a keyless environment, a server activation requires an activation file (*CAF*) and an activation code. The activation file (*CAF*) and the license file (*LIC*) are provided to you. Contact OpenText Global Technical Services at My Support (https://support.opentext.com) to request the activation code. The sequence for activating and licensing an Intelligent Capture Server is:

1. Install the activation file.
2. Request the activation code.
3. Activate the Intelligent Capture Server with the activation code.
4. Install the license file.

If you do not activate the *CAF* file immediately:

1. Install the activation file.

2. From the Windows Services application, stop and restart the Intelligent Capture Server service.
3. Install the license file.
4. Request the activation code.
5. Activate the Intelligent Capture Server with the activation code within the initial grace period.

Related Topics

"Adding and Connecting Intelligent Capture Servers" on page 116

"Importing License Codes from a License File" on page 124

"Intelligent Capture Permissions List" on page 381

Installing the CAF File

The activation file (*CAF*) enables you to use an Intelligent Capture system for an initial grace period.

To install the *CAF* file:

1. In the **Intelligent Capture Administrator** window, select **Licensing / Security** from the navigation panel. The **Licensing / Security** pane displays.
2. Click **View Server Activations** from the **Licensing** pane. The **Server Activations** pane displays the list of Intelligent Capture Servers added to Intelligent Capture Administrator and their activation status.
3. Select the Intelligent Capture Server to activate.
4. In the **Install activation file** field, browse to or type the path of the *CAF* file that contains the Intelligent Capture Server activation information and press **ENTER**. The *CAF* file updates the server information with:
   - **Server ID**: Lists the server ID.
   - **State**: The state is listed as **Initial grace period**.
   - **File**: The status of the *CAF* file.
   - **Profile ID**: A unique alphanumeric code that identifies the server machine.
   - **Grace Period**: The initial grace period ends on this date.
5. Make a note of the Server ID and Profile ID for the activation process.

Requesting an Activation Code

You require an activation code if you are using a software security key (*CAF* file).

After installing the *CAF* file on the Intelligent Capture Server, you can activate this server by using an activation code.

To request the activation code, contact OpenText Global Technical Services at My Support (https://support.opentext.com). Provide the server's **Server ID** and **Profile ID** obtained during the *CAF* file installation.

Activating an Intelligent Capture Server

After receiving the activation code, follow these steps to activate the Intelligent Capture Sever that uses a software security key.

To activate an Intelligent Capture Server:

1. In the **Intelligent Capture Administrator** window, select **Licensing / Security** from the navigation panel. The **Licensing / Security** pane displays.
2. Click **View Server Activations**. The **Server Activations** pane displays the list of Intelligent Capture Servers added to Intelligent Capture Administrator and their activation status.
3. Right-click the server to be activated in the **Server Activations** pane and select **Activate**.
4. In the window that appears, type the activation code in the **Activation Key** field.
5. Click **OK**. The **Server Activations** pane displays the updated status of the activated Intelligent Capture Server.
6. Add license codes to the activated Intelligent Capture Server.

9.1.5 Connecting and Disconnecting Intelligent Capture Servers

Intelligent Capture Servers in the system can be connected or disconnected as required. Connected servers can be monitored.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To connect or disconnect Intelligent Capture Servers:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Servers**. The **Servers** pane displays the list of Intelligent Capture Servers in the system. The **Connected** column displays a selected check box for those Intelligent Capture Servers that are connected. A cleared check box indicates that the Intelligent Capture Server is disconnected.
3. Select the Intelligent Capture Servers you want to connect or disconnect, right-click and select **Connect** or **Disconnect**.

9.1.6 Increasing the Shutdown Period for the Intelligent Capture Server Service

Typically, the Intelligent Capture server service shuts down within 30 seconds. However, depending on the load on the server, it may take 20 minutes or more. If required, increase the shutdown time to allow the Intelligent Capture server service adequate time to shut down. Note that if the Intelligent Capture server service does not shutdown gracefully, it may result in unsynchronized batches and loss of data. This section provides information on increasing the Intelligent Capture server service shutdown period for supported operating systems.

To understand the issues of shutting down the Intelligent Capture server in a clustered environment, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

The Intelligent Capture Server installer sets the `PreshutdownTimeout` registry key for Intelligent Capture server service to 20 minutes. This configuration allows Intelligent Capture server up to 20 minutes to shut down gracefully. If the Intelligent Capture server service requires more than 20 minutes to shut down, increase the shutdown period using the procedure described in this section.

To increase the Intelligent Capture server service shutdown time:

1. Log in to the Intelligent Capture server machine as a member of the Windows **Administrators** group.
2. Stop all instances of the Intelligent Capture server service.
3. Open a command prompt window on the Intelligent Capture server machine.
4. Type the following command line:

   `ias64.exe -repair -s <servicename> -t <timeout>`

   where:

   - `servicename` is the name of the service that runs the Intelligent Capture server (default: InputAccel). This is the true name of the Intelligent Capture server service and not its display name.
   - `timeout` is a numeric value, representing the maximum time allowed, in minutes, for the Intelligent Capture server service to shut down.

   Example: `ias64 -repair -s InputAccel -t 25`
5. Start the Intelligent Capture server service.

9.1.7 Viewing Information on an Intelligent Capture Server

You can view the list of batches, departments, modules, and ScaleServer groups associated with a specific Intelligent Capture Server.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view information on an Intelligent Capture Server:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Servers**. The **Servers** pane displays the list of Intelligent Capture Servers in the system.
3. Select an Intelligent Capture Server from the list, right-click and select from the following options in the **View Selected** menu:
   - **Batches**: Displays the **Batches from Server** window and lists all batches on the selected server(s).
   - **Processes**: Displays the **Processes** pane and lists all processes on the selected server.
   - **Departments**: Displays the **Departments** pane and lists all departments on the selected server.
   - **Modules**: Displays the **Modules** pane and lists all modules running on the selected server.
   - **ScaleServer Groups**: Displays the **ScaleServer Group** pane and lists all ScaleServer groups attached to this server.
   - **Licenses**: Displays the **License Codes** pane and lists all licenses for the selected server.

Related Topics

"Adding and Connecting Intelligent Capture Servers" on page 116

"Activating Intelligent Capture Servers" on page 117

"Viewing the List of Intelligent Capture Servers" on page 115

"Intelligent Capture Permissions List" on page 381

9.2 Managing Intelligent Capture Licenses

Licenses regulate how the software is used in an Intelligent Capture installation. Licensing works by installing a set of license codes on the Intelligent Capture Server. Each license code specifies a single client module and regulates how many copies of the client module can connect to the Intelligent Capture Server at a time, how many pages the module is allowed to process, how long the license is allowed to work, and what extra features are enabled. For more information on Intelligent Capture licenses and how they work, see Understanding License Types.

9.2.1 Viewing License Codes Installed on the System

You can view the list of license codes installed on the Intelligent Capture Servers in the system.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view license codes installed on the system:

1. Log in to the Intelligent Capture Administrator with administrative permissions. The **Intelligent Capture Administrator** window displays.
2. Select **Licensing / Security** from the navigation panel. The **Licensing / Security** pane displays.
3. In the **Licensing** pane, click **View License Codes**. The **License Codes** pane displays the license codes added to the system.

Related Topics

"Centralized Licensing" on page 101

"Importing License Codes from a License File" on page 124

"Adding License Codes Manually" on page 125

"Viewing or Modifying License Code Settings" on page 125

"Viewing License Codes by Module" on page 123

"Intelligent Capture Permissions List" on page 381

9.2.2 Viewing License Codes by Module

The **Module Licenses** pane displays a list of licensed modules on each Intelligent Capture Server.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view license codes sorted by module

1. In the **Intelligent Capture Administrator** window, select **Licensing / Security** from the navigation panel. The **Licensing / Security** pane displays.
2. In the **Licensing** area, click **View Module Licenses**. The **Module Licenses** pane displays a list of licensed modules on each Intelligent Capture Server.

Related Topics

"Centralized Licensing" on page 101

"Importing License Codes from a License File" on page 124

"Adding License Codes Manually" on page 125

"Viewing or Modifying License Code Settings" on page 125

"Viewing License Codes Installed on the System" on page 122

"Intelligent Capture Permissions List" on page 381

9.2.3 Viewing Page Count Usage

The **Page Count Report** pane displays the daily page count usage per license for each Intelligent Capture Server.

To view page count usage:

1. Select **Licensing / Security** > **View Page Count Report**.

   Note: On the **Page Count Report** page, you can also click **Create Audit File** to create an audit file for technical services use only.

2. Select a server and click **View Usage**.

   The number of pages that have been used for each license on each day for the past 15 months (at the most) is displayed.

   On the **Page Count Usage** page, you can click **Export to CSV** to create a CSV file with this information.

   For more information, see "Page Count Report" on page 292.

9.2.4 Importing License Codes from a License File

The Intelligent Capture product package contains license codes in the form of a text file named `ServerID.lic`, where <*ServerID*> is the Intelligent Capture Server identification number stored in the activation file (*CAF* file).

License codes must be added to the system, either by importing the license file or by added them manually. To ensure proper licensing, it is recommended that licenses are imported from the license file when running Intelligent Capture Administrator for the first time.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To add license codes from a license file:

1. In the **Intelligent Capture Administrator** window, select **Licensing / Security** from the navigation panel. The **Licensing / Security** pane displays.
2. Under **Licensing** click **View License Codes**. The **License Codes** pane displays the license codes added to the system.
3. Click **Import License**. The **Import License Code from a File** pane displays.
4. Enter the path to the license file (*LIC*) in the **Select the license file to be installed** field or click **Browse** to select the license file.
5. Click **OK**. The licenses from the license file are added to the Intelligent Capture Server. The license codes in the license file are displayed in the **Licenses contained in the file** table.

Notes

- A validation message displays if the license file fails to load.
- When you upgrade from an Intelligent Capture Server license to an Advanced Recognition license, you must restart Intelligent Capture Designer.

  When you install a new license file that specifies new licenses and a new server ID, you must restart all servers in the ScaleServer group.

Related Topics

"Centralized Licensing" on page 101

"Adding License Codes Manually" on page 125

"Viewing or Modifying License Code Settings" on page 125

"Intelligent Capture Permissions List" on page 381

9.2.5 Adding License Codes Manually

License codes can be added manually using the **License Code Settings** pane.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To add license codes manually:

1. In the **Intelligent Capture Administrator** window, select **Licensing / Security** from the navigation panel. The **Licensing / Security** pane displays.
2. Under **Licensing** click **View License Codes**. The **License Codes** pane displays the license codes added to the system.
3. Click **Add**. The **Add License Code** pane displays.
4. Provide the license code settings.
5. Click **OK**. The license code is added on the selected Intelligent Capture Server.

Notes

- A validation message displays if the license code fails to add to the system.
- The information added to the pane must match the specified license code or the license will fail and not enable any functionality.

Related Topics

"Centralized Licensing" on page 101

"Importing License Codes from a License File" on page 124

"Viewing or Modifying License Code Settings" on page 125

"Intelligent Capture Permissions List" on page 381

9.2.6 Viewing or Modifying License Code Settings

You can view or modify license code information.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view or modify license code information:

1. In the **Intelligent Capture Administrator** window, select **Licensing / Security** from the navigation panel. The **Licensing / Security** pane displays.
2. Under **Licensing** click **View License Codes**. The **License Codes** pane displays the license codes added to the system.

3. Select a license and click **Settings**. The **License Code Settings** pane displays the license settings.
4. Modify the settings as needed.
5. Click **OK**. The license code information is updated on the Intelligent Capture Server.

Notes

- A validation message displays if there is failure in modifying the license code settings.
- When you upgrade from an Intelligent Capture Server license to an Advanced Recognition license, you must restart Intelligent Capture Designer.

Related Topics

"Centralized Licensing" on page 101

"Importing License Codes from a License File" on page 124

"Adding License Codes Manually" on page 125

"Intelligent Capture Permissions List" on page 381

9.3 Managing ScaleServer Groups

The Intelligent Capture Administrator module allows you to configure a ScaleServer group. A ScaleServer group is a group of two or more Intelligent Capture Servers that are licensed and configured to operate together in a single information capture system. Information about ScaleServer technology, their use and benefits, can be found in "Understanding ScaleServer Technology" on page 51.

The following topics describe how to configure a ScaleServer group:

9.3.1 Viewing ScaleServer Groups

ScaleServer groups registered in the system are listed in the **ScaleServer Group** pane.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view the list of ScaleServer groups registered in the system:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. In the **Servers** area, click the **View ScaleServer Groups**. The **ScaleServer Groups** pane displays all the ScaleServer groups added to the system.

3. Click **Add** to add a new ScaleServer group.
4. Select a ScaleServer group from the table and click **Settings** to view or modify the ScaleServer group settings.
5. Select a ScaleServer group from the table and click **Delete** to remove a ScaleServer group from the system.

Note: When an Intelligent Capture Server is removed from a ScaleServer group, the client modules connected to that Intelligent Capture Server will require approximately two minutes to disconnect from the Intelligent Capture Server.

Caution

Do not attempt to remove an Intelligent Capture Server from a ScaleServer group by deleting its license codes or changing its feature codes. Doing so will not remove the server from the group, but will result in a group that no longer functions correctly.

Related Topics

"Adding and Connecting ScaleServer Groups" on page 128

"Viewing or Modifying ScaleServer Settings" on page 130

"Listing Intelligent Capture Servers for each ScaleServer Group" on page 127

"Viewing License Codes Installed on the System" on page 122

"Intelligent Capture Permissions List" on page 381

9.3.2 Listing Intelligent Capture Servers for each ScaleServer Group

You can view the Intelligent Capture Servers attached to each ScaleServer group.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view the list of connected Intelligent Capture Servers for each ScaleServer group:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. In the **Servers** area, click the **View ScaleServer Groups**. The **ScaleServer Groups** pane displays all the ScaleServer groups added to the system.
3. Select a ScaleServer group from the **Registered ScaleServer groups** table. The **Attached servers for the selected ScaleServer groups** table displays the list of connected Intelligent Capture Servers for the selected ScaleServer group.

Related Topics

"Adding and Connecting ScaleServer Groups" on page 128

"Viewing or Modifying ScaleServer Settings" on page 130

"Viewing ScaleServer Groups" on page 126

"Intelligent Capture Permissions List" on page 381

9.3.3 Adding and Connecting ScaleServer Groups

ScaleServer groups can be created with existing Intelligent Capture Servers in the system.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To add and connect ScaleServer groups:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. In the **Servers** area, click the **View ScaleServer Groups**. The **ScaleServer Groups** pane displays all the ScaleServer groups added to the system.
3. Click **Add**. The **Add ScaleServer Group** window displays.
4. Specify a unique **Name** for the ScaleServer group. The name can be a maximum of 50 characters. The names of the current ScaleServer groups are listed in the **Existing Names** list box.
5. The **Available Servers** list box displays the list of Intelligent Capture Servers in the system. Select the Intelligent Capture Servers to add to the ScaleServer group and click **>**. To add all the Intelligent Capture Servers from the **Available Servers** list box, click **>>**. The selected Intelligent Capture Servers are displayed in the **Attached Servers** list box.
6. To remove Intelligent Capture Servers from the ScaleServer group, select the servers from the **Attached Servers** list box and click **<**.
7. You can turn the following kinds of encryption on or off in the **Server Security** section.

   - **Encrypt data while transferring between server and modules**: encrypts data between the Intelligent Capture Server and client modules.
   - **Encrypt staging files on Intelligent Capture Server :** encrypts the batch staging files that temporarily reside on the Intelligent Capture Server .

   Specify the data encryption to use for both client-server and staging files on the Intelligent Capture Server in the ScaleServer group.

Crypto Provider	The cryptographic provider to use. Only providers that are installed on the Intelligent Capture Administrator machine are displayed. The selected provider must also be installed on the servers and client machines.
Algorithm	The symmetric-key algorithm to use.

8. Click **OK**. A ScaleServer group is created with the specified Intelligent Capture Servers.

   Note: The **System.ServerRead** permission is required for any client module attempting to connect to a ScaleServer group. This is because the Intelligent Capture Server must access the configuration information that determines the servers that are part of the group.

9. The ScaleServer group's data encryption settings specify the settings for all servers in the group. If a server's data encryption setting is different from the ScaleServer group's, then the server must be restarted to reset their settings to the ScaleServer group's.

   Servers that need to be restarted are identified by the  icon in the **Systems** > **ScaleServer Groups** > <*ScaleServer_name*> or the **Systems** > **Servers** panes.

   Notes

   - If the Intelligent Capture Server cannot be started using the selected encryption method, then start the server from the command line by using the `-safe` parameter. You can then use Intelligent Capture Administrator to connect to the server. No other connections are allowed.
   - If you are simply resetting a server's data encryption to its previous setting and have not already restarted it, then you do not need to restart it now.

Related Topics

"Viewing or Modifying ScaleServer Settings" on page 130

"Viewing ScaleServer Groups" on page 126

"Listing Intelligent Capture Servers for each ScaleServer Group" on page 127

"Managing Client-Server and Batch Staging File Data Encryption" on page 139

"Intelligent Capture Permissions List" on page 381

9.3.4 Viewing or Modifying ScaleServer Settings

You can view and modify the settings of a ScaleServer group.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view or modify ScaleServer settings:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. In the **Servers** area, click the **View ScaleServer Groups**. The **ScaleServer Groups** pane displays all the ScaleServer groups added to the system.
3. Select a ScaleServer group from the table and click **Settings**. The **ScaleServer Group Settings** window displays the ScaleServer group settings.
4. Modify the ScaleServer group settings as needed and click **OK**.

Related Topics

"Adding and Connecting ScaleServer Groups" on page 128

"Viewing ScaleServer Groups" on page 126

"Listing Intelligent Capture Servers for each ScaleServer Group" on page 127

"Intelligent Capture Permissions List" on page 381

9.4 Managing Security

Administrators use Intelligent Capture Administrator to configure what a user is allowed to do in Intelligent Capture. After initial installation, administrators have complete permissions and can configure the following security features:

- Roles and permissions for individuals responsible for performing tasks
- Network protocols between client modules and the Intelligent Capture Server
- Network encryption between client modules and the Intelligent Capture Server
- Encryption of batch staging files
- Disabling image caching on ScanPlus and RescanPlus.

Intelligent Capture security is managed through Intelligent Capture Administrator roles and Access Control Lists (*ACL*s). In general terms, role permissions are for actions and *ACL*s are for things. Users or groups can use both, but generally speaking, roles are at the top level of securing the system and *ACL*s are for finer-grain control.

- Roles contain two important traits: permissions, and users or groups. A role will have a defined set of permissions that are appropriate for members of that role. Each member (user or group) of that role will inherit the assigned permissions.
- *ACL*s define access for users or groups to modules, batches, departments, or processes. *ACL*s enable administrators control access to these items, separate from role definitions.

Intelligent Capture users and groups are made available to Intelligent Capture Administrator as Windows defined users or groups. Some of the security in Intelligent Capture is provided by Windows. Administrators can take full advantage of built-in Windows security mechanisms, such as *NTFS* file permissions. It is important to note that even if users or groups have permissions to perform tasks in Intelligent Capture, these users or groups may also require specific rights in Windows. For example, a user may have permission to run modules and processes in Intelligent Capture, but if these operations require writing to a folder where the user does not have Windows rights, a conflict may arise.

Related Topics

"Defining Roles, Role Members, and Role Permissions" on page 132

"Adding Users and Groups to Roles" on page 142

"Add Roles and Role Settings" on page 266

"Viewing Roles" on page 131

"Predefined Roles" on page 386

9.4.1 Configuring Roles

There are a number of roles that can be defined in Intelligent Capture Administrator, including administrators, designers, or end users. The installation default is to create an Administrator's role which grants all permissions to the Intelligent Capture system Administrators can configure roles and assign permissions to individuals responsible for performing tasks in Intelligent Capture Administrator.

9.4.1.1 Viewing Roles

Roles define the activities that individuals or groups perform from within Intelligent Capture Administrator as well as Intelligent Capture. You can view, add or modify `Roles` from within the **Licensing / Security** pane.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view assigned Intelligent Capture roles:

1. In the **Intelligent Capture Administrator** window, select **Licensing / Security** from the navigation panel.

2. Under **Security**, select **View Roles** to display the **Roles** pane, listing all the currently defined roles.
3. To view the details assigned to a particular role, select the role and click **Settings**.

Related Topics

"Managing Security" on page 130

"Defining Roles, Role Members, and Role Permissions" on page 132

"Adding Users and Groups to Roles" on page 142

"Configuring Roles" on page 131

"Add Roles and Role Settings" on page 266

"Intelligent Capture Permissions List" on page 381

"Predefined Roles" on page 386

9.4.1.2 Defining Roles, Role Members, and Role Permissions

Roles define the activities that individuals or groups perform from within Intelligent Capture Administrator as well as within all Intelligent Capture client modules. Role definitions include the members assigned to the roles as well as the permissions assigned to the role. Roles are viewed, added or modified from within the **Licensing / Security** pane.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To define roles, role members, and role permissions:

1. In the **Intelligent Capture Administrator** window, select **Licensing/Security** from the navigation panel.
2. Under **Security**, select **View Roles** to display the **Roles** pane, listing all the currently defined roles.
3. If you are modifying an existing role, select the role from the list, and click **Settings** to display the **Role Settings** pane.
4. Use the arrow buttons to move selected permissions between the **Selected Permissions** (those assigned to the role) and **Available Permissions** fields. The **Permission Description** field indicates what actions the selected permissions allow.
5. Use the arrow buttons to move selected members between the **Selected Members** (those assigned to the role) and **Available Members** fields. If necessary, click **Find Member** button to make unlisted members available from the **Select User or Group** window.

6. To define a new role, click **Add** in the **Roles** pane and the **Add Role** pane displays. Type a **Name** and **Definition** for the role.

7. Click **OK** to save the settings. Close Intelligent Capture Administrator and open it again for the settings to take effect.

Related Topics

"Managing Security" on page 130

"Adding Users and Groups to Roles" on page 142

"Defining Roles, Role Members, and Role Permissions" on page 132

"Configuring Roles" on page 131

"Add Roles and Role Settings" on page 266

"Viewing Roles" on page 131

"Intelligent Capture Permissions List" on page 381

"Predefined Roles" on page 386

9.4.1.3 Searching for Users or Groups

Intelligent Capture users and groups are made available to Intelligent Capture Administrator as Windows defined users or groups. Searching for users and groups enables selection of users or groups for use in, for example, assigning roles. The **Select Users or Groups** window provides filters for finding the specific individuals or groups based on domain and name.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To search for users or groups:

1. When you are in a window displaying Available Users or Available Groups, click the appropriate button to add or find users or groups. The **Select Users or Groups** window displays.

2. Use the check boxes to activate the filters for domain, user name, or both and to limit the number of results listed.

   - For **Use domain or workstation filter**, type the name for the domain or workstation.
   - For **Use name filter**, type in the name or names. You can use .NET regular expression syntax to enhance search capabilities.
   - For **Maximum number of results**, type or use the scroll arrows to restrict the number of results displayed.

- For **Include built-in security principals**, select the check box to include the security principals of the operating system.

3. Click **Search** and the **Result List** is populated.
4. Select the user or group, and click **OK** to add them in the window from step 1.

Related Topics

"Managing Security" on page 130

"Defining Roles, Role Members, and Role Permissions" on page 132

"Viewing Roles" on page 131

"Intelligent Capture Permissions List" on page 381

9.4.2 Understanding Permissions

Within Intelligent Capture Administrator, administrators have the ability to define roles, assign users or groups to those roles, and grant permissions to those roles. The permissions granted to the roles will control the ability for users to work in the Intelligent Capture environment, and must be carefully thought out so that, during setup or production, users have the appropriate permissions to do their work. For example, a user might have permission to set up a module, but without access to the server (server logon permission), module settings cannot be saved. This topic includes a number of examples and permission types to guide administrators when creating roles and assigning users. For a complete list of permissions, see "Intelligent Capture Permissions List" on page 381.

Notes

- Role permissions are cumulative. If permission is defined in one role for a member or group and another role has a different set of permissions with the same member or group, all permissions apply to both roles with the same member or group.
- Some database permissions are not controlled from Intelligent Capture Administrator. Insufficient database access rights for a user may block some database operations specifically related to reports, logs, and purges. For more information on database permissions, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

The following list includes those permissions used during creation of production roles. For examples of grouping or permissions for types of roles, see "Permissions for Running in Production Mode" on page 135. For a complete list of permissions, see "Intelligent Capture Permissions List" on page 381.

Basic Module Permissions

- Server.Login: Login to the Intelligent Capture Server.
- System.BatchModify: Write batch data.

- System.BatchRead: Read batch data.
- Server.Read.Module.Data: Read module data (optional, but useful for preserving and recalling module settings such as window size, and position).
- Server.Write.Module.Data: Write module data (optional, but useful for preserving and recalling module settings such as window size and position).

Module Login Permissions (only required for these modules):

- DocumentumAdvancedExport.Login
- ImageDivider.Login
- RescanPlus.Login
- ScanPlus.Login
- WebServices.WSInput.Login
- WebServices.WSOutput.Login

Related Topics

"Managing Security" on page 130

"Defining Roles, Role Members, and Role Permissions" on page 132

"Viewing Roles" on page 131

"Intelligent Capture Permissions List" on page 381

"Predefined Roles" on page 386

9.4.2.1 Permissions for Running in Production Mode

The Intelligent Capture Server expects certain permissions to run the module in production. Many or all of these permissions may need to be granted to users for production.

Intelligent Capture Server Permissions

Depending on the level of responsibility users need to have in the working environment, consider adding these permissions to the appropriate roles:

- Server.Login: Log in to the Intelligent Capture Server.
- System.BatchModify: Write batch data.
- System.BatchRead: Read batch data.
- System.ProcessRead: Read process data.
- System.ProcessModify: Change process data (especially if using naming schema tags).
- System.SecurityRead: Read *ACL* security data.

- System.SecurityModify: Write *ACL* security data. This permission is required to make any security changes to the roles, process, batch, and department ACLs.
- System.ServerRead: Read non-module server data (such as registry values)
- Server.Read.Module.Data: Read module data
- Server.Write.Module.Data: Write module data
- Server.Create.Batch: Create or modify a batch

Permissions Necessary for a User to Run a module in Production Mode

The following permission groupings are provided as a guide to administrators when creating roles and assigning users and permissions. For a complete list of permissions, see "Intelligent Capture Permissions List" on page 381.

- Server.Login: Log in to the Intelligent Capture Server
- System.BatchModify: Write batch data.
- System.BatchRead: Read batch data.
- System.ServerRead: Read non-module server data (such as registry values).
- One or more new module login permissions.
- New module specific permissions.

Example Permissions for a User to run Web Services Input in Production Mode:

- Server.Login: Log in to the Intelligent Capture Server.
- Server.Read.Module.Data: Read module data.
- Server.Write.Module.Data: Write module data.
- Server.Create.Batch: Create or modify a new batch.
- System.BatchModify: Write batch data.
- System.BatchRead: Read batch data.
- System.ServerRead: Read non-module server data (such as registry values).
- System.ProcessRead: Read process data.
- System.ProcessModify: Change process data (if using naming schema tags).
- System.SecurityRead: Read *ACL* security data (necessary to create batches for Web Services Input if used as the first process step).
- System.SecurityModify: Write *ACL* security data. This permission is required to make any security changes to the roles, process, batch, and department ACLs.

Example Permissions for an Operator to Run ScanPlus and RescanPlus in Production Mode:

- ScanPlus.ChangeScanConfig: Change the scanning configuration defined in ScanPlus
- ScanPlus.Login: Log in to ScanPlus.
- ScanPlus.ReorderImages: Add, move, and delete images in ScanPlus.
- ScanPlus.SetupInstance: Set up a ScanPlus step.
- RescanPlus.ChangeScanConfig: Change the scanning configuration in RescanPlus.
- RescanPlus.Login: Log in to RescanPlus.
- RescanPlus.ReorderImages: Add, move, and delete images in RescanPlus.
- RescanPlus.SetupInstance: Set up a RescanPlus step.
- RescanPlus.ShowBatchesWithoutTasks: Displays the **Show only batches with ready tasks** check box for the RescanPlus operator.
- Server.Create.Batch: Create or modify a new batch.
- Server.Login: Log in to the Intelligent Capture Server.
- Server.Read.Module.Data: Read module data.
- Server.Write.Module.Data: Write module data.
- System.BatchModify: Write batch data.
- System.BatchRead: Read batch data.
- System.ProcessRead: Read process data.
- System.ServerRead: Read non-module server data (such as registry values).

Related Topics

"Managing Security" on page 130

"Defining Roles, Role Members, and Role Permissions" on page 132

"Viewing Roles" on page 131

"Intelligent Capture Permissions List" on page 381

"Predefined Roles" on page 386

9.4.3 Configuring the Access Control List

Access Control Lists (*ACL*) allow definition of user or group access permission for modules, batches, departments and processes. The **Access Control List** window is displayed from any pane displaying modules, batches, departments and processes. The **Access Control List** window can remain open while browsing in Intelligent Capture Administrator.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

9.4.3.1 Viewing and Defining Access Control

Defining access control sets the permissions for a user or group. These permissions are specified for modules, batches, departments or processes.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To define access control:

1. When working in any **Intelligent Capture Administrator** window pane displaying modules, batches, departments or processes, select one of the items and right-click to bring up the context menu.
2. Select **View Selected** and select **ACLs** from the submenu. The **Access Control List** window for the selected components displays. The **ACL for the following <objects>** field displays a list of the selected components.
3. The **Select a user or group to view or modify their permissions** table displays all users or groups for which ACLs have already been defined for the selected object.
    a. Click **Delete** to eliminate a selected user or group from the list to remove them from the table. This will remove their access to the module, batch, department or process.
    b. Click the **Add** button to include additional users or groups available from the **Select Users or Groups** window.
4. In the **Select a user or group to view or modify their permissions** table, select a user or group.
5. Under **Permissions for selected users or groups**, select the appropriate options. If no permissions are selected for a user or group, that user or group will be automatically removed from the list when the **Access Control List** window is closed.
6. When completed with the **Access Control Level** settings, you can click **Apply** for the settings to take effect for the selected user or group and leave the window open, or click **OK** to apply the settings and close the window.

Related Topics

"Managing Security" on page 130

"Viewing and Defining Access Control for Departments" on page 148

"Viewing and Defining Access Control for Batches" on page 172

"Viewing and Defining Access Control for a Process" on page 160

"Intelligent Capture Permissions List" on page 381

9.4.4 Disabling Image Caching for ScanPlus and RescanPlus

For security reasons, you might not want to cache images on ScanPlus orRescanPlus machines. You can configure whether images downloaded from Intelligent Capture Server or large imported or scanned images are to be cached locally on ScanPlus orRescanPlus machines. Images are downloaded from Intelligent Capture Server and cached locally when they are edited or displayed in ScanPlus and RescanPlus.

If image caching is disabled, then the time it takes to retrieve the same image from the Intelligent Capture Server might increase. In addition, the maximum size of scanned or imported images that can be processed decreases.

1. Select **Licensing / Security** > **Security Options**.
2. Check **Disable image cache on ScanPlus and RescanPlus**.

9.4.5 Managing Client-Server and Batch Staging File Data Encryption

You can encrypt data using various cryptographic providers, including the standard providers shipped with Windows, you can encrypt the following kinds of data:

- Data transferred between the Intelligent Capture Server and client modules.
- Temporary batch staging files.

To turn on logging for the file security events, turn on the **AuditAdminConsoleSECEvents** rule.

To set up encryption:

1. Select one of the following:
   - For a standalone server:

     Systems > **Servers** > <*server_name*> > **Server Settings**
   - For ScaleServer group:

     Systems > **ScaleServer Groups** > <*ScaleServer_name*> > **ScaleServer Group - <***name***> Settings**

Note: File Security can only be applied to individual servers—not a **ScaleServer Group**.

2. Set the following properties:

Table 9-2: Network Security

Encrypt data while transferring between server and modules	Select to encrypt data while it is being transferred between the Intelligent Capture Server and client modules.
Crypto Provider	The cryptographic provider to use. Only providers that are installed on the Intelligent Capture Administrator machine are displayed. The selected provider must also be installed on the server and client machines. **Note:** Only Crypto API providers are supported.
Algorithm	The symmetric-key algorithm to use.

Table 9-3: File Security

Encrypt staging files on Intelligent Capture Server	Select to encrypt the batch staging files that temporarily reside on the Intelligent Capture Server.
Crypto Provider	The cryptographic provider to use. Only providers that are installed on the Intelligent Capture Servermachine are displayed. **Note:** Only CryptoNG API providers are supported.
Algorithm	The symmetric-key algorithm to use.
Key length	The key length.
Key protection rule	Rule used by Windows DPAPI to secure the encryption key.

Certificate	A security certificate with a private key that is installed in the administrator's private certificate storage on Intelligent Capture Server machine. The security certificate provides additional protection for the encryption key. It is recommended that you keep the security certificate installed on Intelligent Capture Server until all batches with encryption keys that are protected with this certificate have completed. The Intelligent Capture Server processes batches with the encryption keys protected by the certificate until the certificate (even if it is expired) is installed on the Intelligent Capture Server . Removing the certificate from the Intelligent Capture Server stops further processing of such batches; thus, the Intelligent Capture Server would not load such batches and log an error message with the missing certificate hash in the server log. You can check that removing a certificate would affect some batches by comparing the batch creation date against the date of either the file security enabling (log code 477) or file security changing (log code 479) events.

3. Restart the servers.

Notes

- If the Intelligent Capture Server cannot be started using the selected encryption method, then start the server from the command line by using the `-safe` parameter. You can then use Intelligent Capture Administrator to connect to the server. No other connections are allowed.
- The ScaleServer group's network security data encryption settings specify the settings for all servers in the group. If a server's network security data encryption setting is different from the ScaleServer group's, then the server must be restarted to reset their settings to the ScaleServer group's.
- Servers that need to be restarted are identified by the  icon in the **Systems** > **ScaleServer Groups** > <*ScaleServer_name*> or the **Systems** > **Servers** panes.

- If you are simply resetting a server's data encryption to its previous settings and have not already restarted it, then you do not need to restart it now.

9.5 Managing Users and Groups

Users and groups must be defined under the **User Profile** section of Windows to be recognized and assigned to roles in Intelligent Capture. Assigning users or groups to roles is accomplished as a security task in Intelligent Capture Administrator. Intelligent Capture manages permissions through role definitions or using Access Control Lists (ACL). Assigning Windows users or groups to a role enables the assignment of Intelligent Capture permissions to those users or groups.

Related Topics

"Managing Security" on page 130

"Defining Roles, Role Members, and Role Permissions" on page 132

"Configuring Roles" on page 131

"Add Roles and Role Settings" on page 266

"Viewing Roles" on page 131

"Predefined Roles" on page 386

9.5.1 Adding Users and Groups to Roles

Windows users and groups can be added to existing roles or new roles, enabling the assignment of Intelligent Capture permissions to those users and groups.

Notes

- To assign users or groups from other domains to Intelligent Capture security roles, Intelligent Capture Administrator must have the permissions necessary to browse the other domains, or the users from the other domain must be added to Windows groups in the domain where the Intelligent Capture system is running.
- Any user who logs into an Intelligent Capture Server must have the "Windows Login" permission on the machine hosting the Intelligent Capture Server.
- Add only domain users or users on the Intelligent Capture Server to IA roles; that is, do not specify the local Windows user accounts on a client module machine because the Intelligent Capture Server would not be able to access them.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To add users or groups to new roles or existing roles:

1. In the **Intelligent Capture Administrator** window, select **Licensing / Security** from the navigation panel.
2. Select **View Roles** under **Security**. The **Roles** pane displays.
3. Select an existing role and click **Settings**, or click **Add** to assign users to a new role that is to be created. The **Role Settings** or **Add Role** pane displays.
4. Users are added as **Members** from the bottom of the **Role Settings** pane. To find a user or group not listed in the **Available Members** or **Selected Members** list, click **Find Member** and the **Select User or Group** window displays.
   a. Filter the search for users or groups by selecting the check boxes for **Use domain or computer filter**, **Use name filter**, or both. Select **Maximum number of results** to limit the number listed.
   b. Select **Include built-in security principals** to include the built in security principals of the operating system.
   c. Click **Search** and the **Results List** is populated with the results of the search. Select the user or group to add and click **OK**. The selections are added to the **Selected Member** list on the **Role Settings** pane.
5. When listed in **Available Members**, add the user to the **Selected Members** list. These users and groups will inherit the specified permissions for the current role.

Replacing Users in a Role (Command-Line)

Use the `iaadminutil.exe` command line utility to replace all user accounts (including groups) in a specific role with new user accounts. By default, `iaadminutil.exe` is located in `C:\Program Files (x86)\InputAccel\Client\binnt`.

Syntax

```
iaadminutil.exe -s <host><[,port]> -u <username> -p <password>
 -set_role_users <role> <userlistfile> -log_file <path>
```

<host><[,port]>	(Required) The name or IP address of the host machine of the Intelligent Capture Server. If the Intelligent Capture Server uses the default port number, then the port number does not need to be specified; otherwise, the port number must be specified.
<username>	(Required) Name of an administrator account on the Intelligent Capture Server.
<password>	(Required) Password for the administrator account on the Intelligent Capture Server.

<role>	(Required) The role for which its user accounts are to be replaced. A role name with spaces in it must be enclosed in quotes.
<userlistfile>	(Required) The path to the text file that specifies the user accounts (including groups) with which to replace the current ones in the role. The format is as follows: • Each user account name must be in the following format: `<[domain|]><username>` `<[domain|]>` is required for non-local users or groups. • Each user account name must be delimited by a comma or line break. **Notes** • To specify domain users, you must be logged in as a domain user. • To specify local users, you must run this utility on the Intelligent Capture Server machine. • Predefined local users and distribution groups are not supported. • Predefined roles that have been localized must be specified with their initial English name; because a new role created in the localized environment does not have an English equivalent name, use the localized name. • Any spaces before or after a user name are considered to be part of the user name. • Invalid user accounts are skipped. • If there are no valid user accounts or the file is empty, then the role is not changed; that is, the role's existing user accounts remain.
<path>	(Optional) Absolute path to a log file. Log entries are appended to an existing log file.

Return Codes

Return Code	Description
0	No errors occurred during processing. **Note:** An empty user accounts file is not considered to be an error.
1	One of the following errors occurred: • No connection to the Intelligent Capture Server • A parameter is not correctly specified • Cannot open the file that contains the user accounts. • Cannot insert user accounts into the database. • Cannot find the role. • Cannot update the role.

Related Topics

"Managing Security" on page 130

"Defining Roles, Role Members, and Role Permissions" on page 132

"Adding Users and Groups to Roles" on page 142

"Configuring Roles" on page 131

"Add Roles and Role Settings" on page 266

"Viewing Roles" on page 131

"Intelligent Capture Permissions List" on page 381

"Predefined Roles" on page 386

9.5.2 Viewing a List of Users or Groups

Viewing a list of available users or groups is accomplished through the **View Roles** section of Intelligent Capture Administrator.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view a list of users or groups:

1. In the **Intelligent Capture Administrator** window, select **Licensing / Security** from the navigation panel.

2. Select **View Roles**. The **Roles** pane displays.
3. Select an existing role and click **Settings**, or click **Add**. The **Role Settings** or **Add Role** pane displays.
4. To view a list of users or groups, click **Find Member** and the **Select User or Group** window displays.
5. Filter the search for users or groups by selecting the check boxes for **Use domain or computer filter**, **Use name filter**, or both. Select **Maximum number of results** to limit the number listed.
6. Select **Include built-in security principals** to include the built in security principals of the operating system.
7. Click **Search** and the **Results List** is populated with the results of the search.

Related Topics

"Managing Security" on page 130

"Defining Roles, Role Members, and Role Permissions" on page 132

"Adding Users and Groups to Roles" on page 142

"Configuring Roles" on page 131

"Add Roles and Role Settings" on page 266

"Viewing Roles" on page 131

"Intelligent Capture Permissions List" on page 381

"Predefined Roles" on page 386

9.6 Managing Departments

Departments control which tasks go to which operators or module instances by routing tasks based on the department specified in the `-department` argument when the module was started. Departments are defined in *IPP*s at either the step level or the task level. Step-level departments route tasks to a particular module step and require that multiple steps of the module be defined in the *IPP*, one step per department. Task-level departments route tasks directly to a module based solely on the department specified when the module was started. In the case of attended modules, tasks can be routed to operators with specific skills, security clearances, or other classification. In the case of unattended modules, tasks can be routed to separate module instances that have been configured to perform different processing operations. By granting or revoking permissions in each department's *ACL*, you can control which users or groups can process a department's tasks, thereby preventing certain users from processing certain classes of tasks.

9.6.1 Viewing the List of Departments

The departments added to **Intelligent Capture Administrator** are listed in the **Departments** pane.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view the list of departments:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Departments**. The **Departments** pane displays the list of departments in the system.

Related Topics

"Adding and Deleting Departments" on page 147

"Viewing and Defining Access Control for Departments" on page 148

"Viewing and Defining Access Control" on page 138

"Intelligent Capture Permissions List" on page 381

9.6.2 Adding and Deleting Departments

The Intelligent Capture Administrator has the ability to add and delete departments, but in most cases departments are added automatically. Departments that are defined for module steps in a process are automatically added when the process is installed on the Intelligent Capture Server. Dynamically-defined step-level and task-level departments are automatically added to the Intelligent Capture Server when the module step in which the departments are assigned processes the first task in a batch based on the process.

Note: If you need to control access to dynamically-defined tasks based on the departments with which they are associated, you can do so without first processing a batch by manually adding the departments in the Intelligent Capture Administrator and then assigning access control to them.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To manually add departments:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Departments**. The **Departments** pane displays the list of departments that have already been added.

3. Click **Add**. The **Add Department** window displays.
4. Enter a new **Department** name. Be sure that you spell the name exactly as it is defined in the process to which it applies.
5. Click **OK**. The new department is added.
6. View the default ACL assigned to the department and change permissions as needed. Grant Execute permission to users who are allowed to process tasks for the department; revoke Execute permission from users who are not allowed to process tasks for the department.
7. Click **Delete** to delete a selected department.

Notes

- The Intelligent Capture Administrator will not delete departments that are in use. You must first remove any batches and processes in which the department is defined.
- When you click **Cancel** in this pane, the pane does not close. To resolve this issue, follow the instructions described in http://support.microsoft.com/kb/2870699.

Caution

Do not delete the default department nor remove permissions for the default department. The default department is used by the Intelligent Capture Server to create new departments.

Related Topics

"Viewing the List of Departments" on page 147

"Viewing and Defining Access Control for Departments" on page 148

"Viewing and Defining Access Control" on page 138.

"Intelligent Capture Permissions List" on page 381

9.6.3 Viewing and Defining Access Control for Departments

Access Control Lists (*ACL*) enable access permission to be defined for modules, batches, departments and processes. The **Access Control List** window for departments is displayed from the **Departments** pane.

Note: Modules, departments, batches, and processes have access permissions that differ from Intelligent Capture Administrator permissions. Access permissions determine which users or groups can access the module, department, batch, or process, while Intelligent Capture Administrator permissions control determine which users can access panes and windows within Intelligent Capture Administrator. An operator without department

Execute permission can run a module for production. However, until Execute department permissions are granted to an operator, tasks routed to a department cannot be processed by a module even though the operator started the module with that department specification. Grant the operator Execute department permissions to route department tasks to that operator's module instance.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view the access control for a department :

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel.
2. Select **View Departments** from the **Systems** pane.
3. In the **Departments** pane, select the department, and right-click. Select **View Selected** and select **ACLs** from the submenu. The **Access Control List** window for the selected department displays.

"Viewing and Defining Access Control" on page 138 provides more information about creating *ACL*s.

Related Topics

"Intelligent Capture Permissions List" on page 381

9.7 Managing Client Modules

Client modules are applications that create and process tasks from batches that are stored on an Intelligent Capture Server. Intelligent Capture Administrator provides several tools for managing client modules, including assigning access control, managing module connections, and granting module permissions.

9.7.1 Viewing Module Connections and Disconnecting Modules

Modules with currently active connections are listed on the **Connections** pane. This gives information about the module, and provides access to additional information on the associated servers, workstations, and so on, through the context menu. Modules can also be disconnected from here.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view all module connections open in the system:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel.

2. Select **View Module Connections** from the **Systems** pane. The **Connections** pane displays with a list of all connections in the system.
3. Use the **Filter** list to limit by module the connections to be displayed.
4. Select a module, and the **Batches using the selected modules** is updated with the appropriate information associated with the module.
5. Right-click a module and select options from the context menu to reveal additional information associated with the module.
6. To disconnect a module from the system, select the module, and click **Disconnect** to close the connection to the selected module. The module connection is reestablished only when the module is restarted.

Related Topics

"Running Unattended Modules as Windows Services" on page 152

"Viewing, Adding, Modifying, and Deleting Modules" on page 150

"Viewing and Defining Access Control for Modules" on page 151

"Connections" on page 285

"Modules" on page 282

"Intelligent Capture Permissions List" on page 381

9.7.2 Viewing, Adding, Modifying, and Deleting Modules

Intelligent Capture Administrator provides a list of all the modules recognized in the system from the **Modules** pane. Selecting a module also displays listings for all batches and processes associated with the selected module.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view module information:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel.
2. Select **View Modules** from the **Systems** pane. The **Modules** pane displays listing all the modules recognized in the system.
3. Use the **Filter** list to limit the modules displayed based on servers.
4. Select a module to update the batches and processes lists to reflect the current selection. Then click **Settings** to display the settings for the selected module.
5. Right-click a module and select options from the **View Selected** menu to view additional information associated with the module.

6. Click **Add** to include a new module in the list. The **Add Module** window enables specification of the following module parameters:

   - **Display Name**: A user-specified name for the module.
   - **MDF Name**: The name of the module's MDF file.
   - **EXE/DLL Name**: The name of the EXE file or DLL file associated with the module.

     Note: Do not include ".exe" or any extension in the EXE/DLL name.

   - **Related to process** check box: Indicates that the module is related to a process.

7. To delete a module, select it from the list and click **Delete**.

Related Topics

"Running Unattended Modules as Windows Services" on page 152

"Viewing Module Connections and Disconnecting Modules" on page 149

"Viewing and Defining Access Control for Modules" on page 151

"Intelligent Capture Permissions List" on page 381

9.7.3 Viewing and Defining Access Control for Modules

Access Control Lists (*ACL*) enable definition of access permission for modules, departments, batches, and processes. The **Access Control List** window for modules is displayed from the **Modules** pane. The **Access Control List** window can remain open while browsing in Intelligent Capture Administrator.

Note: Modules, departments, batches, and processes have access permissions that differ from Intelligent Capture Administrator permissions. Access permissions determine which users or groups can access the module, department, batch, or process, while Intelligent Capture Administrator permissions control determine which users can access panes and windows within Intelligent Capture Administrator.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view the assigned access control for a module:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel.
2. Select **View Modules** from the **Systems** pane.

3. In the **Modules** pane, select the module, and right-click. Select **View Selected** and select **ACLs** from the submenu. The **Access Control List** window for the selected module displays.

For more information on creating access control levels, see "Viewing and Defining Access Control" on page 138.

Related Topics

"Running Unattended Modules as Windows Services" on page 152

"Viewing Module Connections and Disconnecting Modules" on page 149

"Viewing, Adding, Modifying, and Deleting Modules" on page 150

"Intelligent Capture Permissions List" on page 381

9.7.4 Running Unattended Modules as Windows Services

A service is a program that runs without requiring user intervention. Services can be configured to start when the operating system starts and continue running in the background as long as Windows is running. Services optimize the automation of batch processing and enable client/server environments to operate at maximum efficiency. Before a module can run as a service, it must be installed as a service. When installed, additional configuration is accomplished by using the Services extension of the Microsoft Management Console.

Note: Not all modules run as services. "Appendix—Intelligent Capture Client Modules" on page 569 provides a list of modules that can be run as services.

Related Topics

"Viewing Module Connections and Disconnecting Modules" on page 149

"Viewing, Adding, Modifying, and Deleting Modules" on page 150

"Viewing and Defining Access Control for Modules" on page 151

"Connections" on page 285

"Modules" on page 282

9.7.5 Specifying the Session Timeout Duration for Administrator, Completion, and Identification

The **AttendedClientSessionTimeout** value determines the duration that Administrator, Completion, and Identification can be inactive before the current user is logged out. The default value is 600 seconds (10 minutes).

To specify the session timeout duration:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel.
2. In the **Modules** pane, select **InputAccelEditableValues**, right click, select **View Selected**, and click **Values**.

   Note: InputAccelEditableValues is displayed as a module in the **Modules** pane.
3. In the panel on the right, double-click the value in the **Setting** column for **AttendedClientSessionTimeout** and edit the value.

   Tip: The maximum values have no limit.

9.8 Managing Processes

An Intelligent Capture process defines the modules that the Intelligent Capture Server should use to capture images and data, the order in which to use the modules, and what to do with resulting data. The Intelligent Capture Server comes with a number of pre-configured processes. Information about each of these individual processes is provided in *OpenText Intelligent Capture - System Overview (ECPCORE-GCS)*.

Processes must be installed on Intelligent Capture Administrator to create batches based on the process.

9.8.1 Viewing the List of Processes Installed on the System

A list of all processes installed on the system can be displayed in Intelligent Capture Administrator.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view the list of processes installed on the system:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Processes**. The **Processes** pane displays the list of processes installed on the system.

3. To view the processes installed on a specific Intelligent Capture Server, select the server from the **Filter** list box. To view the processes installed on all Intelligent Capture Servers, select **All Servers** from the **Filter** list box.
4. Select a process and the module steps associated with the selected process are displayed in the **Process steps** table.
5. Select a process and click **Settings** to view or modify process settings including renaming the process.

Caution

Do not rename a process used by an unattended module that creates batches (as the first module step in the process).

6. Select a process and click **Delete** to delete the process.

Notes

- Deleting a process does not delete the batches that are based on the process.
- If a process has at least one associated non-versioned batch, it cannot be deleted.

You can delete a process created with Intelligent Capture Designer only if none of its batches remain on the Intelligent Capture Server. For more information, see the Legacy column description in "Processes" on page 278.

Related Topics

"Intelligent Capture Administrator Component Interactions and User interface Language" on page 92

"Adding a Batch" on page 170

"Configuring a Process Step in Setup Mode" on page 157

"Viewing and Defining Access Control for a Process" on page 160

"Viewing Information about a Process" on page 161

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

9.8.2 Installing a Process on an Intelligent Capture Server

After an *IPP* is created in Process Developer, it must be compiled into a process (*IAP* file) using Process Developer and then installed onto the Intelligent Capture Server using either Process Developer or Intelligent Capture Administrator. After a process is installed, each module step associated with the process can be configured in setup mode.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To install a process on the Intelligent Capture Server using the Intelligent Capture Administrator:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Processes**. The **Processes** pane displays the list of processes added to the system.
3. Click **Add**. The **Install Process** window displays.

   This function is only available for processes created using Process Developer. For more information, see the **Legacy** column description in "Processes" on page 278.
4. Type the **Name** of the process. The name must be unique within the list of existing processes. For the maximum length allowed, see *OpenText Intelligent Capture - Operating Specifications (ECPCORE-RLI)*. The process name may contain the following characters:

   - A-Z, a-z, 0-9, <space>
   - - _ ' ' ~ # ! @ $ % [ ] { } ( ) +
5. In the **Process IAP file, including path** field, type the full path name of the Process File (*IAP* file) and press **ENTER**, or **Browse** for the process file.
6. Select **Set the priority for new batches to the server default** to indicate that the batches created with this process should inherit priority from the server's default priority. If this check box is cleared, type the processing priority for the batches in the **Priority for batches based on this process** field. The priority can be any value from 1-99. The default priority is 50.
7. The **Servers Available** list box lists all the servers in the system. Select the servers to install the process to and click **>** or click **>>** to install the process on all the servers. The selected servers are listed in the **Servers Selected** list box.
8. Provide a **Description** for the process.
9. Click **OK**. The process is now installed onto the Intelligent Capture Servers listed in the **Servers Selected** list box.

Related Topics

"Intelligent Capture Administrator Component Interactions and User interface Language" on page 92

"Monitoring Intelligent Capture" on page 96

"Configuring a Process Step in Setup Mode" on page 157

"Viewing and Defining Access Control for a Process" on page 160

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

9.8.3 Installing an Upgraded Process

Existing processes can be upgraded using Process Developer, enabling replacement of the existing process with the upgraded process file (*IAP* file).

This function is only available for processes created using Process Developer. For more information, see the **Legacy** column description in "Processes" on page 278.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To install an upgraded a process:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Processes**. The **Processes** pane displays the list of processes added to the system.
3. Select the process to be replaced with an upgraded process, right-click and select **Add Upgraded Process**. The **Upgrade Process** window displays.
4. In the **Select a process file (IAP) or project file (IPP) to replace this process** field, specify or **Browse** for either the *IPP* associated with the upgraded process or the upgraded *IAP* file.
5. Select the **Upgrade the IPP with MDFs from this workstation** check box to enable Process Developer to update the *MDF*s in the upgraded process. This field is enabled only if the *IPP* file path is provided. Process Developer must be installed for the upgrade to succeed.

   Note: The *MDF* file must exist in the `Include` directory for each module in the process.

6. Select the **Make a backup copy of the IPP** check box to make a backup of and rename the *IPP* file. The *IPP* file is renamed to include "backup" in its name.

7. Select **Make a backup copy of the process** to make a backup of and rename the existing process that resides on the Intelligent Capture Server. The process is renamed to include "backup" in its name.

8. The **Available Servers**list box lists all the servers that contain a process that has the same name as the selected process. Select the servers to install the upgraded process to and click **>** or click **>>** to select all the listed servers. The selected servers are listed in the **Selected Servers** list box.

9. Click **OK**. The upgraded process is now added to the Intelligent Capture Servers listed in the Selected **Servers** list box.

> **Note:** Performing this procedure is recommended during a period of low productivity. During the deletion of the old process and the renaming of the new process, the process is not available. In addition, there is no method of preventing users from selecting the newly installed process and creating batches before the process has been set up correctly and renamed.

Related Topics

"Intelligent Capture Administrator Component Interactions and User interface Language" on page 92

"Monitoring Intelligent Capture" on page 96

"Configuring a Process Step in Setup Mode" on page 157

"Viewing and Defining Access Control for a Process" on page 160

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

9.8.4 Configuring a Process Step in Setup Mode

Module steps in a process must be configured in setup mode. During setup, each module step must be configured as needed for the work it will do when processing tasks during production. If the process uses multiple steps of the same module, they function independently and must be configured independently in setup mode. The module step settings are then saved, and all future batches created from the process inherit them. However, any batches that were created from the process prior to changing the process setup are not affected.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To run a process step in setup mode:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel to display the **Systems** pane.

2. Click **View Processes** to display the **Processes** pane containing the list of available processes.

3. Select the process containing the module step to configure. The **Steps for process** table lists all the module steps associated with the selected process.

4. Double-click the module step to configure or right-click the step and select **Settings**. The corresponding module is run in setup mode. Configure the module step and click **OK** to return to the **Processes** pane.

Notes

- Setup is always run on a single Intelligent Capture Server, where the process to configure resides. When Intelligent Capture Servers are part of a ScaleServer group, each server must have an instance of the process to be used, that is, the process must be installed on all servers in the group. To configure this process the user can do one of the following:
  - Install and configure the process on one of the Intelligent Capture Servers and then copy the process to the other Intelligent Capture Servers in the ScaleServer group.
  - Install the process on all Intelligent Capture Servers. Run setup on the steps of the process on one of the servers, then copy the settings from that process and paste them to the other instances of the process on the other servers.
- If more than one person configures a process at the same time, the Intelligent Capture Server saves the most recent data received.
- Formware can be set up from within Intelligent Capture Administrator, but it must reside in one of these locations to set up the module.
  - Intelligent Capture client `path\binnt`: This is the location for all the Intelligent Capture client modules. By default, this is `C:\Program Files\InputAccel\Client\binnt`.
  - `Formware\Programs`: This is the usual location when Formware is installed.

Related Topics

"Intelligent Capture Administrator Component Interactions and User interface Language" on page 92

"Monitoring Intelligent Capture" on page 96

"Viewing and Defining Access Control for a Process" on page 160

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

9.8.5 Viewing or Modifying Process Settings

Process settings can be viewed and some of the settings can be changed as needed.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view or modify process settings:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Processes**. The **Processes** pane displays the list of processes added to the system.
3. Select a process and click **Settings**. The **Process Settings** window displays the settings for the selected process.
4. Modify the **Name** settings as needed.

   This function is only available for processes created using Process Developer. For more information, see the **Legacy** column description in "Processes" on page 278.

   Caution

   Do not rename a process used by an unattended module that creates batches (as the first module step in the process).

5. Modify the **Description** and **Priority** settings as needed.
6. Click **OK**. The process settings are modified and saved.

Notes

- It is recommended to set up a module and edit module settings through Intelligent Capture Designer > CaptureFlow Designer. While you can also setup a module using Intelligent Capture Administrator, it is best to use either Intelligent Capture Designer or Intelligent Capture Administrator to setup the module. Do not setup or edit any module settings using both Intelligent Capture Administrator and Intelligent Capture Designer because the settings may not be updated correctly. If you change module settings in Intelligent Capture Administrator, you must click **Download Settings** in CaptureFlow Designer so Intelligent Capture Designer updates its own copy of settings with those currently configured for the process.
- If you are logging in from a domain that is different from the Intelligent Capture Server, then you are prompted to specify a valid user in the Intelligent Capture Server domain.

Related Topics

"Intelligent Capture Administrator Component Interactions and User interface Language" on page 92

"Monitoring Intelligent Capture" on page 96

"Configuring a Process Step in Setup Mode" on page 157

"Viewing and Defining Access Control for a Process" on page 160

"Viewing Information about a Process" on page 161

"Intelligent Capture Permissions List" on page 381

9.8.6 Viewing and Defining Access Control for a Process

Access Control Lists (*ACL*) enable definition of access permission for modules, departments, batches, and processes. The **Access Control List** window for processes is displayed from the **Processes** pane.

Note: Modules, departments, batches, and processes have access permissions that differ from Intelligent Capture Administrator permissions. Access permissions determine which users or groups can access the module, department, batch, or process, while Intelligent Capture Administrator permissions control determine which users can access panes and windows within Intelligent Capture Administrator.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view the assigned access control for a process:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel.
2. Select **View Processes** from the **Systems** pane.
3. In the **Processes** pane, select the process and right-click. Select **View Selected** and select **ACLs** from the submenu. The **Access Control List** window for the selected process displays.

For more information on creating access control levels, see "Viewing and Defining Access Control" on page 138.

9.8.7 Viewing Information about a Process

You can view the list of batches for a process, batches based on a process that are in error or on hold, modules associated with a process, module connections, licenses of the modules associated with a process, IA Values in a process, indexed IA Values specified in a process, and *ACL*s defined for a process.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view information about a process:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Processes**. The **Processes** pane displays the list of processes added to the system.
3. Select a process, right-click and select the following options from the **View Selected** menu:
   - **Batches**: Displays the **Batches from Process** window and lists all batches based on the selected process.
   - **Errors and Holds**: Displays the **Batches from Process** window and lists all batches based on the selected process that are in error or on hold.
   - **Modules**: Displays the **Modules** pane and lists all modules associated with the selected process.
   - **Connections**: Displays the **Connections** pane and lists all active connections for modules associated with the selected process.
   - **Module License**: Displays the **Module Licenses** pane and lists all the modules associated with the process and the license codes for each module.
   - **Values**: Displays the **Values** window and displays the IA Values associated with the process.
   - **Indexed Values**: Displays the **Indexed Values** window and displays all the IA Values in the process that are indexed or can be indexed.
   - **ACLs**: Displays the **Access Control List** window and displays the *ACL*s specified for the process.

Related Topics

"Intelligent Capture Administrator Component Interactions and User interface Language" on page 92

"Monitoring Intelligent Capture" on page 96

"Configuring a Process Step in Setup Mode" on page 157

"Viewing and Defining Access Control for a Process" on page 160

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

9.8.8 Viewing or Modifying IA Values of a Process

The **Values** window displays IA Values associated with the process. The values specified for the IA Values can be modified.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view or modify process IA Values:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Processes**. The **Processes** window displays the list of processes added to the system.
3. Select a process, right-click and select **Values** from the **View Selected** menu. The **Values** window displays. This window consists of a tree view on the left and an IA Values list on the right. The tree view contains various nodes that display and enable navigation through the various IA Value types. The list on the right displays the IA Values for the selected tree node.
4. Select a node from the tree view to view the IA Values for the selected node.
5. To change an IA Value, select the IA Value, right-click and select **Edit Value**. The **Setting** of the selected IA Value can be changed.
6. Click **OK** to save the changes and close the window.

Related Topics

"Intelligent Capture Administrator Component Interactions and User interface Language" on page 92

"Monitoring Intelligent Capture" on page 96

"Configuring a Process Step in Setup Mode" on page 157

"Viewing and Defining Access Control for a Process" on page 160

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

9.8.9 Viewing or Selecting Indexed or Searchable IA Values of a Process

IA Values can be indexed to enable them being searchable. The **Indexed Values** pane displays process IA Values that are indexed or can be indexed.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view or select indexed or searchable IA Values of a process:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Processes**. The **Processes** pane displays the list of processes added to the system.
3. Select a process, right-click and select **Indexed Values** from the **View Selected** menu. The **Indexed Values** window displays.
4. Select the **Level filter** to filter on. The list of IA Values is filtered to display only those IA Values for the selected level. Select **All Levels** to display IA Values for all levels in the process.
5. Select the **Step filter**. The list of **Values available for indexing** is filtered to display only those IA Values for the selected step in the process. Select **All** to display all the IA Values for all the steps in the process.
6. The **Values available for indexing** list box lists the IA Values that can be indexed, filtered on the **Level** and **Step**. Select the IA Values to index and click **>** or click **>>** to select all the IA Values. The selected IA Values are listed in the **Values selected for indexing** list box. A maximum of 10 IA Values can be selected as indexed IA Values.
7. Click **OK** to save the changes and close the window.

Related Topics

"Intelligent Capture Administrator Component Interactions and User interface Language" on page 92

"Monitoring Intelligent Capture" on page 96

"Configuring a Process Step in Setup Mode" on page 157

"Viewing and Defining Access Control for a Process" on page 160

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

9.9 Managing Batches

Batches are created based on the installed processes. A batch is a group of pages that are processed as a unit using a predetermined set of instructions that are specified in a process. A batch is always associated with an Intelligent Capture process and contains all necessary processing instructions, the page files to be processed, and the data that results from processing.

9.9.1 Understanding the Components of the Batch Traffic Pane

The **Batch Traffic** pane (Figure 9-1) provides batch related information that enables administrators to monitor batch traffic in the Intelligent Capture system.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Components of the Batch Traffic Pane

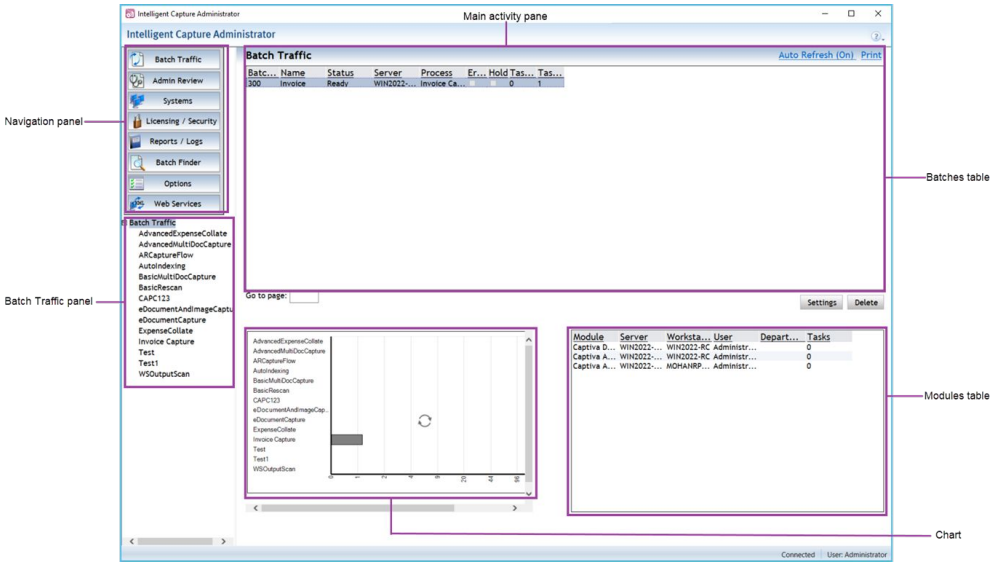

Figure 9-1: Intelligent Capture Administrator—batch traffic window

The **Batch Traffic** pane includes the following components:

- ***Batch Traffic** panel*: Displays below the navigation panel. The **Batch Traffic** panel includes a sub-navigation panel that lists all the processes installed on the system.
- *Batches table (top table)*: Displays the list of batches. The batches list can be filtered by selecting a process from the **Batch Traffic** panel. This displays batches for the selected process. If no process is selected, all batches in the system are displayed. Double-clicking a batch displays various information about the batch depending on the **View** selected in the batch window that displays.
- *Chart*: When no processes or batches are selected, displays all processes. When a process or batch is selected, displays the steps associated with the selection. The bars on the chart provide quantitative data for the displayed processes or steps:
  - *Red hatch bar*: Count of batches in error, hold, or priority 0. Count of tasks in error.
  - *Gray bar*: Count of batches or tasks in ready, working, or sent status.
  - *White bar*: Count of batches or tasks with any status other than the statuses represented by the Red hatch bar and the Gray bar.
- Modules *table (bottom table)*: Displays the connected modules for all installed processes when no batch is selected, or the connected modules associated with the selected batch. This shows all data for the displayed module, not just the steps from the selected batch. Right-click a module to view additional information, disconnect the module, or refresh the module list.

Notes

- The Intelligent Capture Administrator must connect to each Intelligent Capture Server in the system to collect and then display information for the tables and chart. A validation summary is displayed if Intelligent Capture Administrator loses connection with an Intelligent Capture Server. Batches, processes, and modules information from the disconnected Intelligent Capture Server will not be included in the information displayed in the **Batch Traffic** pane.
- Updates to the settings on the **Batch Traffic** pane may not be recorded immediately. To see the changes right away, click **Auto Refresh** twice. Otherwise, wait until the screen refreshes based on the **Page Refresh Rates** specified on the **Default Settings** or **My Preferences** pane.

You can view the following information in the **Batch Traffic** pane depending on the selections you make:

- "Viewing All Batches in the System" on page 166
- "Viewing Batches for a Specific Installed Process" on page 168

Related Topics

"Adding a Batch" on page 170

"Viewing and Modifying Batch Settings" on page 171

"Configuring a Batch Step in Setup Mode" on page 169

"Copying Step, Process, and Batch Settings" on page 197

"Viewing All Batches for a Process, Module, or Server" on page 196

"Intelligent Capture Permissions List" on page 381

9.9.2 Viewing All Batches in the System

Intelligent Capture Administrator can display batches, installed processes, and the module connections currently configured for any of the installed processes. For a description of the various components of the **Batch Traffic** pane, see"Understanding the Components of the Batch Traffic Pane" on page 164.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view all batches in the system:

1. In the **Intelligent Capture Administrator** window, select **Batch Traffic** from the navigation panel. The **Batch Traffic** pane displays the following information:
   - **Batches table**: Initially displays all the batches for all processes that are installed on the system. Selecting any batch(es) in the table, highlights the

batch(es) and filters the information displayed in the chart and **Modules** table.

- **Chart**: Initially displays all processes installed on the system. After a batch is selected, the bars in the chart display the number of batches (including batches that are in error and on hold) associated with each process. The number of batches on error and hold are indicated at the left of the bar and denoted by a diagonal pattern.
  - If a single batch is selected from the **Batches** table, then the chart displays the module steps associated with the batch and the bars in the chart display the corresponding task count for each module step.
  - If multiple batches are selected from the **Batches** table, and the selected batches are associated with the same process, then the chart displays the module steps associated with the batches and the bars in the chart display the corresponding (cumulative for the selected batches) task counts for each module step.
  - If multiple batches are selected from the **Batches** table, and the selected batches are associated with different processes, then the chart displays the processes that are associated with the selected batches.
  - The bars on the chart provide quantitative data for the displayed processes or steps:
    - Red hatch bar: Count of batches in error, hold, or priority 0. Count of tasks in error.
    - Gray bar: Count of batches or tasks in ready, working, or sent status.
    - White bar: Count of batches or tasks with any status other than the statuses represented by the Red hatch bar and the Gray bar.
- **Modules table**: Displays modules and module connections configured for any of the installed processes.
  - If the chart displays a specific process and the steps associated with the process, then the **Modules** list displays modules and module connections configured for the process.

2. Select a batch from the **Batches** table, right-click and select from the available options depending on the task you want to accomplish.

Related Topics

"Understanding the Components of the Batch Traffic Pane" on page 164

"Adding a Batch" on page 170

"Viewing and Modifying Batch Settings" on page 171

"Configuring a Batch Step in Setup Mode" on page 169

"Copying Step, Process, and Batch Settings" on page 197

"Viewing All Batches for a Process, Module, or Server" on page 196

"Intelligent Capture Permissions List" on page 381

9.9.3 Viewing Batches for a Specific Installed Process

Intelligent Capture Administrator can display batches associated with a specific process, the module steps of the process, the task count for each step in the process, and the module connections currently configured for the process. For a description of the various components of the **Batch Traffic** pane, see "Understanding the Components of the Batch Traffic Pane" on page 164.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view batches for a specific process:

1. In the **Intelligent Capture Administrator** window, select a process from the **Batch Traffic** sub-navigation panel. The **Batch Traffic** pane displays the following information:
   - **Batches table**: Displays all the batches for the selected process. Selecting any batch(es) from the **Batches** table, highlights the batch(es) and filters the information displayed in the chart and **Modules** table.
   - **Chart**: Initially displays all module steps associated with the process.
     - If batch(es) are selected from the **Batches** table, then the chart displays the module steps associated with the selected batch(es).
     - The bars on the chart provide quantitative data for the displayed processes or steps:
       - **Red hatch bar**: Count of batches in error, hold, or priority 0. Count of tasks in error.
       - **Gray bar**: Count of batches or tasks in ready, working, or sent status.
       - **White bar**: Count of batches or tasks with any status other than the statuses represented by the Red hatch bar and the Gray bar.
   - **Modules** table: Displays module connections (regular client modules) that are configured for the process.
2. Select a batch from the **Batches** list, right-click and select from the available options depending on the task you want to accomplish.

Related Topics

"Understanding the Components of the Batch Traffic Pane" on page 164

"Adding a Batch" on page 170

"Viewing and Modifying Batch Settings" on page 171

"Configuring a Batch Step in Setup Mode" on page 169

"Copying Step, Process, and Batch Settings" on page 197

"Viewing All Batches for a Process, Module, or Server" on page 196

"Intelligent Capture Permissions List" on page 381

9.9.4 Configuring a Batch Step in Setup Mode

Modules steps in a batch can be configured if the process settings are not appropriate. To configure a batch step, the module corresponding to the step is run in setup mode.

Note: The module to be set up must be installed on the machine where the Intelligent Capture Administrator is running the module for setup.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To run a batch step in setup mode:

1. In the **Intelligent Capture Administrator** window, select **Batch Traffic** from the navigation panel to display the **Batch Traffic** pane. "Understanding the Components of the Batch Traffic Pane" on page 164 describes the various components of the **Batch Traffic** pane.
2. Right-click the batch you want to configure and select **Settings** to display the **Batch Settings** window.
3. Select **Steps** from the **View** list. The **Batch Steps** pane displays the module steps in the batch.
4. From the **Steps** table, double-click the module step to configure or right-click the step and select **Settings**. The corresponding module is run in setup mode. Configure the module step and click **OK** to return to the **Batch Steps** pane.

   Notes

   - If more than one person configures a batch at the same time, the Intelligent Capture Server saves the most recent data received.
   - FormWare can be set up from within Intelligent Capture Administrator, but it must reside in one of these locations to set up the module.
     - Intelligent Capture client `path\binnt`: This is the location for all the Intelligent Capture client modules. By default, this is `C:\Program Files\InputAccel\Client\binnt`.
     - `Formware\Programs`: This is the usual location when FormWare is installed.

The module step changes you made overwrite the inherited process settings for the specific batch. The original process and other batches are not affected, however.

Related Topics

"Viewing All Batches in the System" on page 166

"Viewing Batches for a Specific Installed Process" on page 168

"Adding a Batch" on page 170

"Viewing and Modifying Batch Settings" on page 171

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

9.9.5 Adding a Batch

Add a new batch based on an existing process using the **Add Batch** window. New batches are associated with an existing installed *IAP* file.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To add a new batch:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigational panel.
2. Select **View Processes** from the Systems pane. The **Processes** pane displays a list of processes installed on the Intelligent Capture Servers.
3. Select a process, right-click and select **Add Batch**. The **Add Batch** window displays.
4. The **Add Batch** window displays the following fields:
   - **Based on process**: Displays the name of the process that the new batch is based on.
   - **Batch name**: Type a unique name in the name field. You may use any characters in your batch names.
   - **Name schema**: Displays the new batch schema automatically if the process is configured to name batches using a naming schema.
   - **Use default priority from process**: Specifies that the batch should inherit its priority from the process it is based on. Change the processing priority for the batch in the **Batch Priority** field only if the batch has special processing needs. The default of 50 tells the server to send batch tasks to any available module along with tasks from any other open batches also set to the default

processing priority. If you want the server to process the batch first, set its priority to 1-49. If you want the batch to have a lower priority than other batches, change its priority to 51-99.

Note: To change the priority of a batch at any time, see Viewing and modifying batch settings

- **Description**: Type notes about the batch.

5. Click **OK** to create the batch as specified and close the window.

Related Topics

"Exporting a Batch" on page 181

"Moving a Batch" on page 182

"Intelligent Capture Permissions List" on page 381

"Customizing Information Tables Using the Column Manager" on page 112

9.9.6 Viewing and Modifying Batch Settings

The **Batch Settings** window enables the administration of batch settings from within the **Intelligent Capture Administrator** window.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view or modify batch settings:

1. In the **Intelligent Capture Administrator** window, select **Batch Traffic**. The **Batch Traffic** pane displays.

2. Double-click a batch and select **Settings** from the **View** list box. The **Batch Settings** window displays.

   To make the same changes to multiple batches at the same time, you select multiple batches (**CTRL**+click or **SHIFT**+click) and then right-click and select an action from the context menu.

   You can view or modify the following batch settings:

   - **Name**: Batch name displays the name of the batch.
   - **Description**: Batch description displays a description of the batch.
   - **Priority**: Batch priority, valid values are 1 - 99, with 1 indicating the highest priority and 99 indicating the lowest priority.
   - **Status**: Batch status can be changed by selecting the appropriate check box:
     - **Hold**: Select to set the **Hold** status of the batch.
     - **Error**: Select to set the **Error** status of the batch.

3. You can view the following batch details:

   - **Compile Time**: Date and time when the batch process was compiled.
   - **Intelligent Capture Process Developer Version**: Version of Process Developer used to develop the process.
   - **Original CaptureFlow**: Name of the CaptureFlow with the installed process selected for the batch during its creation.
   - **CaptureFlow Version ID**: Version of the CaptureFlow with the installed process selected for the batch during its creation.
   - **VBA Version**: Version of Visual Basic that was used to create the batch process.
   - **Process Compiler Version**: Version of Process Developer that was used to compile the batch process.

4. Click **OK** to save the new settings and return to the **Batch Traffic** pane, or click **Apply** to save the new settings and to continue working in the **Batch Settings** window.

Related Topics

"Adding a Batch" on page 170

"Exporting a Batch" on page 181

"Locating and Fixing Batch Problems" on page 194

"Intelligent Capture Permissions List" on page 381

9.9.7 Viewing and Defining Access Control for Batches

Access Control Lists (*ACL*) allow definition of access permission for modules, departments, batches, and processes. The **Access Control List** window for batches is displayed from any pane displaying batches in Intelligent Capture Administrator.

Note: Modules, departments, batches, and processes have access permissions that differ from Intelligent Capture Administrator permissions. Access permissions determine which users or groups can access the module, department, batch, or process, while Intelligent Capture Administrator permissions control determine which users can access panes and windows within Intelligent Capture Administrator.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view the assigned access control for a batch :

1. In the **Intelligent Capture Administrator** window, when viewing a batch from the **Batch Traffic**, **Admin Review**, or **Batch Finder** panes, select a batch and right-click.

2. Select **View Selected** and select **ACLs** from the submenu. The **Access Control List** window for the selected batch displays.

For more information on creating access control levels, see "Viewing and Defining Access Control" on page 138.

Related Topics

"Intelligent Capture Permissions List" on page 381

9.9.8 Viewing or Modifying Module Steps of a Batch

The **Batch Steps** pane displays all the module steps in the process associated with a batch.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view or modify module steps for a batch:

1. In the **Intelligent Capture Administrator** window select **Batch Traffic**. The **Batch Traffic** pane displays.
2. Double-click the batch name to display the **Batch Settings** window.
3. Select **Steps** from the **View** list box to display the following information in the **Batch Steps** pane:

   Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

   - **Step ID**: The unique ID associated with the step.
   - **Name**: The step name
   - **Trigger**: The trigger level for the step.
   - **Departments**: The departments associated with the module step.
   - **Module**: The name of the module associated with the step.
   - **Executable**: The executable name of the module associated with the step.
4. Select a module step from the **Steps** list, right-click the step, and choose the relevant option to modify the step settings.
5. Click **OK** to close the pane and display the **Batch Traffic** pane.

Related Topics

"Viewing All Batches in the System" on page 166

"Viewing Batches for a Specific Installed Process" on page 168

"Adding a Batch" on page 170

"Viewing and Modifying Batch Settings" on page 171

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

9.9.9 Viewing the Status of Tasks for a Batch

The **Batch Tasks** pane displays a tree list view of all nodes in the selected batch including the Level 0 node, the steps for that batch, and the current status of each step in the batch.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view the tasks status for a batch:

1. In the **Intelligent Capture Administrator** window, select **Batch Traffic**. The **Batch Traffic** pane displays.
2. Double-click the batch name to display the **Batch Settings** window.
3. Select **Tasks** from the **View** list box to display the **Batch Tasks** pane with the following information:

   Note: If a batch contains a large number of tasks, the tasks are listed across multiple pages. Use the **Go to page** field to define the page number to navigate to and press **ENTER**.

   - **Node**: Displays the batch tree view of all the nodes in the batch including the Level 0 node. Includes a description for each node. You can double-click a Level 0 node to bring up the image view for the selected node.
   - Column for each module step in the batch: Displays the status for the page node in the batch for all the batch steps. Status types include:
     - **Done**: The module step has finished processing the task.
     - **Not Ready**: No tasks are currently queued for the step.
     - **Ready**: Tasks are queued for the step.
     - **Working**: The module step is currently processing the task.
     - **Hold**: The tasks associated with the module step are on hold.
     - **Error**: The tasks associated with the module step contain an error.
     - **Sent**: The tasks associated with the module step are sent by the Intelligent Capture Server.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Related Topics

"Viewing All Batches in the System" on page 166

"Viewing Batches for a Specific Installed Process" on page 168

"Adding a Batch" on page 170

"Viewing and Modifying Batch Settings" on page 171

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

9.9.9.1 Viewing Image Properties of a Level 0 Batch Node

The **Image Properties** window displays the image properties for a selected level 0 batch node (page node).

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view level 0 batch nodes with the Image Viewer:

1. In the **Intelligent Capture Administrator** window, select **Batch Traffic**. The **Batch Traffic** pane displays.
2. Double-click the batch name to display the **Batch Settings** window.
3. Select **Tasks** from the **View** list box to display the **Batch Settings Tasks** pane.
4. Double-click a level 0 node (page node) to display the image view of the selected node in the **Image Viewer** window.
5. Click the  toolbar option to display the **Image Properties** window with the following information about the selected level 0 node.

Table 9-4: Image Properties

Image Property	Description
Annotation Count	Number of annotation objects on the current image.

Image Property	Description
Barcode Count	Number of barcodes detected on the current page. The count displayed is based on the step for which the image is viewed.
ColorFormat	Color format to be used for saving the image.
Width in pixels	Number of columns of pixels in the image.
ImageLength	Number of rows of pixels in the image.
BitsPerSample	Number of bits per sample in the current image.
Compression	Compression type to be used for saving the image.
PhotometricInterpretation	Color space of the image data of the current page.
SamplesPerPixel	Number of samples per pixel in the current image.
Horizontal Resolution in pixels	Horizontal resolution in pixels per inch.
Vertical Resolution in pixels	Vertical resolution in pixels per inch.

Related Topics

"Viewing All Batches in the System" on page 166

"Viewing Batches for a Specific Installed Process" on page 168

"Viewing the Status of Tasks for a Batch" on page 174

"Viewing and Modifying Batch Settings" on page 171

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

9.9.9.2 Viewing Level 0 Batch Nodes with the Image Viewer

The **Image Viewer** displays the image view for a selected level 0 batch node (page node).

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view level 0 batch nodes with the Image Viewer:

1. In the **Administration Console** window, select **Batch Traffic**. The **Batch Traffic** pane displays.
2. Double-click the batch name to display the **Bath Settings** window.

3. Select **Tasks** from the **View** list box to display the **Batch Settings Tasks** pane.

4. Double-click a level 0 node (page node) to display the image view of the selected node in the **Image View** window.

Note: You can only view images imported using ScanPlus. An error is displayed if you double-click a page node to display images imported with any other batch creating module.

The following table describes the toolbar options available to modify the image view:

Table 9-5: Image Viewer Window

Button	Button Name	Description
	**Fit to Window**	Scales the image to fit the current width and height of the **Image Viewer** window.
	**Fit to Width**	Scales the image to fit the width of the image to the current width of the **Image Viewer** window.
	**Actual Size**	Displays the image with its actual width and height.
	**90 Degrees Counterclockwise**	Changes the image orientation to 90 degrees counter clockwise.
	**180 Degrees**	Changes the image orientation to 180 degrees.
	**90 Degrees Clockwise**	Changes the image orientation to 90 degrees clockwise.
	**Pointer**	Resets the cursor to a pointer if it was previously set as a **Zoom In** or **Zoom Out** cursor.
	**Zoom In**	Zooms in the image.
	**Zoom Out**	Zooms out the image.

Button	Button Name	Description
	**Save As**	Saves the image to the specified location.
	**Print**	Prints the image.
	**Settings**	Displays the properties of the image. "Viewing Image Properties of a Level 0 Batch Node" on page 175 lists the various image properties.

Note: Changing the orientation of pages only affects the image view but does not change the image output by the module.

Related Topics

"Viewing All Batches in the System" on page 166

"Viewing Batches for a Specific Installed Process" on page 168

"Viewing the Status of Tasks for a Batch" on page 174

"Viewing and Modifying Batch Settings" on page 171

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

9.9.10 Viewing or Modifying Batch IA Values

The **Batch Values** pane displays IA Values associated with the batch.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view or modify batch IA Values:

1. In the **Intelligent Capture Administrator** window, select **Batch Traffic**. The **Batch Traffic** pane displays.
2. Double-click the batch name to display the **Batch Settings** window.
3. Select **Values** from the **View** list box to display the **Batch Values** pane. This pane consists of a tree view on the left and an IA Values list on the right. The tree view contains various nodes that display and enable navigation through the various IA Value types. The IA Values list on the right displays the actual IA Values for the selected tree node. The following information is displayed:

- Tree view (left area):
  - **Step Values**: Contains a subnode for each module step in the batch. Selecting a module step node displays the global setup values and default batch level values for the module associated with the selected module step.
  - **Tree Values**: Displays the graphic representation of the batch and contains the batch tree structure and its subnodes. Selecting a node displays the batch IA Values for the selected node.
  - **Default Node Level Values**: Contains a subnode for each batch level (0-7). Selecting a subnode displays the default IA Values defined in the *MDF* file for the selected level. The batch **Tree Values** are populated with these default values before the batch is processed. As the batch is processed, the default values are replaced with the actual IA Values of the batch. After a default value has been set, nodes created after that point will not be affected by subsequent changes to the default value.

    Note: Changes to a default value propagate to existing nodes if the default value has never been set prior to creating the nodes.
  - **Non-Nodal Values**: Global values for the batch. These values are not associated with any nodes.
- IA Values list (right area) displays the following information about the IA Values for the selected tree node in the tree view:

  Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.
  - **Value Name**: Name of the IA Value shown as <*InstanceName.ValueName*>.
  - **Value Type**: Type of IA Value: **Integer**, **Long**, **File**, **String**, etc.).
  - **Setting**: Value set in the IA Value.
  - **Input**: Selected if the IA Value is an Input IA Value (variable that is used as input data).
  - **Output**: Selected if the IA Value is an Output IA Value (variable that is used as output data).
  - **Trigger**: Selected if the IA Value is a Trigger IA Value (variable that is used to notify an Intelligent CaptureServerthat a task is ready for processing).
  - **Prefetch**: Selected if the IA Value is a Prefetch IA Value (file that is sent with the task).

- **Prime**: Selected if the IA Value is a Prime IA Value (variable that is sent with the task).
- **Step**: The name of the module step if the IA Value is associated with a module.
- **Level Name**: The level name where the module step IA Value exists.
- **Level Number**: Tree level number of the module step IA Value.

4. Select a node from the tree view to view the IA Values for the selected node.
5. To change an IA Value, select the IA Value from the IA Values list, right-click and select **Edit Value**. For most data types, the **Setting** column of the selected IA Value can be changed to a new value in place. If the value is a string that contains document type data from Extraction or Completion, a separate window will display the **Document Type Editor**.

   The **Document Type Editor** displays all of the fields defined in the document type, including those that have no associated user interface or are hidden from the Completion module operator. Fields in the editor are always editable and are never read-only or disabled. Tables are always displayed as a grid. Cells in the grid can be edited but rows cannot be added or deleted. The editor only displays a form for viewing and editing the data; it does not execute validation rules to confirm whether the data is correct and it does not run scripts that would modify the data in the Completion module. After making changes, click **OK** to save the document type data in the selected IA Value.
6. Click **OK** to close the pane and display the **Batch Traffic** pane.

Related Topics

"Viewing All Batches in the System" on page 166

"Viewing Batches for a Specific Installed Process" on page 168

"Copying and Replacing Batch IA Values on the Server" on page 204

"Intelligent Capture Permissions List" on page 381

9.9.11 Viewing and Unlocking Locked Nodes on a Batch

When batch creation modules create new nodes, they keep those nodes exclusively locked until the module (or the operator, in case of attended modules) releases the batch. If the batch is closed without releasing it, or if a malfunction such as a power failure interferes with batch closing, nodes may remain locked and never advance to the next processing step. In these cases, an administrator must remove the saved locks.

The **Batch Locks** pane displays the locked nodes of a batch tree and enables them to be manually unlocked.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view and unlock nodes on a batch:

1. In the **Intelligent Capture Administrator** window, select **Batch Traffic** from the navigation panel. The **Batch Traffic** pane displays.
2. Double-click a batch and select **Locks** from the **View** list box. The **Batch Locks** pane displays the batch nodes that are locked.
3. Select the nodes to unlock, right-click, and select **Unlock** to unlock the selected node or select **Unlock All** to unlock all batch nodes in the list.
4. Right-click the list and select **Refresh** to update the list and retrieve new locked nodes information from the connected Intelligent Capture Servers.

Related Topics

"Viewing All Batches in the System" on page 166

"Viewing Batches for a Specific Installed Process" on page 168

"Retriggering a Batch Step" on page 195

"Intelligent Capture Permissions List" on page 381

9.9.12 Exporting a Batch

Batches can be exported to a different directory as a zip compressed archive. Exported batches cannot be processed until they are restored onto an Intelligent Capture Server.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To export a batch:

1. In the **Intelligent Capture Administrator** window, select **Batch Traffic** from the navigational panel. The **Batch Traffic** pane displays.
2. Select the batch to export, right-click and select **Export Batch**. The **File Download** window displays.
3. Click the appropriate option to continue:
   - **Open**: To view the file.
   - **Save**: To save the file. The **Save As** window displays, select where to save the file.

Related Topics

"Adding a Batch" on page 170

"Moving a Batch" on page 182

"Copying Batches to Another Server" on page 183

"Intelligent Capture Permissions List" on page 381

9.9.13 Moving a Batch

Move selected batches between Intelligent Capture Servers, if the servers are on the same system. Processing continues after the entire batch has been moved.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To move a batch:

1. Connect to two or more Intelligent Capture Servers. For more information, see "Adding and Connecting Intelligent Capture Servers" on page 116.
2. Select **Batch Traffic** from the navigational panel. The **Batch Traffic** pane displays.
3. Select one or more batches, right-click and select **Move to Server**. The **Move Batch** window displays.
4. From the **Server** list box, select the server to receive the batch(es).
5. Click **OK** to move the specified batch(es) to the new server. An **Error** message displays if the batch is already on the Intelligent Capture Server.

Note: When a batch is moved from one server ("source" server) to another ("target" server), the batch report for the source server will show the batch has been deleted. This does not mean it has been deleted from the system, but only from the server where it previously resided. The batch is now on the target server and information about the batch will be displayed in reports for that server. Thus, when a server report shows a batch as deleted, it may have been permanently deleted from the system or it may have been moved to another server.

Related Topics

"Adding a Batch" on page 170

"Exporting a Batch" on page 181

"Copying Batches to Another Server" on page 183

"Locating and Fixing Batch Problems" on page 194

"Intelligent Capture Permissions List" on page 381

9.9.14 Copying Batches to Another Server

`BatchCopy.exe` can perform the following tasks:

- Export batches to a zip file to a local directory or an FTP server.
- Import a zip file (of batches) from a local directory or an FTP server to a server in the same or different capture systems.
- Copy batches directly from one server to another one (in the same or different capture systems).

By default, this utility is located in `C:\Program Files (x86)\InputAccel\Client\binnt\`.

Notes

- By default, existing batches, profiles, document types, CaptureFlow scripts and recognition projects are not overwritten. If there are existing batches, then the import or copy operation fails. If there are existing profiles, document types, CaptureFlow scripts or recognition projects, the import or copy operation succeeds, but unpredictable behavior might result because they were not overwritten.

  Set the appropriate options for overwriting existing batches, profiles, document types, CaptureFlow scripts and recognition projects.

- To copy recognition projects, you must check **Copy Recognition Data** and make sure that the `RecognitionProjectSharedDirectory` directory (on either or both the source and destination servers, as appropriate) is accessible to the user running `BatchCopy.exe` and that the appropriate recognition project files reside in that directory (if you are exporting batches to a zip file).

  The `RecognitionProjectSharedDirectory` directory is specified in Intelligent Capture Designer's **System** > **System Configuration** > **Configuration Settings** > **Other Options** > **GlobalOptions** > **Recognition Project** > **RecognitionProjectSharedDirectory** option.

- For FTP, the following protocols are required:

  – FTP (File Transfer Protocol) and FTPS (File Transfer Protocol plus SSL or FTP/SSL) extension.

  – SFTP (Secure File Transfer Protocol or SSH File Transfer Protocol) protocol.

- Canceling an import, export, or copy operation only stops processing at that exact moment; completed work is not rolled back. See the status log for work completed.

To copy batches directly from one server to another...	In Intelligent Capture Batch Copy, select **From server to server** and follow the instructions. **Notes** • Only specify one destination server. If multiple servers are specified, then only the first server is connected. • Scale Server Groups are not supported. If a Scale Server Group is specified as a destination server, then only the first server in the group is connected. • The **Copy Recognition Data** option includes only the Advanced Recognition modules (that is, Classification, Identification, Extraction, and Collector). • If you are copying recognition projects (checked **Copy Recognition Data**), then the `RecognitionProjectSharedDirectory` directory must meet the requirements as specified for exporting and importing batches to and from zip files.

To export batches to a zip file on an FTP server...	In Intelligent Capture Batch Copy, follow these steps: 1. Select **From server to files**. 2. Go to the next step and follow the instructions to select the batches. 3. Go to the next step, select **FTP Server**, and follow the instructions to specify the connection to the FTP server. **Notes** • The remote **FTP Directory** option is optional and can be declared as a relative path so that archived files are not copied to the root directory of the FTP server. • If you are exporting multiple batches and you specify a folder that contains existing zip files, then you are prompted to overwrite the existing zip files. • The **Copy Recognition Data** option includes only the Advanced Recognition modules (that is, Classification, Identification, Extraction, and Collector). • If you are copying recognition projects (checked **Copy Recognition Data**), then the `RecognitionProjectSharedDirectory` directory must contain the recognition project data and be one of the following: – A shared directory that is accessible from the machine on which `BatchCopy.exe` is running. – A local directory on the machine on which `BatchCopy.exe` is running.

To import batches from a zip file on an FTP server...	In Intelligent Capture Batch Copy, follow these steps: 1. Select **From files to server**. 2. Go to the next step, select **FTP Server**, and follow the instructions to specify the connection to the FTP server. **Notes** • If you are importing a zip file that contains recognition projects, then the `RecognitionProjectSharedDirectory` directory into which to extract the recognition project files must be one of the following: – A shared directory accessible from the machine on which `BatchCopy.exe` is running. – An existing local directory (or a valid path on which to create the directory) on the machine on which `BatchCopy.exe` is running. • If the `RecognitionProjectSharedDirectory` value has not been specified, then the recognition project is extracted to a local directory on the machine on which `BatchCopy.exe` is running. This directory is recorded in the status and trace logs.

To export batches to a zip file...	In Intelligent Capture Batch Copy, follow these steps: 1. Select **From server to files**. 2. Go to the next step and follow the instructions to select the batches. 3. Go to the next step, select **File Directoy**, and follow the instructions. **Notes** • If you are only exporting one batch, you must specify the zip file name. • If you are exporting multiple batches and you specify a folder that contains existing zip files, then you are prompted to overwrite the existing zip files. • The **Copy Recognition Data** option includes only the Advanced Recognition modules (that is, Classification, Identification, Extraction, and Collector). • If you are copying recognition projects (checked **Copy Recognition Data**), then the `RecognitionProjectSharedDirectory` directory must contain the recognition project data and be one of the following: – A shared directory that is accessible from the machine on which `BatchCopy.exe` is running. – A local directory on the machine on which `BatchCopy.exe` is running.

To import batches from a zip file...	In Intelligent Capture Batch Copy, follow these steps: 1. Select **From files to server**. 2. Go to the next step, select **File Directory**, and follow the instructions. **Note:** If you are importing a zip file that contains recognition projects, then the `RecognitionProjectSharedDirectory` directory into which to extract the recognition project files must be one of the following: • A shared directory accessible from the machine on which `BatchCopy.exe` is running. • An existing local directory (or a valid path on which to create the directory) on the machine on which `BatchCopy.exe` is running. If the `RecognitionProjectSharedDirectory` value has not been specified, then the recognition project is extracted to a local directory on the machine on which `BatchCopy.exe` is running. This directory is recorded in the status and trace logs. You can also drag and drop zip files to be imported.

Related Topics

"Adding a Batch" on page 170

"Exporting a Batch" on page 181

"Moving a Batch" on page 182

9.9.15 Searching for Batches

Use the **Batch Finder** pane to perform simple batch searches or to create search filters. Search criteria can include batch name, process name, and any IA Values associated with the batch.

9.9.15.1 Finding a Batch

Users can perform simple batch searches. Search criteria can include batch name, process name, and any IA Values associated with the batch. The search string can be a maximum of 256 characters long, wildcard characters are not allowed, and search strings with spaces in them need to be enclosed in quotes. To use an IA Value as a search criteria it must be indexed.

To find a batch:

1. In the **Intelligent Capture Administrator** window, select **Batch Finder** from the navigational panel. The **Find a Batch** pane displays.
2. Type a batch name, process name, or an IA Value in the text box and click **Find**. The **Batch Finder Results** pane displays the search results.

Notes

- Do not use the < character when searching for a batch name as it results in an error.
- Use the special substring `&cln;` as a substitute for a colon (:). For example, to search for a batch name called `009-TERRADE-DOMINGUEZ-VALERIE-17/10/2012-142815-773254 [Pages:7]`, your search string would be `009-TERRADE-DOMINGUEZ-VALERIE-17/10/2012-142815-773254 [Pages&cln;7]`
- Use the colon symbol to split the search string into different values. For example, the search string `batchName1:batchName2` searches for batches with names `batchName1` and `batchName2`.

The rules for searching for a batch using the advanced search feature are slightly different. For more information, see "Specifying Batch Search Filters" on page 190.

- *Batches table (top table)*: Displays the list of batches.
- *Chart*: Displays the installed processes or module steps in a process depending on the user's selection.
- *Modules table (lower right area in the right pane)*: Displays the modules connected for all installed processes or specific processes depending on the user selection.

Note: To understand how the tables interact in the window, see "Understanding the Components of the Batch Traffic Pane" on page 164.

Related Topics

"Specifying Batch Search Filters" on page 190

"Viewing and Modifying Batch Search Filters" on page 192

"Displaying Batch Search Results" on page 193

9.9.15.2 Specifying Batch Search Filters

Users can specify search filters to find batches in the system. Use the filter name and the description to save and identify the search filters. See "Viewing and Modifying Batch Search Filters" on page 192.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To specify a batch search filter:

1. In the **Intelligent Capture Administrator** window, select **Batch Finder** from the navigational panel. The **Find a Batch** pane displays. The **Batch Finder** panel displays below the navigation panel.
2. Select **Advanced Search** from the **Batch Finder** panel. The **Batch Finder - (New Search)** pane displays.
3. Under **Filter Name for This Search**, type the **Name** and the **Description** for the filter.
4. Select **Batch Properties to Match**. Batches are retrieved based on the batch settings specified:

   Notes

   - Users can use the "%" character for wildcard searches on **Name**, **Description**, or **In any indexed value**. For example, typing `%Accounting%` in the **Name** field will search and filter all batches with **Accounting** in the name.
   - Use the special substring `[[]` as a substitute for a `[` For example, to search for a batch name called `009-TERRADE-DOMINGUEZ-VALERIE-17/10/2012-142815-773254 [Pages:7]`, your search string would be `009-TERRADE-DOMINGUEZ-VALERIE-17/10/2012-142815-773254 [[]Pages:7]`

   - **Name**: Specify the name of the batch to search for. Do not use the < character when searching for a batch name as it results in an error.
   - **Description**: Type the description of the batch.
   - **Server**: Select the Intelligent Capture Server to search. The batches are searched for in the selected Intelligent Capture Server. The default is the current Intelligent Capture Server name.

- **Process**: Select the process associated with the batch.
- **Status**: Specify the batch status.
- **Priority less than or equal to**: Specify a batch priority. The filter searches for batches with a priority less than the number selected in this list box.
- Select the appropriate **Batch was created** option:
  - **Anytime**: The search will not filter based on batch creation date and time.
  - **At least this many days ago**: Search displays batches whose creation date and time occurred before the specified number of days in the past.
  - **Before this date**: The search filters the available batches based on batch creation date and time.
  - **Batch contains value**: The search filters the available batches based on the contents of a searchable IA Value. Searchable IA Values are IA Values of a process that have been indexed. Select one of these options to specify a searchable IA Value to use in the search:
    - **In any indexed value**: Searches all searchable IA Values for the selected text.
    - **In value**: Select the IA Value from the list box to use in the search. The list box displays all the searchable IA Values in the system.

5. Click the appropriate option:

- **Run Search**: Runs the filter to search for batches. Displays the **Batch Finder Results** pane.
- **OK**: Saves the current search as a filter, or updates the existing filter if it was saved as a filter previously.

Related Topics

"Specifying Batch Search Filters" on page 190

"Viewing and Modifying Batch Search Filters" on page 192

"Displaying Batch Search Results" on page 193

"Locating and Fixing Batch Problems" on page 194

"Intelligent Capture Permissions List" on page 381

9.9.15.3 Viewing and Modifying Batch Search Filters

The **Batch Filters** pane displays a list of stored batch filters created by the user. A batch filter is a set of search criteria entered in the **Advanced Search** window.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view and modify batch search filters:

1. In the **Intelligent Capture Administrator** window, select **Batch Finder** from the navigational panel. The **Batch Finder** panel displays below the navigation panel.
2. Select **Filters** from the **Batch Finder** panel. The **Batch Filters** pane displays a list of the stored batch filters created by the current user.
3. Select a batch filter from the list of filters.
4. Click the appropriate button:
   - **View Results**: Apply the filter to the current set of batches and display the results.
   - **Add**: Opens the **Batch Finder - (Copy of filter name)** pane to enable the user to create a filter.
   - **Save As**: Creates a Copy of the selected filter and displays it in the **Batch Finder - Copy of <filter name>** pane.
   - **Settings**: Displays the batch filter settings for the selected filter.
   - **Delete**: Deletes the selected filter.

Related Topics

"Specifying Batch Search Filters" on page 190

"Displaying Batch Search Results" on page 193

"Intelligent Capture Permissions List" on page 381

"Viewing and Modifying Batch Search Filters" on page 192

9.9.15.4 Displaying Batch Search Results

The **Batch Finder Results** pane displays the results of a batches search.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view batch search results:

1. In the **Intelligent Capture Administrator** window, select **Batch Finder** from the navigational panel. The **Batch Finder** panel displays below the navigational panel.
2. Select **Last Results** from the **Batch Finder** panel. The batch search results are displayed in the **Batch Finder Results**. The search results can be from a simple search, or an applied filter, whichever was used last. The results displayed include:
   - *Batches table (top table)*: Displays the list of batches.
   - *Chart*: Displays the installed processes or module steps in a process depending on the user's selection.
   - *Modules table (lower right area in the right pane)*: Displays the modules connected for all installed processes or specific processes depending on the user selection.

   Note: For more information about this pane and how the tables displayed interact with each other, see "Understanding the Components of the Batch Traffic Pane" on page 164.

Related Topics

"Specifying Batch Search Filters" on page 190

"Viewing and Modifying Batch Search Filters" on page 192

"Locating and Fixing Batch Problems" on page 194

"Customizing Information Tables Using the Column Manager" on page 112

"Intelligent Capture Permissions List" on page 381

9.9.16 Locating and Fixing Batch Problems

In Intelligent Capture Administrator, use the **Admin Review** pane to display batches with errors or holds.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To locate and fix batch problems:

1. In the **Intelligent Capture Administrator** window, select **Admin Review** from the navigational panel. The **Admin Review** pane displays all the batches that are in an error or hold state. If there are no batches with errors or on holds an error message displays.

   Note: A list of all the processes on the Intelligent Capture Server displays in the **Admin Review** panel on the bottom left of the navigational panel.

2. The results are displayed in the right pane of **Admin Review**. The right pane has three views:

   - **Batches table (top table)**: Displays the list of batches that have a status of error or hold.
   - **Chart**: When no processes or batches are selected, displays all processes. When a process or batch is selected, displays the steps associated with the selection. The bars on the chart provide quantitative data for the displayed processes or steps:
     - **Red hatch bar**: Count of batches in error, hold, or priority 0. Count of tasks in error.
     - **Gray bar**: Count of batches or tasks in ready, working, or sent status.
     - **White bar**: Count of batches or tasks with any status other than the statuses represented by the Red hatch bar and the Gray bar.

     Note: This chart displays processes or module steps information for all processes, not just those processes associated with batches that are in error or hold.
   - **Modules table (bottom table)**: Displays the connected modules for all installed processes when no batch is selected, or the connected modules associated with the selected batch. This shows all data for the displayed module, not just the steps from the selected batch. Right-click a module to view additional information, disconnect the module, or refresh the module list.

     Note: For more information about this pane and how the panes interact with each other, see "Understanding the Components of the Batch Traffic Pane" on page 164.

3. To fix errors and holds double-click a batch. The **Batch Settings** window displays.
4. Clear the **Hold** and **Error** check boxes under the **Status** field.
5. Click **Apply**.

Related Topics

"Retriggering a Batch Step" on page 195

"Customizing Information Tables Using the Column Manager" on page 112

"Viewing All Batches for a Process, Module, or Server" on page 196

"Intelligent Capture Permissions List" on page 381

9.9.17 Retriggering a Batch Step

Intelligent Capture Administrator enables you to retrigger a specific module step in a batch.

Note: Depending on your permissions, some of these options might be disabled in Intelligent Capture Administrator.

1. In **Intelligent Capture Administrator**, select **Batch Traffic** from the navigation panel.
2. In the **Batch Traffic** pane, select one or more batches with the module steps that need to be retriggered.
3. Right-click the module step displayed in the bottom left of the pane and select **Retrigger**.

   If the step has tasks in error, select **Clear Task Errors**. You might also need to select **Retrigger**.

Note: You can also double-click the batch with the module step that needs to be retriggered to display the **Batch Settings** pane. In that pane, select **Steps** from the **View** list box, and then in the **Batch Steps** pane, right-click a step and select **Clear Task Errors** or **Retrigger** as appropriate.

Related Topics

"Viewing All Batches in the System" on page 166

"Viewing Batches for a Specific Installed Process" on page 168

"Viewing and Unlocking Locked Nodes on a Batch" on page 180

9.9.18 Viewing All Batches for a Process, Module, or Server

You can view the list of batches

- Associated with a specific process.
- That have a specific module step in the process.
- That are processed on a specific Intelligent Capture Server.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view the batches for a specific process, module, or server:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Select one of the following options from the **Systems** pane:
   - **View Processes**: Displays the **Processes** pane and lists all installed processes.
   - **View Modules**: Displays the **Modules** pane and lists all installed modules.
   - **View Servers**: Displays the **Servers** pane and lists all Intelligent Capture Servers in the system.
3. Right-click a specific process, module, or server from the displayed pane and select **View Selected > Batches**. The **Batches** list displays the batches for the process, module, or server.

   For an explanation about the columns in the list, see **Batch Traffic** , specifically the “Available columns in the batches table” section in the table.

Related Topics

“Viewing All Batches in the System” on page 166

“Viewing Batches for a Specific Installed Process” on page 168

“Exporting a Batch” on page 181

“Configuring a Batch Step in Setup Mode” on page 169

“Moving a Batch” on page 182

“Copying Step, Process, and Batch Settings” on page 197

“Intelligent Capture Permissions List” on page 381

9.10 Copying Step, Process, and Batch Settings

Intelligent Capture Administrator enables you to copy settings from one step, process, or batch to another. You can directly copy settings and then paste them to the target. Or, you can save settings to a text file and load them into a step, process, or batch file later.

When copying settings, the following conditions apply:

- Step settings of a module can only be copied to another step of the same module.
- When copying process or batch settings to another process or batch, the target process or batch must have equal numbers of module steps with the same step names.
- If you copy settings from a process or batch that has not yet been configured to one that has been configured, the settings for the two will not be identical. (The target will contain more setup values because the server adds values to processes and batches when they are first configured.)
- If you want to revert to the default settings for a module, create a batch or install a new process. (Copying the settings from a process or batch that has never been set up may not result in the default settings due to the added values mentioned in the previous bullet point.)
- Interdependent module settings, such as tree view configurations and level definitions, are not copied when copying a step.

9.10.1 Saving and Loading the Process Settings of a Batch

The process settings of a batch can be saved to a text (TXT) file. These saved settings can then be loaded into other batches.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To save the process settings of a batch:

1. In the **Intelligent Capture Administrator** window, select **Batch Traffic** from the navigation pane. The **Batch Traffic** pane displays a list of all batches in the system.
2. Select a batch, right-click and select **Batch Process Settings > Save Settings to File**. The **File Download** window displays and click **Save**.
3. Browse to the folder where you want to save the file, type the **File name** of the text file you want to save, and then click **Save**. The process settings of the file are saved to the text file.

You can load the saved process settings of a batch into other batches or processes that have the same set of steps as the saved process.

To load the saved process settings of a batch to another batch:

1. From the **Batch Traffic** pane, select the batch(es) to load the process settings into, right-click and select **Batch Process Settings > Load Settings from File**. The **Upload From a File** window displays.
2. Click **Browse** to locate the text file that contains the process settings you want to load, and then click **OK**. The process settings are saved to the target batch(es).

Related Topics

"Copying and Pasting Process Settings from a File" on page 198

"Copying Processes to Other Servers" on page 200

"Viewing Batches for a Specific Installed Process" on page 168

"Copying Process or Batch Settings" on page 201

"Intelligent Capture Permissions List" on page 381

9.10.2 Copying and Pasting Process Settings from a File

Process settings can be saved to a text file. These saved settings can then be loaded into other processes.

Note: Documentum Advanced Export only: These copying and loading procedures are not available for duplicate processes containing Documentum Advanced Export steps. When pasting settings using these procedures, `Docbase` login errors and problems loading settings may occur.

This function is only available for processes created using Process Developer. For more information, see the **Legacy** column description in "Processes" on page 278.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To copy process settings to a text file:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Processes**. The **Processes** pane displays the list of processes added to the system.
3. Select a process, right-click and select **Copy > Settings to File**. The **File Download** window displays.
4. Click **Save**. The **Save As** window displays, click **Save** and the process settings are saved to the text file.

You can load the saved process settings into other processes.

To load the saved process settings to other processes:

1. In the **Processes** pane, select the process(es) to load the process settings into, right-click and select **Paste > Settings from File**. The **Import Process Settings** window displays.
2. Click **Browse** to locate the text file that contains the process settings you want to paste, and then click **OK**. The process settings are saved to the target process(es).

Related Topics

"Saving and Loading the Process Settings of a Batch" on page 197

"Copying Processes to Other Servers" on page 200

"Viewing Batches for a Specific Installed Process" on page 168

"Copying Process or Batch Settings" on page 201

"Intelligent Capture Permissions List" on page 381

9.10.3 Copying a Process to a File

You can copy a process to a file.

This function is only available for processes created using Process Developer. For more information, see the **Legacy** column description in "Processes" on page 278.

To copy a process to a file:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Processes**. The **Processes** pane displays the list of processes added to the system.
3. Select the process to copy, right-click and select **Copy > Copy Process to File**. The **File Download** window displays.
4. Select **Find** to open the file or**Save** to save the file.

Related Topics

"Saving and Loading the Process Settings of a Batch" on page 197

"Copying and Pasting Process Settings from a File" on page 198

"Viewing Batches for a Specific Installed Process" on page 168

"Copying Process or Batch Settings" on page 201

"Intelligent Capture Permissions List" on page 381

9.10.4 Exporting Processes to a Zip File

To help automate the deployment of processes, you can use `XppCompile.exe` to export a specific version of a process to a zip file. `XppCompile.exe` exports a process (as well as their associated code-behind script DLLs and step settings) from Intelligent Capture Designer and packages them into a zip file. You can then use `BatchCopyCmd.exe` to import the zip file into Intelligent Capture Server. You can later change the capture flow or process settings and create different versions of processes, and these changes are compiled into new zip files, which enables customers to automate the procedure of deploying different versions of processes.

Notes

- The `XppCompile.exe` utility does not require a connection to the Intelligent Capture Server.
- For information on using the `XppCompile.exe` utility, see the command line help.
- By default, this utility is located in `C:\Program Files (x86)\InputAccel\Client\binnt\`.
- When started without any parameters (or without mandatory parameters), the utility displays information about how to use the parameters, and then terminates.

9.10.5 Copying Processes to Other Servers

Processes can be copied to servers within the same or different systems.

`BatchCopyCmd.exe` is used to copy processes to servers in other systems. By default, this utility is located in `C:\Program Files (x86)\InputAccel\Client\binnt\`. To help automate the deployment of processes, `BatchCopyCmd.exe` can import processes packaged in zip files that were created by `XppCompile.exe`.

Use the following procedure to copy one or more processes to other servers in the same system.

This function is only available for processes created using Process Developer. For more information, see the **Legacy** column description in "Processes" on page 278.

To copy processes to other servers:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Processes**. The **Processes** pane displays the list of processes added to the system.
3. Select the process(es) to copy, right-click and select **Copy > Process**. The **Copy Process** window displays.

4. The **Servers Available** list box lists all the servers in the system. Select the target servers to copy the process(es) to and click **>** or click **>>** to select all the servers. The selected servers are listed in the **Servers Selected** list box.

5. Click **OK** to copy the processes to the servers listed in the **Servers Selected** list box.

9.10.6 Copying Process or Batch Settings

Process settings can be copied and then pasted into other processes or batches.

Note: This function is only available for processes created using Process Developer. For more information, see the **Legacy** column description in "Processes" on page 278.

Batch settings can also be copied and then pasted into other processes or batches.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To copy process or batch settings:

1. In the **Intelligent Capture Administrator** window, select one of the following from the navigation panel:

   - **Systems**: Displays the **Systems** pane. Click **View Processes** to display the **Processes** pane which lists all installed processes.
   - **Batch Traffic**: Displays the **Batch Traffic** pane and lists all batches.

2. Select the process or batch from which you want to copy settings, right-click and select **Copy > Settings**. The process or batch settings are copied.

You can paste the copied settings into other processes or batches.

To paste the copied process or batch settings to other processes or batches:

1. Select the process(es) or batch(es) to which you want to paste settings.

2. Right-click and select **Paste > Settings**. The process or batch settings are pasted to the selected processes or batches.

Related Topics

"Saving and Loading the Process Settings of a Batch" on page 197

"Copying and Pasting Process Settings from a File" on page 198

"Viewing Batches for a Specific Installed Process" on page 168

"Copying Process or Batch Settings" on page 201

"Intelligent Capture Permissions List" on page 381

9.10.7 Copying Indexed Values to a File

You can copy indexed values or setting from a selected process to a file.

To copy indexed values to a file:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Processes**. The **Processes** pane displays the list of processes added to the system.
3. Select the process to copy the index values from, right-click and select **Copy > Indexed Values to File**. The **File Download** window displays.
4. Click **Open** to open the file or**Save** to save the file.

9.10.8 Copying Indexed Values

You can copy indexed values.

To copy indexed values:

1. In the **Intelligent Capture Administrator** window, select **Systems** from the navigation panel. The **Systems** pane displays.
2. Click **View Processes**. The **Processes** pane displays the list of processes added to the system.
3. Select the process to copy the indexed values from, right-click and select **Copy > Indexed Values**. The process or batch indexed values are copied.

You can paste the copied settings into other processes or batches.

To paste indexed values:

1. Select the process(es) or batch(es) to which you want to paste the copied indexed values.
2. Right-click and select **Paste > Indexed Values**. The process or batch indexed values are pasted to the selected processes or batches.

9.10.9 Copying and Pasting a Single Process or Batch Setup Value

You can copy a single process or batch setup value and then paste the setup value to other processes or batches. Setup values are created when a process or batch step is configured for setup.

This function is only available for processes created using Process Developer. For more information, see the **Legacy** column description in "Processes" on page 278.

Note: Some setup values are related to other setup values and all the values must be copied in order for the process or batch to work properly. Since only one setup value can be copied at a time, it is best to avoid copying setup values that are dependent upon other setup values for the process or batch to work.

To copy a single process or batch setup value:

1. In the **Intelligent Capture Administrator** window, select one of the following from the navigation panel:
   - **Systems**: Displays the **Systems** pane. Click **View Processes** to display the **Processes** pane which lists all installed processes
   - **Batch Traffic**: Displays the **Batch Traffic** pane and lists all batches
2. Select the process or batch with the setup value you want to copy, right-click, and select **Copy > Single Setup Value**. The **Single Setup Value** window displays.
3. Select the value to copy and click **OK**.

You can paste the copied setup value to other processes and batches.

To paste a single process or batch setup value:

1. Select the process(es) or batch(es) to which you want to paste the single setup value.
2. Right-click and select **Paste > Single Setup Value** to paste the setup value.

Related Topics

"Saving and Loading the Process Settings of a Batch" on page 197

"Copying and Pasting Process Settings from a File" on page 198

"Copying Processes to Other Servers" on page 200

"Viewing Batches for a Specific Installed Process" on page 168

"Copying Process or Batch Settings" on page 201

"Intelligent Capture Permissions List" on page 381

9.10.10 Copying and Replacing Batch IA Values on the Server

Batch IA Values of file type can be copied from and replaced on the Intelligent Capture Server.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To copy IA Values from the server to a file:

1. In the **Intelligent Capture Administrator** window, select **Batch Traffic**. The **Batch Traffic** pane displays.
2. Double-click a batch to display the **Batch Settings** pane and select **Values** from the **View** list box. The **Batch Values** pane displays.
3. Select an IA Value of "file" type (the type is displayed in the **Value Type** column), right-click and select **Copy File from Server**. The **Save Web Page** window displays.
4. Browse to the folder where you want to save the file to, type the **File name** of the file to be copied, and then click **Save**.

IA Values of type "file" can be replaced on the Intelligent Capture Server.

To replace IA Values on the server:

1. From the **Batch Values** pane, select an IA Value of type "file" (the type is displayed in the **Value Type** column), right-click and select **Replace File on Server**. The **Browse** window displays.
2. Locate the file to replace and replace the existing file on the server.

Related Topics

"Saving and Loading the Process Settings of a Batch" on page 197

"Copying and Pasting Process Settings from a File" on page 198

"Copying Processes to Other Servers" on page 200

"Viewing Batches for a Specific Installed Process" on page 168

"Copying Process or Batch Settings" on page 201

"Intelligent Capture Permissions List" on page 381

9.11 Managing Reports and Logs

Intelligent Capture Administrator provides logging and reporting functionality for all Intelligent Capture modules and components, as well as system components. This covers reporting, monitoring, and measurement of the quality, performance, and overall state of the software by recording key elements in module execution, and creating logs for auditing, error and warning, statistics and debugging. Administrators control when, where and how logs are written. Custom module developers can also use the same mechanism for logging within their custom modules.

Notes

- The Reporting functionality is available only for users that install the Intelligent Capture Database.
- Some database permissions are not controlled from Intelligent Capture Administrator. Insufficient database access rights for a user may block some database operations specifically related to reports, logs, and purges. For more information on database permissions, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

Administrators specify which reports are needed, specify the parameters to pass to the stored procedures that run the report. For more information on stored procedures, see "Creating or Modifying a Report Definition" on page 233.

Monitoring of Intelligent Capture is based on logs, log view filters, log rules, and reports.

- Logs are kept by the system to note when specific events or actions have occurred. Logs are written only when the appropriate log rules are enabled.
- Log view filters limit display of logs to a subset based on specific viewing criteria.
- Log rules control the type of logs produced and define what types of logs are created, where they are written, and how they are formatted. When an event occurs that matches a log rule, the rules are used to prepare the log and send it to the defined destination, often referred to as the sink in Intelligent Capture Administrator. Log rules need to be enabled before the logs are written to the sink.
- Reports are based on report definitions that define the parameters that are used to run the report. Reports are generated by sending a request from Intelligent Capture Administrator to the Intelligent Capture Database. Report output is displayed on-screen, and can be output to a display, printer, or file system.
- Purges enable clearing of data from the system. Purges can be configured and scheduled from Intelligent Capture Administrator.

9.11.1 Managing Logs

Logs are kept by Intelligent Capture to indicate when specific actions or events have occurred, including, but not limited to, errors, audits, statistics, performance, and debug information.

9.11.1.1 Understanding Logs

Logs form the basis for Intelligent Capture reports, and are kept by the system to note when specific events or actions have occurred. System logs can be viewed from the **Logs** pane. The logs view can be limited using log view filters. Filters can be general filters, limiting log display to, for example, view of only error logs, or can be custom filters defined by the user. Custom filters can limit the view of logs based on several categories, such as errors, warnings, and audits. Log filters can further refine the view based on date/time, processes and batches, and workstations and servers.

Logs are built on these components:

- The Logging Library coordinates evaluation and writing of errors, auditing, and statistics. This determines what information will be written and to what location.
- Statistics logging is done by the Intelligent Capture Server. Statistics are sent from the modules to the Intelligent Capture Server as IA Values. Statistics logging allows generation of reports that can help in making key Intelligent Capture operation decisions.

Management of logs is accomplished with log rules. Log rules define the type of logs, how logs are formatted, and when and where logs are written. Manipulation of log rules is controlled with security permissions, so not every user has access to modify log rules.

There are two general types of log rules:

- System logging rules are an inherent part of Intelligent Capture and cannot be modified. However, they can be enabled or disabled. System logging rule descriptions help in when deciding when to enable or disable a rule. All system log rules are disabled by default.
- Custom logging rules are user defined rules that can be created, modified, deleted, enabled, or disabled if the appropriate permissions are granted.

Note: The logging subsystem cannot log client module events until a client module successfully connects to an Intelligent Capture Server. Therefore, errors that when a client module is not connected are instead written directly to the Windows Event Log. For example, if an invalid department name is specified, the client log in does not complete; therefore, the logging system cannot log the error. Instead, the client module writes the error to the Windows Event Log.

Related Topics

"Understanding Log Rules" on page 215

"Understanding Log View Filters" on page 212

"Understanding Report Definitions" on page 232

"Managing Reports and Logs" on page 205

9.11.1.2 Understanding Log Types

Logs are kept by the system to note when specific events or actions have occurred. Several log types are available.

- **Error** logs report any error that occurs.
- **Warning** logs report events that are either suspicious in nature, or may cause a significant degradation in performance.
- **Audit** logs report important informational events that have occurred in the system but are not related to errors.
- **Debug** logs are intended for use when troubleshooting problems in a module or component and by default are not activated. Debug logs record detailed information to find the cause of a problem. A custom log rule must be created to start recording debug messages.
- **Statistics** logs are used for the reports that are shipped with Intelligent Capture.

Notes

- Purging operations are not logged, specifically when table content is modified or deleted.
- Debug and Warning logs are not supported for modules new in 7.0.

Related Topics

"Exporting Logs" on page 211

"Logs" on page 300

"Understanding Logs" on page 206

"Viewing a List of Logs" on page 208

"Viewing Log Details" on page 209

9.11.1.3 Viewing a List of Logs

Logs are kept by the system to note when specific events or actions have occurred. The list of logs is available from the **Reports / Logs** pane of the **Intelligent Capture Administrator** window. The entire list of logs can be viewed, or a partial list based on log view filters can be displayed. For information on limiting the list of logs, see "Creating a Log View Filter" on page 213.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view the list of logs:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Logs** from the **Reports / Logs** pane.
3. In the **Logs** pane, logs are listed by the **Log Type** (**All**, **Error/Warning**, **Audit**, or custom filters). Select type of logs to view from the **Filter** list box.

   All logs of the selected type are displayed. If there are several pages of logs of the selected type, the number of pages of logs is displayed.

   Notes

   - The **Batch Name** column does not display the name of the batch, but instead displays the name of the process on which the batch is based. This column might not be displayed.
   - In a log rule, if information messages (indicated by selecting **FilterAllDebugInfos** from the **Filter definition** list) are logged to **AuditToDBSink**, **ErrorToDBSink**, or **GeneralEventLogSink**, then the **Logs** pane will not display all the log messages.

Related Topics

"Deleting Logs Manually" on page 210

"Exporting Logs" on page 211

"Logs" on page 300

"Setting the Log Refresh Rate" on page 212

"Understanding Log Types" on page 207

"Understanding Logs" on page 206

"Viewing Log Details" on page 209

"Intelligent Capture Permissions List" on page 381

9.11.1.4 Viewing Log Details

Logs are kept by the system to note when specific events or actions have occurred. Display of the specific details of a log shows the parameters applied for the selected log.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view log details:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Logs** from the **Reports / Logs** pane.
3. In the **Logs** pane, logs are listed by type (**All**, **Error/Warning**, **Audit** or any user defined custom log filters). Click the **Filter** list box and select the type of log to view. All the logs of the selected type are displayed. The number of pages of logs is displayed.
4. Select a log and click **Details**, or double-click a log to display the **Log Details** window. The **Log Details** table displays the settings for the selected log, and the bottom pane displays a **Log Message** associated with the specific log entry. Clicking **Previous** or **Next** displays the log details for the adjacent logs in the filtered view on the **Logs** pane.

   Note: If two or more logs are selected, the **Log Details** window will only provide details for the first selected log.

Note: The logging subsystem cannot log client module events until a client module successfully connects to an Intelligent Capture Server. Therefore, errors that when a client module is not connected are instead written directly to the Windows Event Log. For example, if an invalid department name is specified, the client log in does not complete; therefore, the logging system cannot log the error. Instead, the client module writes the error to the Windows Event Log.

Related Topics

"Deleting Logs Manually" on page 210

"Exporting Logs" on page 211

"Logs" on page 300

"Understanding Logs" on page 206

"Understanding Log Types" on page 207

"Viewing a List of Logs" on page 208

"Intelligent Capture Permissions List" on page 381

9.11.1.5 Deleting Logs Manually

When viewing the list of logs, one or more logs can be deleted.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To clear a single log, selected logs, or the entire log list:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Logs** from the **Reports / Logs** pane.
3. Select the type of logs to display using the **Filter** list box to select **All**, **Error/ Warning**, **Audit**, or any defined custom log filters.
4. To delete individual or specific groups of logs, select them from the log list. Use the **CTRL** or **SHIFT** keys to make multiple selections. If deleting all logs, selection is not necessary.
5. Click **Delete** to delete the selected logs. To delete all logs, right-click in the log list, and the context menu displays. Select **Delete All**. If there are multiple pages of logs, they will all be deleted.

Related Topics

"Exporting Logs" on page 211

"Setting the Log Refresh Rate" on page 212

"Understanding Log Types" on page 207

"Understanding Logs" on page 206

"Viewing a List of Logs" on page 208

"Intelligent Capture Permissions List" on page 381

9.11.1.6 Exporting Logs

Exporting logs is a way to preserve records of logs for viewing at a later time. Exporting logs is useful, for example, if the log view is to be cleared but you want to keep a record of the logs. Exporting logs allows creation of text files.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To export a single log, selected logs, or the entire log list:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Logs** from the **Reports / Logs** pane.
3. Select the type of logs to display, using the list box to select **All**, **Error/Warning**, **Audit**, or any defined custom log view filters.
4. To export individual or specific groups of files, select them from the log list. Use the **CTRL** or **SHIFT** keys to make multiple selections. If exporting all logs, selection is not necessary.
5. Right-click in the log list, and the context menu displays. Select **Export Logs** and the **File Download** window displays.
6. Either click **Open** to view the log in a text editor, or click **Save** to save the log as a text file.

Related Topics

"Deleting Logs Manually" on page 210

"Logs" on page 300

"Understanding Log Types" on page 207

"Understanding Logs" on page 206

"Viewing a List of Logs" on page 208

"Viewing Log Details" on page 209

"Intelligent Capture Permissions List" on page 381

9.11.1.7 Setting the Log Refresh Rate

The refresh rate for log views is set in the **Default Settings** pane or the **My Preferences** pane. Default settings are overridden by custom settings.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To set the log refresh rate:

1. In the **Intelligent Capture Administrator** window, select **Options** from the navigation panel.
2. Select either **Default Settings** (for settings available for all users) or **My Preferences** (for settings specific to your work environment).
3. Under **Page Refresh Rates**, select **Logs** and set the **Default Refresh Rate** in **seconds**.
4. Click **OK** to save the values.

Related Topics

"Logs" on page 300

"Understanding Logs" on page 206

"Understanding Log Types" on page 207

"Viewing a List of Logs" on page 208

"Intelligent Capture Permissions List" on page 381

9.11.2 Managing Log View Filters

Log view filters are used to limit the log display to a subset of logs instead of all the logs in the system.

9.11.2.1 Understanding Log View Filters

Log view filters limit display to a subset of logs instead of all logs. The **Log View Filters** pane lists all saved log filters and enables creating, editing, and deleting of the log filters. If the log filters occupy more than one page, page numbers are displayed. Log view filters are provided with Intelligent Capture (**All**, **Error/ Warning**, and **Audit**) or users can create custom filters.

Related Topics

"Log View Filter Settings and Add Log View Filter" on page 325

"Log View Filters" on page 302

"Understanding Log Rules" on page 215

"Understanding Logs" on page 206

"Managing Reports and Logs" on page 205

9.11.2.2 Creating a Log View Filter

Log view filters restrict the list of logs displayed in the **Logs** pane. Filters can be defined by **Date/Time**, **Log Type and Codes**, **Processes and Batches**, and **Workstations and Modules**. Use any single option or combination of options when defining the filter. In the **Log View Filters** pane, the bottom section changes depending on the filter definition selected.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To create a log view filter:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Log View Filters** from the **Reports / Logs** pane. This displays the **Log View Filters** pane that lists all the currently defined log filters.
3. Click **Add** to create a log view filter, or select a filter from the list and click **Save As**. The **Add a Log View Filter** window displays.
4. Type a **Name** and optional **Description** for the filter.
5. From the **Filtering** list box, specify **Date/Time**, **Log Type and Codes**, **Processes and Batches**, or **Workstations and Modules** types (for more information, see**Log View Filter Settings**). When you select the various types, the **Settings** area of the window changes, enabling selection of the filter settings. Select the settings for the selected log view filter, and repeat the process to define any combination of settings you want to apply to the filter.
6. Click **OK** and the new log view filter is displayed in the **Log View Filters** pane.
7. Select a filter and click **View Results**. The **Logs** pane displays with the results of the selected log filter.

Note: After you have created a log filter, it becomes available on the **Logs** pane. Click the **Filter** box and select the log filter from the list.

Related Topics

"Log View Filter Settings and Add Log View Filter" on page 325

"Log View Filters" on page 302

"Understanding Log View Filters" on page 212

"Viewing Log View Filter Results" on page 214

"Intelligent Capture Permissions List" on page 381

9.11.2.3 Viewing Log View Filter Results

Log view filter results can be viewed from either the **Logs** pane or the **Log View Filters** pane.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view log filter results:

- In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel. Either:

  a. Select **View Logs** from the **Reports / Logs** pane. Select **Filter** and specify the preferred log view filter. The **Logs** pane displays the results of the selected log view filter.

  b. Click **View Log View Filters** from the **Reports / Logs** pane. Select a filter and click **View Results**. The **Logs** pane displays with the results of the selected log view filter.

Related Topics

"Creating a Log View Filter" on page 213

"Log View Filter Settings and Add Log View Filter" on page 325

"Log View Filters" on page 302

"Understanding Log View Filters" on page 212

"Intelligent Capture Permissions List" on page 381

9.11.3 Managing Log Rules

Log rules define the types of logs created, when they are created and the messages they log, where they are written, and how they are formatted. Log rules are user customizable from Intelligent Capture Administrator.

9.11.3.1 Understanding Log Rules

Log rules define the types of logs created, where they are written, and how they are formatted. When an event occurs that matches a log rule, the rules are used to prepare the log and send it to the defined sink. The sink then prepares the data and sends it to its destination. If the event does not match a log rule, the log is ignored. Not all aspects of System log rules can be changed, although you can make a copy of a system log rule and modify the copy. All logs created can be viewed through the **Logs** pane in Intelligent Capture Administrator.

Note: When too many log rules have to be evaluated at runtime, performance may suffer.

There are two general types of log rules:

- System log rules are an inherent part of Intelligent Capture and cannot be modified. All system log rules are disabled by default. System log rules are listed in "System Log Rules" on page 387.
- Custom log rules are created and modified by users that are granted the appropriate permissions. Custom log rules can be created based on an existing rule or can be created as a completely new rule.

There are several aspects to log rules, and these can be user defined for custom log rules:

- **Scope component** defines the module or service that is logging the event. If **Scope component** is empty, the rule applies to events logged by all modules and services.
- **Scope user** defines the user executing the module or service that is logging the event. If **Scope user** is empty, the rule applies to all modules or services that match **Scope Component** run by any user.
- **Scope workstation** defines the workstation on which the module or service that is logging the event is running. If **Scope workstation** is empty, the rule applies to all modules or services that match **Scope Component** running on any workstation.

  Note: Each of the scope fields may contain one value only or they may remain empty. A combination of different scope settings can be used. So, for example, a rule where **Scope component** is <*ModuleX*>, **Scope user** is blank and **Scope workstation** is blank would apply to all running steps of <*ModuleX*> regardless of which user is executing them or which workstation they are running on.

- **Log Rule Filter Definitions** indicate the events that determine when the log is written.
- **Log Data Definitions** indicate what additional data to pass with the log.
- **Sink Definitions** indicate where the log will be written.

Note: Log rules indicate whether a log should be sent or not. Excluded entries always take precedence over non-excluded entries regardless of the order of the entries.

Related Topics

"Log Rule Data Definition Settings" on page 318

"Log Rule Settings and Add Log Rule" on page 323

"Log Rule Filter Definition Settings and Add Log Rule Filter Definition" on page 319

"Log Rules" on page 303

"Understanding Log View Filters" on page 212

"Managing Reports and Logs" on page 205

9.11.3.2 Viewing Log Rules and Log Rule Settings

The **Log Rules** pane displays a list of all log rules registered in the system.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view log rules:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Log Rules** and the **Log Rules** pane displays.
3. From the **Filter** list box, select **All**, **System**, or **Custom**. The list of log rules matching the filter is displayed.
4. To view settings for a specific log rule, select it from the list and click **Settings**. The **Log Rule Settings** pane displays. For **System** log rules, this displays the settings, but does not allow modification of the settings. Custom log rules can be modified from this location.

Related Topics

"Creating or Copying a Log Rule" on page 219

"Defining Log Rule Filter Definitions" on page 221

"Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218

"Log Rule Data Definition Settings" on page 318

"Log Rule Filter Definition Settings and Add Log Rule Filter Definition" on page 319

"Log Rule Settings and Add Log Rule" on page 323

"Log Rules" on page 303

"Understanding Log Rules" on page 215

"Viewing Log Rule Settings" on page 217

"Intelligent Capture Permissions List" on page 381

9.11.3.3 Viewing Log Rule Settings

Log rule settings are the specific criteria set for the log rule. Log rule settings include:

- **Name** and **Definition**.
- **Status** specifies whether to evaluate or eliminate the data generated by the rule.
  - **Enabled** - The rule will be evaluated when a log is sent to the logging library.
  - **Block logs that meet these criteria** - If selected, any log sent to the logging library that matches this criteria will not be written even if it also matches other log rules that are enabled. **Enabled** must be selected for this option to be available.
- **Scope component** defines the module or service that is logging the event.
- **Scope user** defines the user executing the module or service that is logging the event.
- **Scope workstation** defines the machine on which the module or service that is logging the event is running.
- **Filter definition** indicate which events cause a log to be written.
- **Data definition** indicate what additional data to pass with the log.
- **Sink definition** indicate where the log will be written.

Note: In a log rule, if information messages (indicated by selecting **FilterAllDebugInfos** from the **Filter definition** list) are logged to **AuditToDBSink**, **ErrorToDBSink**, or **GeneralEventLogSink**, then the **Logs** pane will not display all the log messages.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view log rule settings:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.

2. Select **View Log Rules** and the **Log Rules** pane displays.
3. In the **Log Rules** pane, select **All**,**System**, or **Custom** from the **Filter** list box. The log rules of the selected type display.
4. From here you have two options:
   a. Double-click the log rule or right-click and select **Settings** from the context menu to display the **Log Rule Settings** pane for the selected log rule. From here, you can evaluate the **Scope components**, **Scope users**, or **Scope workstations**. Also, click **Settings** for the **Data definition**, **Filter definition** or **Sink definition** settings.
   b. To review the **Data definition**, **Filter definition** or **Sink definition** settings, click the appropriate **Settings** button, or right-click the log rule to be evaluated. Select one of the options from the **View Selected** menu in the context menu.

Related Topics

"Creating or Copying a Log Rule" on page 219

"Defining Log Rule Filter Definitions" on page 221

"Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218

"Log Rule Settings and Add Log Rule" on page 323

"Log Rules" on page 303

"Understanding Log Rules" on page 215

"Viewing Log Rules and Log Rule Settings" on page 216

"Intelligent Capture Permissions List" on page 381

9.11.3.4 Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules

Enabling, disabling log rules, and blocking logs that meet log rule criteria is accomplished from the **Log Rule Settings** and **Add Log Rule** windows.

Blocking log rules can be used to override subordinate rules. For example, if four enabled rules log information for ModuleX, you can create one rule to block all logs from ModuleX, rather than finding and blocking all the rules individually. To enable the rules again, just disable the blocking rule.

Note: By default, all system log rules are disabled. Log rules must be enabled to log the required data.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To enable, disable or block a rule:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Log Rules** and the **Log Rules** pane displays.
3. From the **Filter** list box, select **All**, **System**, or **Custom**. The **Log Rules** pane displays the list of log rules specified.
4. To view settings for a specific log rule, select it from the list and click **Settings**. The **Log Rule Settings** pane displays.
5. Select **Enabled** to use the log rule. Clear **Enabled** to disable the option.
6. To block groups of logs that use the same criteria, select **Enabled** and **Block logs that meet these criteria**.

Related Topics

"Creating or Copying a Log Rule" on page 219

"Defining Log Rule Filter Definitions" on page 221

"Log Rule Settings and Add Log Rule" on page 323

"Log Rules" on page 303

"Understanding Log Rules" on page 215

"Viewing Log Rule Settings" on page 217

"Viewing Log Rules and Log Rule Settings" on page 216

"Intelligent Capture Permissions List" on page 381

9.11.3.5 Creating or Copying a Log Rule

Creation of new rules can be accomplished by creating an entirely new rule where all settings are customized, or by copying an existing rule and modifying only some of the copied parameters.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To create a rule or copy a rule for use in creating a rule:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Log Rules** and the **Log Rules** pane displays.
3. From the **Filter** list box, select **All**, **System**, or **Custom**. The **Log Rules** pane displays the list of log rules specified.

4. To create a rule, click **Add**. Alternatively, select a rule and click **Save As** to modify the settings for the selected rule to create a rule. The **Add Log Rule** pane displays.
5. Type a **Name** and optional **Description** for the rule.
6. Select the options for Enabling, disabling, or blocking logs that meet these criteria.
7. Specify the **Scope component**, **Scope user**, and **Scope workstation** parameters. Scope parameters limit the log to the specified component, user, or workstation.

   Note: Each of the scope fields may contain one value only or they may remain empty. And a combination of different scope settings can be used. So, for example, a rule where **Scope component** is <*ModuleX*>, **Scope user** is blank and **Scope workstation** is blank would apply to all running steps of <*ModuleX*> regardless of which user is executing them or which workstation they are running on.

8. Select a **Filter definition** that defines when to create a log. Click **Add** to create a filter definition from the **Add Log Rule Filter Definition** window.
9. Select a **Data definition** that defines what additional data to include with the log. Click **Add** to create a data definition from the **Log Rule Data Definition Settings** window.
10. Select a **Sink definition** that defines the configuration of a log sink. This includes where the log will be written and how it will be written including any connection information and the format of the log output. Click **Add** to create a sink definition from the **Logging Rule Sink Definition** window.

    Notes

    - In a log rule, if information messages (indicated by selecting **FilterAllDebugInfos** from the **Filter definition** list) are logged to **AuditToDBSink**, **ErrorToDBSink**, or **GeneralEventLogSink**, then the **Logs** pane will not display all the log messages.
    - Predefined system **Filter definitions**, **Data definitions**, or **Sink definitions** cannot be changed or deleted. User created **Filter definitions**, **Data definitions**, or **Sink definitions** can be deleted, but only when they are not in use by any log rule. To delete user created definitions:
      - Open the log rules using the definitions to be deleted.
      - Select a different definition than the one to be deleted.
      - Save the log rule.
      - Edit any other log rule, select the definition to be deleted, and click delete.
      - Reset the correct definition for the open log rule and click **OK**.

11. Click **OK** to save the settings and add the log rule to the list of available log rules.

Related Topics

"Defining Log Rule Filter Definitions" on page 221

"Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218

"Log Rule Data Definition Settings" on page 318

"Log Rule Filter Definition Settings and Add Log Rule Filter Definition" on page 319

"Log Rule Settings and Add Log Rule" on page 323

"Log Rules" on page 303

"Log Rule Sink Definition" on page 329

"Understanding Log Rules" on page 215

"Viewing Log Rule Settings" on page 217

"Viewing Log Rules and Log Rule Settings" on page 216

"Intelligent Capture Permissions List" on page 381

9.11.3.6 Defining Log Rule Filter Definitions

Log rule filter definitions specify when an event is preserved in a log. This can be based on several factors, including the type of event, the processes or modules involved, and the workstations and users involved. Filter definitions can be specified when a log rule is created, or when editing an existing log rule. Log filters are modified or created from the **Log Rule Filter Definition Settings** window.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To define log rule filter definitions:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Log Rules**. From the **Log Rules** pane, click **Add** or select a log rule and click **Save As** or **Settings**. This displays the **Log Rule Settings** or **Add Log Rule** window.
3. By **Filter definition**, click **Add** or **Settings**. This displays the **Add Log Rule Filter Definition** or **Log Rule Filter Definition Settings** window. The Filter definition list box lists all the predefined and custom filter definitions. For a list of all system filter definitions, see "System Filter Definitions" on page 399.

4. Specify a **Name** and optional **Description** if creating a definition or leave them as is if modifying an existing definition.
5. Select either **Log Type and Codes**, **Processes and Modules**, or **Workstations and Users** from the **Setting** list box. The bottom part of the window changes to reflect the choice.
6. Specify the parameters for the **Setting** selection. Switch the **Setting** selection to make additional modifications to any of the needed filters.
7. When completed, click **OK** to preserve the settings and return to the previous pane.

Related Topics

"Creating or Copying a Log Rule" on page 219

"Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218

"Understanding Log Rules" on page 215

"Viewing Log Rule Settings" on page 217

"Viewing Log Rules and Log Rule Settings" on page 216

"Intelligent Capture Permissions List" on page 381

9.11.3.7 Defining Log Rule Filter for Log Type and Codes

The **Log Type and Codes** setting from the **Log Rule Filter Definition Settings** window is the primary point for log rule definition. This is where the type of log to be created is specified by editing filter name, description, and specifying log type, log codes and log categories for new or existing filter definitions.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To define a log rule filter for Log Type and Codes:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation pane.
2. Select **View Log Rules**. From the **Log Rules** pane, click **Add** or select a log rule and click **Save As** or **Settings**. This displays the **Log Rule Settings** or **Add Log Rule** window.
3. By **Filter definition**, click **Add** or **Settings**. This displays the **Add Log Rule Filter Definition** or **Log Rule Filter Definition Settings** window.
4. Select **Log Type and Codes** from the **Setting** list box.
5. Select the **Log type** from the list box.

- **Error**: Used to log errors.
- **Warning**: Used to log warnings that describe events that are either suspicious in nature, or may cause a significant degradation in performance.
- **Audit**: Used to log an important informational event that has happened in the system and not related to errors. To log Server events, choose the **Audit** Log Type.
- **Debug**: Used to log low-level developer debug messages.
- **Statistic**: Used for logging statistics. Statistics logs are identical to Audit logs except that they contain data specific to the execution of Intelligent Capture modules. All logging of statistics information is done by the Intelligent Capture Server, and the server reporting feature must be licensed for statistics to be available.

6. Select a log code from the **Log codes** list. This selection determines the code assigned to the event, such as an error code, warning code, or audit code. Select **Any** to choose all log codes.

   Notes

   - A complete list of client module error and log codes is listed in the *OpenText Intelligent Capture - Module Reference (ECPCORE-CMD)* section of the *OpenText Intelligent Capture - Module Reference (ECPCORE-CMD)*.
   - To log Server events, select the **Audit** log type and select the log code that corresponds to a Server event. For a list of log codes that correspond to server events, see "Intelligent Capture Server Events: Log Code Details" on page 469.

7. Select from the list of **Available Categories** and move them to **Selected Categories**. Categories are used by the modules to identify the area of execution being logged. If you selected a log code for a Server event in step 6, make sure you select the correct server event category. "Intelligent Capture Server Events: Log Code Details" on page 469 lists the category applicable to each server event log code.

8. When completed, click **OK** to preserve the settings and return to the **Log Rule Settings** or **Add Log Rule** pane.

Related Topics

"Specifying Log Rule Data Definitions" on page 227

"Defining Log Rule Filter Definitions" on page 221

"Defining Log Rule Filters for Processes and Modules" on page 224

"Specifying Log Rule Sink Definition" on page 228

"Defining a Log Rule Filter for Workstations and Users" on page 225

"Log Rule Settings and Add Log Rule" on page 323

"Understanding Log Rules" on page 215

"Intelligent Capture Permissions List" on page 381

9.11.3.8 Defining Log Rule Filters for Processes and Modules

The **Processes and Modules** setting from the **Log Rule Filter Definition Settings** window is where the processes, steps, and modules to be evaluated are specified.

- For processes, if the **Scope component** specified in the log rule is an Intelligent Capture module or the Intelligent Capture Server, a process can be added to the filter. This will limit the log to only events that happen when tasks for that process are being processed by the module or server. Specifying a process setting when the **Scope component** is not a module or the server, will result in the rule not matching any logs sent by the **Scope component**. Multiple processes can be specified.
- For modules, if the **Scope component** for the rule is the Intelligent Capture Server, the module setting will limit the log to only events sent by the Server when tasks from the module are logged. If Module is specified for Scope Components other than the Server, this setting will be ignored. Multiple modules can be specified.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To define log rule filters for Processes and Modules:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Log Rules**. From the **Log Rules** pane, click **Add** or select a log rule and click **Save As** or **Settings**. This displays the **Log Rule Settings** or **Add Log Rule** window.
3. By **Filter definition**, click **Add** or **Settings**. This displays the **Add Log Rule Filter Definition** or **Log Rule Filter Definition Settings** window.
4. In the **Log Rule Filter Definition Settings** window, select **Processes and Modules** from the **Setting** list box.
5. The **Available Processes** list is populated with all processes installed on the Intelligent Capture Server. Move processes to **Selected Processes** and this populates the list for the **Available Steps**.

   Note: If the selected process name is changed on the server after setting up the log rule filter, the filter will no longer be valid for that process.
6. Select from the **Available Steps** list and move them to the **Selected Steps** list. This property applies only to log rules for the Intelligent Capture Server or Intelligent Capture modules.

7. Select from the **Available Module Attributes** list and move them to the **Selected Module Attributes** list. This property applies only to rules for the Intelligent Capture Server when logging step events.
8. Select from the **Available Modules** list and move them to the **Selected Modules**. If no task module is specified, all task modules will match the rule.
9. Click **OK** to save the settings and return to the **Log Rule Settings** or **Add Log Rule** pane.

Related Topics

"Log Rule Settings and Add Log Rule" on page 323

"Understanding Log Rules" on page 215

"Defining Log Rule Filter Definitions" on page 221

"Defining Log Rule Filter for Log Type and Codes" on page 222

"Defining a Log Rule Filter for Workstations and Users" on page 225

"Specifying Log Rule Data Definitions" on page 227

"Specifying Log Rule Sink Definition" on page 228

"Intelligent Capture Permissions List" on page 381

9.11.3.9 Defining a Log Rule Filter for Workstations and Users

The **Workstations and Users** setting from the **Log Rule Filter Definition Settings** window is where the specific workstations and users to be evaluated are specified.

- For workstations:
  - If **Scope component** for the rule is the Intelligent Capture Server, the **Workstations** setting will limit the log to only events sent by the server when tasks from the modules running on the workstation are logged.
  - If **Workstation** is specified for **Scope components** other than the Intelligent Capture Server, this setting will be ignored. Multiple workstations can be specified.
- For users:
  - If the **Scope component** for the rule is the Intelligent Capture Server, the **Users** setting will limit the log to only events sent by the server when tasks from the modules executed by the user are logged.
  - If **User** is specified for **Scope component** other than the Intelligent Capture Server, this setting will be ignored. Multiple users can be specified and must be entered in the form domain\user.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To define a log rule filter for Workstations and Users:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Log Rules**. From the **Log Rules** pane, click **Add** or select a log rule and click **Save As** or **Settings**. This displays the **Log Rule Settings** or **Add Log Rule** window.
3. By **Filter definition**, click **Add** or **Settings**. This displays the **Add Log Rule Filter Definition** or **Log Rule Filter Definition Settings** window.
4. Specify a **Name** and optional **Description** if creating a definition or leave them as is if modifying an existing definition.
5. Select **Workstations and Users** from the **Setting** list box. The bottom part of the window changes to reflect the choice.
6. Type the **Workstations** names, separated by semicolons if more than one is specified.
7. Type the **Users** names, including the domain, separated by semicolons if more than one is specified.
8. Click **OK** to save the settings and return to the **Log Rule Settings** or **Add Log Rule** pane.

Related Topics

"Specifying Log Rule Data Definitions" on page 227

"Defining Log Rule Filter Definitions" on page 221

"Defining Log Rule Filter for Log Type and Codes" on page 222

"Defining Log Rule Filters for Processes and Modules" on page 224

"Log Rule Settings and Add Log Rule" on page 323

"Specifying Log Rule Sink Definition" on page 228

"Understanding Log Rules" on page 215

"Intelligent Capture Permissions List" on page 381

9.11.3.10 Specifying Log Rule Data Definitions

Data definitions specify additional data to pass with the log messages that apply to server events. A data definition can be specified when the **Scope component** for the rule is the Server, the **Log Type** selected when specifying the filter definition is **Audit**, and the **Log Code** specified is for numbers ranging from 1–192 because these log codes represent server events.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To specify log rule Data Definitions:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View All Log Rules** from the **Reports / Logs** pane.
3. From the **Log Rules** pane, click **Add** or select a log rule and click **Save As** or **Settings**. This displays the **Log Rule Settings** or **Add Log Rule** window.
4. By **Data definition**, click **Add** or **Settings**. This displays the **Add Log Data Definition** or **Log Data Definition Settings** window. The **Data definition** list box lists custom data definitions and predefined "System Data Definitions" on page 412.
5. Specify a **Name** and optional **Description** if creating a definition or leave them as is if modifying an existing definition.
6. To modify an existing definition, double-click the **Name**, **Custom Data Value**, or both, from the table.
7. Use the **Add** button and specify a **Name** and **Custom Data Value** for the new definition. **Name** is used when defining the format for the rule **Sink definition**. **Custom Data Value** provides the data to pass in the log for the server event. Make sure the **Custom Data Value** conforms to the syntax defined for the log code in the "Data syntax" column of the "Intelligent Capture Server Events: Log Code Details" on page 469 table. To log data for IA Values that are stored in `Tbl_ValueAttribute` table in the Intelligent Capture Database, the **Custom Data Value** syntax is `Attribute.<IAValue>`.
8. Click **OK** to save the settings and return to the **Log Rule Settings** or **Add Log Rule** pane.

Related Topics

"Defining Log Rule Filter Definitions" on page 221

"Defining Log Rule Filter for Log Type and Codes" on page 222

"Defining Log Rule Filters for Processes and Modules" on page 224

"Specifying Log Rule Sink Definition" on page 228

"Defining a Log Rule Filter for Workstations and Users" on page 225

"Log Rule Settings and Add Log Rule" on page 323

"Understanding Log Rules" on page 215

"Intelligent Capture Permissions List" on page 381

9.11.3.11 Specifying Log Rule Sink Definition

Sink definitions specify the destination where the log is written. Intelligent Capture Administrator includes several "System Sink Definitions for Client Modules and Components" on page 421 and supports the following sinks:

- Event sink: Writes logs to the Windows Event Log. When specifying LogName in the `EventSinkDestination.xsd` schema file, only Application is supported at this time. Applications may not write entries to the Security or System log.
- File sink: Writes the log to a file on the machine running the scope component. Entries logged to the File Sink that are longer than 511 bytes may be truncated. Truncated entries end with "…".
- Database sink: Writes the log to a table in the database.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To specify log rule Sink Definitions:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View All Log Rules** from the **Reports / Logs** pane.
3. From the **Log Rules** pane, click **Add** or select a log rule and click **Save As** or **Settings**. This displays the **Log Rule Settings** or **Add Log Rule** window.
4. By **Sink definition**, click **Add** or **Settings**. This displays the **Logging Rule Sink Definition** window.

   Note: In a log rule, if information messages (indicated by selecting **FilterAllDebugInfos** from the **Filter definition** list) are logged to **AuditToDBSink**, **ErrorToDBSink**, or **GeneralEventLogSink**, then the **Logs** pane will not display all the log messages.
5. Specify a **Name** and optional **Description** if creating a definition or leave them as is if modifying an existing definition.
6. Under **Destination**, specify the **Sink type**, including any information needed by the sink to locate and connect to, if necessary, the destination where the log is to be written. The destination is used to determine the creation of a sink object to write the log. Some sinks can handle more than one destination and others cannot. For example:

- Each file sink object writes to a single file, so if this rule writes to the same file as another rule, it should use the same destination string. If it writes to a different file, the destination string should be different. So for the file sink object, it is easiest to make the destination the name of the file to be written.
- Each database sink object writes to the Intelligent Capture Database. Multiple database sink definitions can be created, each will always write to the Intelligent Capture Database.
- For the event sink object, the same name should be used for all sink objects.

7. Under **Destination Settings File**, specify the **XML file to upload** that contains *XML* that conforms to the destination *XML* schema for the sink type. This may not be available depending on the designated sink.
8. Under **Format Configuration File**, specify the **XML file to upload** that contains *XML* that conforms to the format *XML* schema for the sink type. This may not be available depending on the designated **Data definition**.

   Notes

   - For more information, see "XML Schema for the Logging Sink Definitions" on page 424.
   - Not all sinks require a format *XML* file.

9. Click **OK** to save the settings and return to the **Log Rule Settings** or **Add Log Rule** pane.

Note: Sink definitions cannot be downloaded on a Windows 2012 system. To resolve this issue, follow the instructions described in http://support.microsoft.com/kb/2870699.

Related Topics

"Specifying Log Rule Data Definitions" on page 227

"Defining Log Rule Filter Definitions" on page 221

"Defining Log Rule Filter for Log Type and Codes" on page 222

"Defining Log Rule Filters for Processes and Modules" on page 224

"Defining a Log Rule Filter for Workstations and Users" on page 225

"Log Rule Settings and Add Log Rule" on page 323

"Log Rule Sink Definition" on page 329

"Intelligent Capture Permissions List" on page 381

"Understanding Log Rules" on page 215

"XML Schema for the Logging Sink Definitions" on page 424

9.11.3.12 Logging IA Values that are Viewed

A custom log rule must be created to log entries for IA Values that are viewed.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To create a custom log rule to log viewed IA Values:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Log Rules** to display the **Log Rules** pane.
3. Click **Add**. The **Add Log Rule** pane displays.
4. Type a **Name** and optional **Description** for the rule.
5. In the Status area, select the **Enabled** check box to enable the log rule.
6. Select **Server** from the **Scope component** list box.
7. In the **Filter definition** area, click **Add** and then specify the following settings in the **Add Log Rule Filter Definition** window:
   a. Select **Log Type and Codes** from the **Setting** list.
   b. Select **Audit** from the **Log type** list.
   c. Select **161** from the **Log codes** list.
   d. Select **Value** from the list of **Available Categories** and move them to **Selected Categories**.
   e. Click **OK** to save the settings and return to the **Add Log Rule** pane.
8. Select **DataServerValueEvents** from the **Data definition** list.
9. Select **AuditToDBSink** from the **Sink definition** list.
10. Click **OK** to save the settings and add the log rule to the list of available log rules.

Related Topics

"Defining Log Rule Filter Definitions" on page 221

"Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218

"Log Rule Data Definition Settings" on page 318

"Log Rule Filter Definition Settings and Add Log Rule Filter Definition" on page 319

"Log Rule Settings and Add Log Rule" on page 323

"Log Rules" on page 303

"Log Rule Sink Definition" on page 329

"Understanding Log Rules" on page 215

"Viewing Log Rule Settings" on page 217

"Viewing Log Rules and Log Rule Settings" on page 216

"Intelligent Capture Permissions List" on page 381

9.11.4 Managing Reports

Reports provide information about an Intelligent Capture system using data obtained from the Intelligent Capture Database. The reports functionality is available only if you have installed the Intelligent Capture Database.

Administrators use reports to:

- Analyze the current performance and accuracy of the Intelligent Capture system against its performance and accuracy in the past.
- Determine actions needed to improve the performance and accuracy of the Intelligent Capture system.
- Track batches to completion.
- Show how many batches entered an Intelligent Capture system on a given day, how many of those batches are currently in a step in a process, and how many batches did not complete all of the steps in a process on that day.
- Provide an audit trail to record when an Intelligent Capture module creates, accesses, processes, modifies, or deletes an image or batch. The audit trail can be used for security purposes.
- Generate reports and export the results to various formats.
- Collect statistics. View statistics in the Intelligent Capture Administrator and export to a third party repository using an export module.

From Intelligent Capture Administrator, you create reports based on report definitions. Intelligent Capture installs predefined report definitions that provide system information based on commonly performed tasks, such as scanning, operator data entry, *OCR* processing, file auditing, and batch reconciliation. You can use the report definitions as is or make a copy and modify it based on your requirements.

Note: The Intelligent Capture Database is case insensitive. This means that upper and lower case characters are not differentiated and instead are treated the same way when performing searches or using the reports functionality in Intelligent Capture.

9.11.4.1 Understanding Report Definitions

Report definitions tell the Intelligent Capture Administrator how to run a report. It describes the stored procedure to be called, the parameters to pass to the stored procedure, and the Crystal Reports project file (*RPT*) to use. This information is contained in the following files loaded into each report definition:

- Stored procedure: Specifies the data that a report extracts from the Intelligent Capture Database. Used in conjunction with the *XML* file, the input parameters display in Intelligent Capture Administrator to refine the information returned from the output dataset. The names of the predefined *SQL* files are stored in the Microsoft SQL Server in the `Tbl_ReportStoredProcedures` table. You can modify or create new stored procedures using the predefined stored procedures as examples. A complete list of all of the available input parameters and output datasets are located in the "Predefined Reports Stored Procedures" on page 449 section.
- *XML* file: Describes the input parameters and designs the display for the parameter sections of the **Add** and **Add Report** windows in Intelligent Capture Administrator. In these windows, you define the input parameters that are used in a report. For example, you can specify the start and end dates of a report. The predefined *XML* files are located in the Root directory in the `Reports` folder. The `ParameterDefinitions.xsd` schema file, which is located in the `Inetpub\wwwroot\AdministrationConsole\Secure\AC\Reporting` directory, defines the allowed elements in the *XML* files. If you create or modify an *XML* file, it must conform to the `ParameterDefinitions.xsd` file to view it from the Intelligent Capture Administrator.
- Crystal Reports project file: Specifies the output of the report in a Crystal Reports Viewer. The report file (*RPT*) calls the stored procedure and outputs the data collected from the Intelligent Capture Database based on the input parameters. The predefined Crystal Reports files are located in the `Inetpub\wwwroot\AdministrationConsole\Secure\AC\Reporting` directory. See Crystal Reports **Help** for information on creating a report file.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

"Predefined Reports Stored Procedures" on page 449

9.11.4.2 Creating or Modifying a Report Definition

Intelligent Capture installs predefined report definitions for creating reports to perform common tasks.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To create or modify a report definition:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Report Definitions**. On the **Report Definitions** pane:
   - Click **Add** to create a report definition. The **Add Report Definition** pane displays.
   - Select a report definition and click **Save As** to create a copy of it. The **Add Report Definition** pane displays.
3. Type a name in the **Name** field. The **Description** field is optional.
4. Select an **Associated stored procedure**, which collects the data set from the Intelligent Capture Database for the report.

   Note: Add the stored procedure for a new report to the `Tbl_ReportStoredProcedures` table in the Intelligent Capture Database before creating the report definition or it will not be found. To update the stored procedure list, use an insert *SQL* statement to create an entry in `Tbl_ReportStoredProcedures` or `Tbl_PurgeStoredProcedures`.
5. Specify an **XML Parameter File**. which describes the input parameters and designs the **Parameter** area of the **Add Report** and **Add Report Definition** panes. To display a report in the Intelligent Capture Administrator, the report definition the *XML* file must conform to the `ParameterDefinitions.xsd` schema file. If a file is not listed under **Current XML parameter file**, click **Browse** to specify the **XML file to upload**. Click **Export File** to view the file or save it.
6. Specify a **Crystal Reports Project File**, which displays the report using the Crystal Reports Viewer. If a file is not specified in the **Current report file** field, click **Browse** to select the **Report file to upload**. Click **Export File** to view or save the file.
7. Under **Sample Report Image**, a thumbnail representation is displayed as the **Current database image**. Click **Open Full Size Image** to display the image in Intelligent Capture Administrator, or click **Export File** to save the image to a file. If a file is not listed, click **Browse** to specify the **Image to upload**. This field is optional.
8. Click **OK** to save the report definition, which is now available for creating and generating reports.

Related Topics

"Creating or Modifying a Report" on page 235

"Generating and Viewing Reports in Crystal Reports Viewer" on page 236

"Report Definitions" on page 295

"Reports" on page 294

"Understanding Report Definitions" on page 232

"Viewing Report Definitions" on page 234

"Intelligent Capture Permissions List" on page 381

9.11.4.3 Viewing Report Definitions

To view the contents of a report definition file, use the following steps.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view a report definition:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Report Definitions**. On the **Report Definitions** pane, select a report definition, and click **Settings**.
3. The settings for the selected report definition display in the **Report Definition Settings** pane.

Related Topics

"Understanding Report Definitions" on page 232

"Creating or Modifying a Report Definition" on page 233

"Creating or Modifying a Report" on page 235

"Generating and Viewing Reports in Crystal Reports Viewer" on page 236

"Report Definitions" on page 295

"Reports" on page 294

"Intelligent Capture Permissions List" on page 381

9.11.4.4 Creating or Modifying a Report

You create a report or modify a predefined report to meet the requirements of your Intelligent Capture System. New or modified reports are added to the **Reports** pane.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To create or modify a report:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel, and select **View Reports** from the pane. The **Reports** pane displays.
   - Click **Add** to create a report.
   - Select a report and click **Settings** to modify the existing report. The **Report Settings** pane displays.
   - Select a report and click **Save As** to create a copy of the existing report. The **Add Report** pane displays.
2. Type a **Name** and optional **Description** for new reports. Change the name and description when you modify an existing report to preserve the original report.
3. Select an **Associated report definition**. The selected report definition controls the parameters that are displayed in the bottom portion of the **Add Report** pane. You cannot change the **Associated report definition** field when you modify an existing report.
4. Configure the parameters that display in the parameters area for the report.
5. Click **Generate Report** to view the results of the report.

   Note: For generating reports with characters in the supported languages, set the language of the Intelligent Capture Administrator to the language required to be displayed in the report.
6. Click **OK** to save the report. The saved report displays on the **Reports** pane.

Related Topics

"Creating or Modifying a Report Definition" on page 233

"Generating and Viewing Reports in Crystal Reports Viewer" on page 236

"Report Definitions" on page 295

"Reports" on page 294

"Understanding Report Definitions" on page 232

"Viewing Report Definitions" on page 234

"Intelligent Capture Permissions List" on page 381

9.11.4.5 Generating and Viewing Reports in Crystal Reports Viewer

You create a report or modify a predefined report to meet the requirements of your Intelligent Capture System. New or modified reports are added to the **Reports** pane. Use these steps to view a report in a Crystal Reports Viewer window.

Note: If you have upgraded to Intelligent Capture 16.5 and want to view a report generated in Intelligent Capture 6.0 and 6.5 versions. View the report settings, save the report settings without making any changes, and then generate the report.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Note: For generating Crystal reports, the user must have owner/admin permissions. When you create a user account with SQL Server authentication, ensure that all required permissions to generate reports are granted to this user. You must complete the procedure for encrypting or decrypting the connection string used in the `CaptivaAdministator.exe.config` file.

To encrypt the connection string:

1. Open `ConnectionStringEncryptApp.exe.`in the folder`C:\Program Files (x86)\InputAccel\Client\src\Encryption Form`.
2. Enter all the details and click **Encrypt**.
3. In the file `CaptivaAdministrator.exe.config` located at `C:\Program Files (x86)\InputAccel\Client\binnt`, do the following:
    1. Copy the encrypted string and paste it as the value for *`ReportConnectionString`*.
    2. Set the value for *`EnableReportConnectionConfig`* as "True".
4. Close the file.

To view a report:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Reports** from the **Reports / Logs** pane.
3. In the **Reports** pane, select a report.
4. Click **Generate Report** and the report displays in the Crystal Reports Viewer window.

    Note: If your report takes more time to generate than the duration specified by the global **AttendedClientSessionTimeout** value (default 600

seconds) and Intelligent Capture Administrator is inactive for that duration, you will be logged out before the report is finished generating. You can change the **AttendedClientSessionTimeout** value to a maximum of 32767 seconds (546 minutes) to avoid being timed out during report generation. However, if your report takes longer than 20 minutes to generate, you should consider purging the report tables to increase performance and speed of report generation. Note that the **AttendedClientSessionTimeout** value is shared by Intelligent Capture Administrator, Completion, and Identification.

5. Use the Crystal Reports Viewer controls to view, print, or export the report to several different formats.

Notes

- Make sure the appropriate log rules are enabled so that the data you want displayed in the report is logged. See "Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218.
- The **ReportTaskFinishTask** log rule logs every task which is finished. However, this log rule does not log finished tasks for the eIndex module.
- The Intelligent Capture Database supports installation on a case sensitive SQL Server. The Intelligent Capture Database, however, is case insensitive. This means that upper and lower case characters are not differentiated and instead are treated the same way when performing searches or using the reports functionality in Intelligent Capture.
- Adobe® Reader® must be installed on the same workstation as Intelligent Capture Administrator to print or view the exported reports in *PDF* format.

Related Topics

"Creating or Modifying a Report" on page 235

"Creating or Modifying a Report Definition" on page 233

"Report Definitions" on page 295

"Reports" on page 294

"Understanding Report Definitions" on page 232

"Viewing Report Definitions" on page 234

"Intelligent Capture Permissions List" on page 381

9.11.4.6 Generating and Viewing Reports in OpenText Information Hub

The Intelligent Capture reporting functionality is made available as an OpenText Information Hub (hereafter referred to as *iHub*) Analytics Designer project.

To enable reporting to iHub, you set up the Intelligent Capture Database connection string and deploy the Intelligent Capture reports Analytics Designer project to iHub.

Note: Also make sure to enable the appropriate log rules such that the data you want to be displayed in the report is logged. For more information, see "Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218.

1. In iHub Analytics Designer, import the **CaptivaAnalytics** Analytics Designer project (available on http://support.opentext.com).
2. In the **CaptivaAnalytics** project, change the database connection properties in the `ConnectionProfiles.acconprofiles` file to point to your Intelligent Capture Database.
3. Verify the database connection by locally running a **CaptivaAnalytics** report or dashboard.
4. Deploy the **CaptivaAnalytics** project's reports and dashboard by publishing the entire **CaptivaAnalytics** project to the iHub server.

9.11.5 Creating Custom Reports

Intelligent Capture installs predefined or out-of-box reports. These reports use predefined report definition files that consist of a stored procedure, a parameter *XML* file, and a Crystal Reports (*RPT*) file that are used to generate the report. A sample image file for the report, such as a *GIF* file, is optional.

Users can create their own reports by modifying or creating new report definition files. This section includes procedures to generate a custom report based on certain scenarios.

Prerequisite: To create custom reports, users must have expertise in working with SQL Server and Crystal Reports Designer.

Note: See Crystal Reports documentation for information related to localizing custom reports.

9.11.5.1 Adding Text, Images, or Deleting Data from an Existing Predefined Report

This procedure enables you to make minor changes to an existing predefined report. Changes include adding text or images (a company logo, for example) to a predefined report, or deleting some report data from a predefined report.

To modify an existing predefined report

1. Using Intelligent Capture Administrator, export the *XML* parameters file and the Crystals Reports Project file of the report you want to modify:

   a. In Intelligent Capture Administrator, navigate to **Reports / Logs > View Report Definitions**.

   b. From the **Report Definitions** table, select the report that you want to modify and click **Settings**. The **Report Definition Setting** pane displays information about the stored procedure, parameter *XML* file, and Crystal Reports (*RPT*) file associated with the selected report definition.

   c. Click **Export File** in the **Current XML parameter file** row to export the *XML* file associated with the report definition and then **Save** it to the file system.

   d. Click **Export File** in the **Current report file** row to export the *RPT* file associated with the report definition and then **Save** it to the file system.

2. Modify the report file in Crystal Reports Designer:

   a. Open the exported *RPT* file in Crystal Reports Designer and make the changes you need, such as adding text, adding images, or deleting existing text from the report. Test these changes.

   

   Note: See Crystal Reports Help for information on creating a report file. To install the Crystal Reports software from the Intelligent Capture installation media, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

   b. Export the report to a *PDF* file and then covert it to an image file.

   c. Save the modified *RPT* file with a new name and make sure Preview mode is disabled when you save the *RPT* file.

3. In Intelligent Capture Administrator, generate the report with the modified text and data:

   a. Create a new report definition and associate it with the changed Crystal Reports file (*RPT* file):

   b. Create a report and reference the new report definition.

   c. Make sure the appropriate log rules are enabled so that the data you want displayed in the report is logged. See "Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218.

d. Create batches and process tasks so that appropriate data is logged to the reports tables.

e. Generate the report.

9.11.5.2 Adding Data to an Existing Predefined Report

This procedure enables you to add report data to a predefined report. This procedure assumes that the additional data is already logged by existing log rules and is stored in existing reports tables.

To add additional data to an existing predefined report

1. Review the contents of the Intelligent Capture Database tables to determine the data that needs to be added to the predefined report. For a list of Intelligent Capture report tables and the columns in each table, see Reports Tables.

2. Update the stored procedure for the predefined report to return the additional data required and add the updated stored procedure to the Intelligent Capture Database:

   a. Make a copy of the stored procedure (default location: `C:\Program Files\InputAccel\Databases\DBScripts\ReportsDB\Procedures`) for the predefined report.

   b. In SQL Server, modify the stored procedure to return additional reports data and if required to specify additional input parameters and output datasets. Save the changed stored procedure.

      Note: A complete list of all of the available reports stored procedures, their input parameters and output datasets are located in the "Predefined Reports Stored Procedures" on page 449 section.

   c. Using SQL Server, connect to the **IADB** database, open the modified stored procedure file, and execute the stored procedure. If executed successfully, the stored procedure is added in `Databases\IADB\Programmability\Stored Procedures`.

   d. Add the name of the modified stored procedure to the `Tbl_ReportStoredProcedures` table in the Intelligent Capture Database.

3. Using Intelligent Capture Administrator, export the *XML* parameters file and the Crystals Report file of the report you want to modify:

   a. In Intelligent Capture Administrator, navigate to **Reports / Logs > View Report Definitions**.

   b. From the **Report Definitions** table, select the report that you want to modify and click **Settings**. The **Report Definition Setting** pane displays information about the stored procedure, parameter *XML* file, and Crystal Reports (*RPT*) file associated with the selected report definition.

   c. Click **Export File** in the **Current XML parameter file** row to export the *XML* file associated with the report definition and then **Save** it to the file system.

d. Click **Export File** in the **Current report file** row to export the *RPT* file associated with the report definition and then **Save** it to the file system.

4. Modify the report file in Crystal Reports Designer:

   a. Open the exported *RPT* file in Crystal Reports Designer.

   Note: See Crystal Reports Help for information on creating a report file. To install the Crystal Reports software from the installation media, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

   b. Set the **Datasource Location** to the Intelligent Capture Database and update the references to the new stored procedure.

   c. Verify that the correct stored procedure is used by running the **Database> Show SQL Query** option.

   d. Add the new database fields that were added to the stored procedure to the *RPT* file.

   e. Test these changes and make sure the report generates as required.

   f. Export the report to a *PDF* file and then covert it to an image file.

   g. Save the modified *RPT* file with a new name. Make sure Preview mode is disabled when you save the *RPT* file.

5. If the updated stored procedure has different input parameters from the original stored procedure, update the exported *XML* parameter file. The *XML* file must conform to the `ParameterDefinitions.xsd` schema file, which is located in the `Inetpub\wwwroot\AdministrationConsole\Secure\AC\Reporting` directory. Save this *XML* parameter file with a new name.

6. In Intelligent Capture Administrator, generate the report:

   a. Create a new report definition and associate it with the updated stored procedure, updated XML Parameter file, and the updated Crystal Reports file (*RPT* file.

   b. Create a report and reference the new report definition.

   c. Make sure the appropriate log rules are enabled so that the data you want displayed in the report is logged. See "Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218.

   d. Create batches and process tasks so that appropriate data is logged to the reports tables.

   e. Generate the report

9.11.5.3 Creating a Custom Report

This procedure enables you to create a custom report that contains data already being logged by existing log rules and is stored in existing reports tables.

To create a custom report to contain data logged by existing log rules:

1. Review the contents of the Intelligent Capture Database reports tables to determine the data that needs to be in the report. For a list of report tables and the columns in each table, see Reports Tables.
2. Develop a stored procedure to display the reports data required and add the stored procedure to the Intelligent Capture Database.
    a. Write a new stored procedure or make a copy of an existing stored procedure (default location: `C:\Program Files\InputAccel\Databases\DBScripts\ReportsDB\Procedures`). Specify the input parameters and output datasets used to extract data from the Intelligent Capture Database.
    b. Add the stored procedure to the Intelligent Capture Database.
    c. Add the modified stored procedure name to the `Tbl_ReportStoredProcedures` table in the Intelligent Capture Database.
3. Write a parameter *XML* file that describes the report parameters that will be passed to the stored procedure when the report is run. The *XML* file must conform to the `ParameterDefinitions.xsd` schema file, which is located in the `Inetpub\wwwroot\AdministrationConsole\Secure\AC\Reporting` directory. Save this parameter *XML* file.
4. Use Crystal Reports Designer to design a Crystal Reports *RPT* file. Make sure you select the data source connection type as **OLBD (ADO)** and are connected to the Intelligent Capture Database because Crystal Reports needs to access the stored procedure you created from the database. Save the *RPT* file but make sure Preview mode is disabled when you save the file.
5. In Intelligent Capture Administrator, generate the custom report:
    a. Create a new report definition and associate it with the stored procedure, XML Parameter file, and the Crystal Reports file (*RPT* file.
    b. Create a report and reference the new report definition.
    c. Make sure the appropriate log rules are enabled so that the data you want displayed in the report is logged. See "Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218.
    d. Create batches and process tasks so that appropriate data is logged to the reports tables.
    e. Generate the report.

Related Topics

"Creating or Modifying a Report Definition" on page 233

"Understanding Report Definitions" on page 232

"Viewing Report Definitions" on page 234

"Intelligent Capture Permissions List" on page 381

"Predefined Reports Stored Procedures" on page 449

9.11.5.4 Creating a Report for Data Not Currently Logged

This procedure enables you to create a custom report that contains data that is currently not being logged by existing log rules.

To create a custom report to contain data that is not logged by existing log rules:

1. Determine the Intelligent Capture Server event that will return the new data required in the report. "Intelligent Capture Server Events: Log Code Details" on page 469 lists the server events, a description of the event, and the data syntax associated with the event. If the data required is returned from a module task as an IA Value, use the server's `TaskFinish` event. For example, to log data returned by the IndexPlus module IA Values <*CharCount*>, <*DocCount*>, <*FieldCount*>, and <*KeyTime*>, you would use the `TaskFinish` server event.

2. Define a new reports table to capture the data you require, develop a stored procedure to display the reports data required, and add the stored procedure to the Intelligent Capture Database:

    a. This step is required only if the data required is returned as an IA Value from a module task. Using SQL Server, connect to the Intelligent Capture Database (**IADB**) and add a row to the table `Tbl_ValueAttribute` to define an attribute to identify the IA Value to the Intelligent Capture Server. For example, to identify the IndexPlus IA Value <*CharCount*>, you would add a row in the table `Tbl_ValueAttribute` where `VAAttributeName=CharCount` and `VAModuleName=INDXPLUS`.

    b. Define a reports table in the Intelligent Capture Database for the data you require. If the data is an IA Value from a module task, link the new table to the `Tbl_ReportTasks` table using the foreign key `TaskUUID`. For example, for the IndexPlus module example used in this procedure, if you created a new table called `Tbl_ReportIndexTasks`, you would link it to `Tbl_ReportTasks` using the `TaskUUID`.

    c. Write a stored procedure to populate the new table when the required server event occurs. See the predefined stored procedure, `up_LogTaskFinishIndexTask`, as an example.

    d. Add the stored procedure to the Intelligent Capture Database.

    e. Add the stored procedure name to the `Tbl_ReportStoredProcedures` table.

3. In Intelligent Capture Administrator, create a log rule to log the data you require when the server event occurs. See the system log rule **ReportTaskFinishIndexTask** as an example.

   a. In the log rule, if the data required to be logged is an IA Value, make sure the **Scope Component** for the new log rule is set to **Server**.

   b. In the filter definition for the log rule, make sure the **Log code** specified is the code for the server event identified in step 1. For example, if you want to log data when the `TaskFinish` event occurs, then you would select **123** as the **Log code**. Set all other parameters appropriately.

   c. The data definition for the log rule defines additional data to be passed to the stored procedure. Data to be passed must include the data parameter names and custom data value settings. For all server events, the syntax of the **Custom Data Value** column is listed in the **Data Syntax** column of the "Intelligent Capture Server Log Codes" on page 469 table. For any new IA Values you may have defined, the **Custom Data Value** syntax is `Attribute.<IA Value Name>`. Use the attributes you defined in step 1 to define the IA Value data to log. For example, to capture the Batch ID, Task ID, and the IndexPlus IA Values you need logged, you would provide the following data parameter names and custom data value settings.

Name	Custom Data Value
BatchUUID	Batch.UUID
TaskUUID	Task.UUID
DocCount	Attribute.DocCount
CharCount	Attribute.CharCount
FieldCount	Attribute.FieldCount
KeyTime	Attribute.KeyTime
TaskModule	Attribute.TaskModule

   d. Make sure the log rule sink definition is for the Intelligent Capture Database . Make sure the Database Sink format XML file references the stored procedure you created and the parameters to be passed to it. To ensure it matches the `DbSinkDestination.xsd` schema, see "DbSinkFormat XML" on page 428.

   e. Test your logging mechanism. Enable the log rule you created and any other related log rules, create batches associated with the module you are logging data for, and verify that the report data is generated in the new table you added.

4. Write a parameter *XML* file that describes the report parameters that will be passed to the stored procedure when the report is run. The *XML* file must conform to the `ParameterDefinitions.xsd` schema file, which is located in the `Inetpub\wwwroot\AdministrationConsole\Secure\AC\Reporting` directory. Save this parameter *XML* file.

5. Use Crystal Reports Designer to design a Crystal Reports *RPT* file. You must be connected to the Intelligent Capture Database when designing the report because Crystal Reports needs to access the stored procedure you created from the database. Save the *RPT* file. Make sure the Preview mode is disabled when you save the file.
6. Create a report definition for the new or modified report that references the new stored procedure, new parameter *XML* file, and the new Crystal Reports (*RPT*) file.
7. Create the report and reference the new report definition. Generate the report.

9.11.5.5 Adding Data from Custom Modules to Predefined Reports

If you have custom modules, you will need to add an entry for the module in the Intelligent Capture Database to ensure that data from the module is logged in the Reports tables and later displayed in the predefined reports.

To add custom module data into predefined reports:

1. Using SQL Server, connect to the Intelligent Capture Database (**IADB**) and add an entry for the module to the `Tbl_Module` table.
2. Set the correct module attributes for the module by adding rows to the `Tbl_ModuleAttributeLink` table. This table connects the attributes in `Tbl_ModuleAttribute` to the custom module.
3. Review the list of value attributes in the `Tbl_ValueAttribute` table. Determine the attributes returned as IA Values by the custom module. Add rows in the `Tbl_ValueAttribute` table for all IA Values that are applicable.
4. Create batches associated with the custom module and verify that data associated with the module is logged to existing reports tables.
5. Create a report.
6. Generate the report.

9.11.6 Managing Purging

Intelligent Capture Administrator enables creation, alteration, and deletion of purges and sets the schedule for running purges.

9.11.6.1 Understanding Purging

Intelligent Capture Administrator enables creation, alteration, and deletion of purges and sets the schedule for running purges. Purge definitions are the building blocks for purges. Purge definitions encapsulate general information such as the name and description as well as an *XML* file containing the definition of the tunable arguments for the purge. Purges use stored procedures to specify how old the data has to be before being purged, and what if any types of data (performance data, statistical data, error, audit, etc.) are the targets of the purge. The Intelligent Capture Database may grow large with all of the report data and it will be necessary to periodically purge this data.

Two configured purges are included with Intelligent Capture:

- **Purge Audit/Error Logs**
- **Purge Report Detail** purges report data from batches deleted before a specific date. It is recommended that the users keep at least one year of data available for reporting. Users should delete batches that are no longer being actively processed by Intelligent Capture. Data purged will be rolled into summary tables. This allows summary reports to be run against the data without using too much space in the database. After the deleted batches data is purged, those batches will no longer appear on the detail reports. They will appear on the summary reports.
- **Default Report Detail Purge** is added to reduce the size of the reporting tables in the Intelligent Capture Database since large reporting tables cause performance issues when using the Reports functionality. This purge is scheduled to run once a week to summarize and purge detailed reporting data. This purge summarizes report detail data logged by various reporting log rules, saves it in several different report summary tables, then systematically deletes the detail rows. The purge is automatically scheduled to run once a week, on Sunday at 2:05 A.M. It purges details logged prior to the previous Saturday at midnight. The day and time to begin the purge are converted from Sunday 2:05 A.M. in local database time to the corresponding day and time in UTC. The `Default Report Detail Purge` is enabled at install time, and set to begin on the Sunday after the database has been installed or upgraded. Since configured purges are triggered by an Intelligent Capture Server, the server must be started for this purge to be executed. If a scheduled purge already exists, then a new one is not added. Users can view or change the schedule, frequency and configuration of the purge using the Administration Console.
- **Purge Report Summary** permanently purges summary data older than a certain date. After the summary data has been purged, it will no longer be available for reporting. The purge of the summary tables uses an **OlderThan** date as a guide for purging the summary tables. The summary tables are organized by batch creation date and so this date refers to the batch creation date (not the batch deletion date as in the **Purge Report Detail**). A row in a table will not be purged if any data summarized in the row is newer than the date entered.
- **Purge Document Type Statistics**

Notes

- Logging is not applied to purging operations, specifically when table content is modified or deleted.
- Not all of these pre-configured purge definitions are available with the internal database because some types of logging are not performed by an internal database.

Related Topics

"Purge Definitions" on page 298

"Purges" on page 297

"Managing Reports and Logs" on page 205

"Viewing Purges" on page 251

9.11.6.2 Purging the Intelligent Capture Database

Purging the Intelligent Capture Database removes data that is no longer useful, or frees up more space in the database.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To purge the Intelligent Capture Database:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Purges** from the **Reports / Logs** pane.
3. In the **Purges** pane, select a single purge.
4. Click **Run Purge**, and the purge commences.

Related Topics

"Creating a Purge Definition" on page 248

"Creating a Purge" on page 249

"Purge Definitions" on page 298

"Purges" on page 297

"Understanding Purging" on page 246

"Viewing Purge Definitions" on page 250

"Viewing Purges" on page 251

"Intelligent Capture Permissions List" on page 381

9.11.6.3 Creating a Purge Definition

Purge definitions are the initial building blocks of purges. Purge definitions encapsulate general information such as the name and description as well as an *XML* file containing the definition of the tunable arguments for the purge. Purge parameters are provided in a *XML* file that is passed into the associated stored procedure along with other general properties. The **Purge Definition Settings** pane is the mechanism by which all purge definition properties are set and committed to the database.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To create or modify a purge definition:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Purge Definitions**. On the **Purge Definitions** pane:
   - Click **Add** to create a definition.
   - Select a custom definition and click **Settings** to modify the existing definition.
   - Select a custom definition and click **Save As** to create a copy of an existing definition.

   The **Purge Definition Settings** pane or **Add Purge Definition** pane displays.
3. Specify a **Name** and optional **Description**. If you are modifying an existing definition you can leave the **Name** and optional **Description** as they appear.
4. Select an **Associated stored procedure**, which will indicate the appropriate data for the purge.

   Note: Stored procedures can be created and manually inserted in the database as well. To update the stored procedure list, use an insert *SQL* statement to create an entry in `tbl_reportStoredProcedures` or `tbl_PurgeStoredProcedures`.
5. Specify an **XML Parameter File** which will determine the configurable parameters for the purge. If no file is listed under **Current XML parameter file**, click **Browse** to specify an **XML file to upload**. When a parameter file is listed, clicking **Export File** provides an opportunity to either view the file or save it.
6. When all parameters are set, click **OK** to save the purge definition. This is now available for creating a purge.

Related Topics

"Creating a Purge" on page 249

"Purge Definitions" on page 298

"Purges" on page 297

"Purging the Intelligent Capture Database" on page 247

"Understanding Purging" on page 246

"Viewing Purge Definitions" on page 250

"Viewing Purges" on page 251

"Intelligent Capture Permissions List" on page 381

9.11.6.4 Creating a Purge

Purges are based on purge definitions, which specify the purge parameters. Upon initial installation of Intelligent Capture, there are no purges, but there are a number of predefined purge definitions from which to configure purges. Purge definitions can be customized or created for configuring custom purges.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To create a purge or modify an existing purge:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Purges** from the **Reports / Logs** pane. The **Purges** pane displays.
3. To create a purge, click **Add** or select an existing purge and click **Save As**. To modify an existing purge, select the purge from the grid and click **Settings**. These choices open the **Purge Settings** pane.
4. Specify a **Name** and optional **Description** for new purges.

   Note: If a purge is created which has same name as an existing purge in SQL Server Agent\jobs, the new purge will overwrite the existing purge without any warning.
5. Specify an **Associated purge definition**. The selected purge definition controls the configurable parameters displayed in the **Parameters** portion of the **Purge Settings** pane. The **Purge creation date and user** and **Last saved** values also display.
6. Configure **Scheduling** parameters for the purge. The **Status** area indicates the last time the purge was run and the outcome.

7. Specify the **Parameters** displayed. These are dynamically generated based on the *XML* parameter file specified in the **Associated purge definition**.
8. Click **OK** to save the purge. The saved purge is displayed on the **Purges** pane.

Related Topics

"Creating a Purge Definition" on page 248

"Purge Definitions" on page 298

"Purges" on page 297

"Purging the Intelligent Capture Database" on page 247

"Understanding Purging" on page 246

"Viewing Purge Definitions" on page 250

"Viewing Purges" on page 251

"Intelligent Capture Permissions List" on page 381

9.11.6.5 Viewing Purge Definitions

Purge definitions are the initial building blocks of a user configured purge.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view purge definitions:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Purge Definitions**. On the **Purge Definitions** pane, select a definition and click **Settings**.
3. The settings for the selected definition are displayed in the **Purge Definition Settings** pane.

Related Topics

"Creating a Purge Definition" on page 248

"Creating a Purge" on page 249

"Purge Definitions" on page 298

"Purges" on page 297

"Purging the Intelligent Capture Database" on page 247

"Understanding Purging" on page 246

"Viewing Purges" on page 251

"Intelligent Capture Permissions List" on page 381

9.11.6.6 Viewing Purges

The **Purge Settings** pane displays the settings and parameters of a purge.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view purges:

1. In the **Intelligent Capture Administrator** window, select **Reports / Logs** from the navigation panel.
2. Select **View Purges**. On the **Purges** pane, select a purge and click **Settings**.
3. The settings for the selected purge are displayed in the **Purge Settings** pane.

Related Topics

"Creating a Purge Definition" on page 248

"Creating a Purge" on page 249

"Purge Definitions" on page 298

"Purges" on page 297

"Purging the Intelligent Capture Database" on page 247

"Understanding Purging" on page 246

"Viewing Purge Definitions" on page 250

"Intelligent Capture Permissions List" on page 381

9.12 Managing Web Services and Hosting

Managing the Intelligent Capture Web Services subsystem is necessary when using the Web Services Input module, or the Web Services Coordinator or Web Services Hosting services. The Web Services Output module functions by itself, without additional configuration.

Notes

- Web Services functionality is available only for users that install the Intelligent Capture Database.

- Web Services Output does have a maximum allowed number of pages limit. When this limit is reached Web Services Output stops processing tasks, but no error message is displayed. When enabled, the Intelligent Capture Server log rule (`AllServerWarnings`) will log all warnings to the Intelligent Capture Database.

Managing the Intelligent Capture Web Services subsystem involves three main activities: Configuring Web Services, configuring hostings, and defining Web Services settings.

9.12.1 Configuring Web Services

To process requests from a third-party web service client, begin by adding and registering the web service within the Web Services subsystem. All web services registered in the Web Services subsystem are listed in the Intelligent Capture Administrator.

9.12.1.1 Adding a Web Service

To add a web service, define the service, map any *`Correlation IDs`* for asynchronous processing, and then register the service within the Intelligent Capture Web Services subsystem.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To add a new web service:

1. Before you can add a new web service, verify that the Intelligent Capture Server and the Web Services Coordinator Service are both running.
2. In the **Intelligent Capture Administrator** window, select **Web Services** from the navigation panel. The **Web Services** pane displays.
3. Select **View Services** from the **Web Services** pane. This displays the **Services** pane which lists available services.
4. At the bottom of the **Services** pane, click **Add**. The **Define Service** pane of the **New Service Setup Wizard** displays.
5. Complete the **Define Service** step:
   a. In the **Select WSDL** field, type the full path and file name of the Web Services Description Language (*WSDL*) file that describes the available methods within the web services client. Click **Browse**, then navigate to the *WSDL* file located here: `<<drive>>:\Program Files\InputAccel\Client\src\Sample Capture System\ScriptSource\Client-side Scripts\WSInput\Rescan\IARescanWS.wsdl`. Click **Open**. This displays the path and file name of the selected file in the **Select WSDL** field.
   b. Click **Parse**. The **Select WSDL** field clears and, if parsing succeeds, the **Service** field displays the Service Name defined within the *WSDL* file. If an

error occurs while parsing, the **Service** field remains empty and an error message appears near the top of the pane.

c. Under **Define service name**, select the appropriate option to keep the Service Name that was parsed from the *WSDL* file or set a different name. If you select the **Set different name** option, type the Service Name in the adjacent field.

> **Note:** The specified service name will become part of a *URL* when the service is published to a web service hosting; therefore, the virtual path to the *URL* should not exceed 2000 characters and may only use characters that are valid in an *HTTP* request.

d. (Optional) Type a description of the web service in the **Description** field.

6. Click **Next** to display the **Correlation Mapping** pane.

7. Complete the **Correlation Mapping** step:

a. Under **Methods**, select each of the listed methods in turn and do one of the following:

- If the method will create new batches, then select the **No Correlation ID** option.
- If the method will insert data into an existing batch, then map one or more methods to a *`Correlation ID`* by using one of the following:
  - To use a *`Correlation ID`* located in the *SOAP* header, choose the **Correlation ID is Located in SOAP Header** option, and then type the name of the *SOAP* header parameter in the adjacent field. *SOAP* header parameter identifiers may contain only letters (A-Z, a-z), numerals (0-9) and '_' symbol, and must not begin with a numeral.
  - To use a *`Correlation ID`* located in a method parameter, select the **Correlation ID is Located in Method Parameter** option, and then select one or more parameters in the adjacent list.

> **Notes**
>
> - If the Web Services Input module will be using this service to create batches (as the first module step in a process), do not map a *`Correlation ID`*. Only methods that do not have a *`Correlation ID`* mapped to them will be present in the **Mapped method** list. If all methods are mapped, then the service will not be present in the **Service for mapping** list. Both lists are displayed in the Web Services Input setup mode window.
> - If the Web Services Input module will use this service to add data to an existing batch (in a position other than the first module step in a process), then map at least one method to a *`Correlation ID`*. Only methods that have a *`Correlation ID`* mapped to them will be present in the Web Services Input module's **Mapped method** list. If

no methods are mapped, then the service will not be present in the **Service for mapping** list. Both lists are displayed in the Web Services Input setup mode window.

The **Methods** table displays a red check (✔) in the Mapped column for each method that is mapped to a *`Correlation ID`*.

b. Click **Next** to display the **Register Service** pane.

8. Verify the settings with which the web service will be registered. To make changes, click **Back** to return to the **Correlation Mapping** pane; otherwise, click **OK** to register the web service and close the wizard.

Related Topics

"Permissions Required for Web Services" on page 254

"Configuring Hostings" on page 256

9.12.1.2 Permissions Required for Web Services

An important aspect of adding a web service, as with setting up any module in Intelligent Capture, is to create operator roles and give those roles the appropriate permissions for running a module or service. For more information on roles and permissions, see "Managing Security" on page 130.

Permissions required for a user to run Web Services Input:

- Server.Login - Login to the Intelligent Capture Server.
- Server.Read.Module.Data - Read module data.
- Server.Write.Module.Data - Write module data.
- Server.Create.Batch - Create or modify a new batch.
- System.BatchModify - Write batch data.
- System.BatchRead - Read batch data.
- System.ServerRead - Read non-module server data (such as registry values).
- System.ProcessRead - Read process data.
- System.ProcessModify - Change process data (if using naming schema tags).
- System.SecurityRead - Read *ACL* security data (necessary to create batches for Web Services Input if used as the first process step)
- System.SecurityModify - Write *ACL* security data. This permission is required to make any security changes to the roles, process, batch, and department ACLs.

Related Topics

"Configuring Roles" on page 131

"Intelligent Capture Permissions List" on page 381

"Understanding Permissions" on page 134

9.12.1.3 Viewing All Web Services

The details of each web service registered within the Intelligent Capture Web Services subsystem are available in the Intelligent Capture Administrator.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view all web services:

1. In the **Intelligent Capture Administrator** window, select **Web Services** from the navigation panel to display the **Web Services** pane.
2. Select **View Services**. The **Services** pane displays a table of registered web services.
3. Under **Services**, select a web service, and then do any of the following:
   - If the first column of the table displays a  button, then the web service has been published to one or more hostings. Click the button to expand the entry and display the hosting information, including computer name, status, virtual directory, port, and whether the hosting is using Secure Sockets Layer (*SSL*).
   - To add a new web service, click **Add**. This displays the **New Service Setup Wizard: Define Service** pane.
   - To delete the selected web service, click **Delete**. This displays the **Remove Service** window, listing the processes and batches dependent on the selected web service. To delete the web service, click **OK**.
   - To view and change the settings of the selected web service, click **Settings**. This displays the **Service Properties** window for editing the web service description and the *`Correlation ID`* mappings.
   - To refresh the list of web services, right-click to open the context menu and click **Refresh**.

Related Topics

"Intelligent Capture Permissions List" on page 381

9.12.1.4 Changing Web Service Settings

Use the Intelligent Capture Administrator to change certain settings of web services that have been registered in the Intelligent Capture Web Services subsystem.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To change the settings of a web service:

1. In the **Intelligent Capture Administrator** window, select **Web Services** from the navigation panel to display the **Web Services** pane.
2. Select **View Services**. The **Services** pane displays a table of registered web services.
3. In the **Services** table, select a web service and click **Settings**. This displays the **Service Properties** window.
4. In the **View** list box, select one of the following options:
   - **General Settings**: Displays the **Name** and **Description** fields. The **Name** field is read-only and displays the registered Service Name that was specified when the web service was initially added. The **Description** field displays the web service description.
   - **Mapping Settings**: Displays the same options as the **New Service Setup Wizard: Correlation Mapping** pane, to change how *`Correlation IDs`* are mapped.

Related Topics

"Intelligent Capture Permissions List" on page 381

9.12.2 Configuring Hostings

Adding a web service hosting prepares an instance of a web server to handle requests from and responses to third-party web service clients. One step in adding a hosting is publishing one or more web services that have been registered within the Intelligent Capture Web Services subsystem. Add multiple web service hostings as needed (one per computer name), either to balance high traffic or to isolate external (internet) requests and responses from internal (intranet) requests and responses. The Intelligent Capture Administrator displays a list of existing hostings and enables users to configure settings on individual hostings.

9.12.2.1 Adding a Hosting

To add a hosting, define the computer that will act as a web server, select the web services to publish on the hosting, and then register the hosting within the Intelligent Capture Web Services subsystem.

The Web Services Hosting service requires administrator permissions to accept *HTTP* connections. However, a small utility called `PortReserve` enables you to reserve a port for a non-administrative account through which the Web Services Hosting service can accept *HTTP* connections. This utility is installed in the `Client\binnt` folder.

To reserve port 8080 with this utility, run the following at the command prompt:

```
portreserve -p:8080 -u:User -d:Domain
```

To remove the reservation of port 8080, run the following at the command prompt:

```
portreserve -p:8080 -u:User -d:Domain -r
```

Note: To add, remove, or query *HTTPS* reservations, add the /*SSL* key to command line.

HTTP and *HTTPS* reservations cannot exist simultaneously at the same port.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To add a new hosting:

1. In the **Intelligent Capture Administrator** window, select **Web Services** from the navigation panel to display the **Web Services** pane.
2. Select **View Hostings** from the **Web Services** pane. This displays the **Hostings** pane.
3. At the bottom of the **Hostings** pane, click **Add** to display the **Define workstation** pane of the **New Hosting Setup Wizard**.

   Note: If a hosting is added or the hosting configuration is changed while processing a web request, the Web Services Hosting service will reject the connection with the web client and abort all connections affected by these changes.

4. Complete the **Define workstation** step:

   a. In the **Hosting name** field, type the machine name or *IP* address of the computer that will service the hosting. The **Hosting name** must be less than 1000 characters and may only contain characters that are valid in a Microsoft Windows computer name or a valid *IP* address.

   b. (Optional) Type a description of the web service in the **Description** field.

   c. Click **Next**. The **Set Services** pane displays.

5. Complete the **Set services** step:

   a. Under **Available services to register on this hosting**, select a web service to publish on this hosting. If the web service is not listed, then return to "Adding a Web Service" on page 252 for instructions on how to register the web service. To skip publishing a web service at this time, skip to step c. Web services can be published at any time after the hosting is registered.

   b. Click **Register** to publish the selected web service.

   c. In the **Service Registration** window that displays, enter the **Virtual path**. This value represents the *URI* to be used when making a request to the Web Services Input module.

   d. Select the **Use SSL** check box to ensure secure communications on this hosting.

   e. Click **OK** to close this window. The assigned *URL* displays in the **Registered services** list.

   f. Click **Next** to display the **Register Hosting** pane.

6. Complete the **Register hosting** step by verifying the settings with which the hosting will be registered. To make changes, click **Back** to return to the **Set services** pane; otherwise, click **OK** to register the hosting and close the wizard.

Caution

Do not attempt to connect one instance of the Web Services Hosting service to multiple Web Services Coordinator instances. This is not a supported configuration and will result in a sharing conflict, as each Web Services Coordinator attempts to reconfigure the common hosting instance with its own rules.

Related Topics

"Intelligent Capture Permissions List" on page 381

"Configuring Web Services" on page 252

9.12.2.2 Viewing All Hostings

After a hosting has been registered within the Intelligent Capture Web Services subsystem, its settings are displayed in the Intelligent Capture Administrator.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To view all hostings:

1. In the **Intelligent Capture Administrator** window, select **Web Services** from the navigation panel to display the **Web Services** pane.

2. Select **View Hostings**. This displays the **Hostings** pane that displays a table of all of the registered web service hostings.

3. In the **Hostings** table, select a hosting, and then do any of the following:

   - Check the status of the hosting by noting the icon in the **Status** column. It displays a green up arrow ( ) to indicate that the hosting is up, or a red down arrow ( ) to indicate that the hosting is down. For a hosting to properly display a green arrow, it must be configured with a valid *IP* or machine name, and must be running the Web Services Hosting service.
   - If the first column of the table displays a button, then the hosting has one or more published web services associated with it. Click the button to expand the entry and display the web services information, including Service Name, virtual directory, port, whether the hosting is using Secure Sockets Layer (*SSL*), and description.
   - To add a new hosting, click **Add**. The **New Hosting Setup Wizard: Define workstation** pane displays.
   - To delete the selected hosting, click **Delete**.
   - To view and change the settings of the selected hosting, click **Settings**. The **Hosting Properties** window displays.
   - To refresh the list of hostings, right-click to display the context menu, and click **Refresh**. If any other instances of the Intelligent Capture Administrator have registered or modified any hostings, refreshing updates the table with the latest information.

Related Topics

"Intelligent Capture Permissions List" on page 381

9.12.2.3 Changing Hosting Settings

Certain settings of hostings registered in the Intelligent Capture Web Services subsystem are modifiable in Intelligent Capture Administrator.

Note: If a hosting is added or the hosting configuration is changed while processing a web request, the Web Services Hosting service will reject the connection with the web client and abort all connections affected by these changes.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To change the settings of a hosting:

1. In the **Intelligent Capture Administrator** window, select **Web Services** from the navigation panel to display the **Web Services** pane.

2. Select **View Hostings**. The **Hostings** pane displays a table or registered hostings.
3. In the **Hostings** table, select a hosting and then click **Settings**. This displays the **Hosting Properties** window.
4. Do any of the following:
   - To change the hosting description, type new text in the **Description** field.
   - To publish a web service, select the web service under **Available services to register on this hosting**, and then click **Register**. The **Service Registration** window displays, where you can enter the **Virtual path** and select to **Use SSL**. After configuring these settings, click **OK**. The assigned *URL* is displayed in the **Registered Services** list.
   - To remove a published web service from the hosting, select the web service from the **Registered services** list, and then click **Unregister**.

Related Topics

"Intelligent Capture Permissions List" on page 381

9.12.3 Defining Web Services Settings

Global options are settings that affect the entire Intelligent Capture Web Services subsystem.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

To define web services settings:

1. In the **Intelligent Capture Administrator** window, select **Web Services** from the navigation panel to display the **Web Services** pane.
2. Select **Web Services Settings**. This displays the **Web Services Settings** pane.
3. In the **WS Hosting connection: attempt interval (sec)** field, specify the interval, in seconds, at which the Web Services Coordinator attempts to connect to the Web Services Hosting service. The default value is 20 seconds.
4. In the **Incoming web request timeout (sec)** field, specify the number of seconds the Web Services Coordinator should wait before deleting web service requests that have not been processed. The default value is 86,400 seconds (24 hours).

   Note: Changing this value has no impact on current tasks. Restart the Web Services Coordinator before this change takes effect for all incoming *SOAP* requests.
5. In the **TCP port used for connections to Web Services Coordinator** field, specify the *TCP* port that the Intelligent Capture Administrator and the Web

Services Input module use to connect to the Web Services Coordinator service. The default value is 12007.

6. Click **OK** to save these settings and return to the previous pane.

Related Topics

"Intelligent Capture Permissions List" on page 381

9.13 Common Tasks in the Intelligent Capture Administrator

Some tasks and functionality are common throughout the Intelligent Capture Administrator. These tasks are described in this section.

9.13.1 Using the Print Feature

All Intelligent Capture Administrator windows and panes display a **Print** link in the right top corner. The **Print** link has two functions:

- The **Print** link generates a new page if the window or pane contains an information table. The print page displays a preview of the table. Users can select the rows to print.
- If the window or pane does not contain an information table then the **Print** link invokes the print feature. To **Print** use the default print features.

To print a table:

1. In a window or pane that displays a table click **Print**. The **Print** window displays.
2. The window is divided into frames (top, bottom, bottom left, and bottom right). Select the appropriate frame options to print:
   - **Frame at the top**: Prints the frame at the top of the page.
   - **Frame at the bottom**: Prints the frame at the bottom left of page.
3. Select one of the following options to select the print options:
   - **Selected rows**: Prints the selected rows of the table. The **Print Preview** window displays only the selected rows.
   - **Current page**: Prints all of the rows displayed in the table.
   - **Page range**: Prints all of the rows specified in the page range.
     - In the **From** and **To** field set the first page and the last page of the print range.
   - **All pages**: Prints all rows in the table.
4. Click **OK** the **Print Preview** window displays.

5. In the **Print Preview** window click:

   Note: In **Print Preview** the term page is the physical piece of paper sent to the printer and not the frames of the table. When you select a page range from 1 to 2 (2 table frames) the print preview may display more than 2 pages and print more than 2 pages.

   a. **Previous**: To go to the previous page. The **Previous** button is disabled if the first page is displayed.

   b. **Next**: To go to the next page. The next button is disabled if the last page is displayed.

   c. **Print**: To send the pages to the printer. The print window displays.

      - Select **Print** to print the selected data.

Related Topics

"Customizing Information Tables Using the Column Manager" on page 112

9.13.2 Renaming a Component in Intelligent Capture Administrator

Most components in Intelligent Capture Administrator can be renamed.

To rename a component:

1. In the **Intelligent Capture Administrator** window, navigate to the pane that lists the component to rename.
2. Select the item to rename and click **Settings**. The settings for the selected item is displayed.
3. Rename the item and the click **OK**. The item is now renamed.

Related Topics

"Deleting a Component in Intelligent Capture Administrator" on page 263

"Using the Print Feature" on page 261

9.13.3 Deleting a Component in Intelligent Capture Administrator

Most components in Intelligent Capture Administrator can be deleted.

To delete a component:

1. In the **Intelligent Capture Administrator** window, navigate to the pane that lists the component to delete.
2. Select the item to delete and click **Delete**. The selected item is deleted from the system.

Related Topics

"Renaming a Component in Intelligent Capture Administrator" on page 262

"Using the Print Feature" on page 261

9.13.4 Updating or Refreshing the Information Listed in Intelligent Capture Administrator Panes

Changes made in the Intelligent Capture Administrator are updated when you refresh the relevant pane.

To refresh a pane:

1. In the **Intelligent Capture Administrator** window, navigate to the pane that lists the component that is updated. For instance, if the information for an installed process is updated or another process is installed, select **Systems** from the navigation panel and then click **View Processes** to list all installed processes.
2. Select an item from the table, right-click, and then select **Refresh List** from the menu. The pane is updated with the latest information.

Note: Pressing the **F5** key does not refresh any of the Intelligent Capture Administrator panes. Instead, it displays the default start page (**Batch Traffic** pane), or the start page configured in the **Default Settings** or **Custom Settings** panes.

Related Topics

"Specifying Intelligent Capture Administrator Default Settings" on page 110

"Setting Preferences for Your Work Environment" on page 111

"Using the Print Feature" on page 261

9.14 Error Messages in Intelligent Capture Administrator

In Intelligent Capture Administrator, error messages and validation messages are displayed when there are errors in the requested functionality. Validation error messages display in popup windows or are embedded in the Intelligent Capture Administrator

panes. Error messages consist of a title and a description of the error.

A comprehensive list of error messages is available in *OpenText Intelligent Capture - Module Reference (ECPCORE-CMD)*.

Chapter 10

Intelligent Capture Administrator Windows

The topics within this section provide descriptions of windows accessible from the software. The topics list the *UI* element name and a brief description of actions available from the window.

10.1 Access Control List

Access Control Lists (*ACL*) allow definition of access permission for modules, departments, batches, and processes. The **Access Control List** window is displayed from any pane displaying modules, departments, batches, or processes. The **Access Control List** window can remain open while browsing in Intelligent Capture Administrator.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-1: Access Control List Window

Element	Description
ACL for the following (objects)	Displays a list of the selected items.
Select a user or group to view or modify their permissions	Select a user or group from the list. If necessary, click the **Add** button to open the **Select User or Group** window to add to the list.
Permissions for selected users or groups	Select the permissions to assign to the selected users or groups.

Related Topics

"Intelligent Capture Permissions List" on page 381

"Predefined Roles" on page 386

10.2 Add Batch

Batches are created from an existing installed process using the **Add Batch** window. For information about creating a batch, see "Adding a Batch" on page 170.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-2: Add A Batch Window

Element	Description
Based on process	Displays the name of the process that the batch is based on.
Batch name	The name of the batch.
Name schema	The naming schema, displays if the process is configured to use a naming schema.
Use default priority from Process	Indicates that the batch should inherit its priority from the process it is based on.
Batch priority	The processing priority for the batch.
Description	Additional notes about the process.
OK	Saves the new batch and exits the window.
Cancel	Closes the window without saving the batch.

Related Topics

"Exporting a Batch" on page 181

"Moving a Batch" on page 182

"Intelligent Capture Permissions List" on page 381

"Customizing Information Tables Using the Column Manager" on page 112

10.3 Add Roles and Role Settings

The **Add Roles** and **Role Settings** panes enable definition of roles and the permissions and members assigned to those roles.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-3: Add Roles and Role Settings Panes

Element	Description
Name	The name assigned to the role.

Element	Description
Description	The description of the role.
Available Permissions	Permissions available to assign to the role.
Selected Permissions	Permissions assigned to the role.
Permission Description	Provides a brief description of the selected permissions.
Available Members	Members registered in Intelligent Capture Administrator that are available to assign to the role.
Selected Members	Members registered in Intelligent Capture Administrator that are assigned to the role.
Find Member	Opens the **Select User or Group** window to add to the **Current Member** list.

Related Topics

"Adding Users and Groups to Roles" on page 142

"Roles" on page 292

"Intelligent Capture Permissions List" on page 381

10.4 Intelligent Capture Administrator

This section discusses the options available in the **Intelligent Capture Administrator** window. Options include:

Table 10-4: Intelligent Capture Administrator Window

Element	Description
Batch Traffic	Provides batch related information that enables administrators to monitor batch traffic in the Intelligent Capture system.
Admin Review	Displays a quick status of all batches that are on hold or that have errors, enabling an administrator to quickly locate trouble spots in their work centers.
Systems	Provides the functionality to view and manage system settings, including managing Intelligent Capture Servers, ScaleServer groups, Workstations, Departments, Data Access Layers, Processes, Modules, and Connections.

Element	Description
Licensing/Security	Defines various aspects of Intelligent Capture security, including adding and managing license codes, activating Intelligent Capture Servers, defining roles and assigning permissions to users and groups.
Reports/Logs	Manages reporting, logging, and purging capabilities of the Intelligent Capture system.
Batch Finder	Performs simple and advanced searches and filtering to help find batches, and enables users to save search and filter definitions for future use.
Options	Defines global and user options for the Intelligent Capture Administrator. Global options define the options that apply to all instances of the Intelligent Capture Administrator running on any workstation. User options override global options and apply only to the logged-in user.
Web Services	Manages web services for Intelligent Capture, including managing web services and web service hostings. **Note:** The **Web Services** options are unavailable unless the Web Services components have been installed.

10.4.1 Batch Traffic

The Batch Traffic pane provides the following batch related information that enables administrators to monitor batch traffic in the Intelligent Capture system.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Page Refresh Rates automatically refresh this page. If auto refresh occurs while performing administrative tasks on one of the screens, any work being performed can be disrupted. When performing administrative tasks on this screen, use the **Auto Refresh** link on the particular pane to turn off auto refresh. When finished, click the link again to switch auto refresh back on.

Table 10-5: Batch Traffic Pane

Element	Description
Batches table	Lists batches in the system.
Settings	Click to display the settings of the selected batch.
Delete	Click to delete the selected batch. If prompted, enter a reason. **Notes** • The maximum length for the reason is 4000 characters. • Whether to prompt for a reason is set by the CaptivaBatchDeleteReason log rule.
Available columns in the batches table:	
Batch ID	The batch ID.
Name	The batch name.
Status	The batch status. Batch status includes the following types: • **Done**: The module step has finished processing the task. • **Not Ready**: No tasks are currently queued for the step. • **Ready**: Tasks are queued for the step. • **Working**: The module step is currently processing the task. • **Hold**: The tasks associated with the module step are on hold. • **Sent**: The tasks associated with the module step are sent by the Intelligent Capture Server. • **Error**: The entire batch is in error. • **Batch Task Error**: At least one batch task is in error. **Note:** The default status for the batch is **Not Ready**. But if at least one task is **Done** and others are **Not Ready**, then the batch status will be **Done**. **Done** really means there are currently no more tasks to process for this batch. It does not mean the batch has completely been processed.
Server	The name of the Intelligent Capture Server where the batch resides.

Element	Description
Process	Name of the process on which the batch is based.
Error	A selected check box indicates that the batch is in error. If the batch is in error, the server does not send any tasks from this batch.
Hold	A selected check box indicates that the batch is on hold.
Tasks with Errors	The number of tasks in the batch that are in error.
Tasks Active	The number of active tasks for the batch.
Tasks Completed	The number of tasks for the batch that have the "Done" status.
Tasks Not Ready	The number of tasks for the batch that are not yet ready to be processed.
Tasks Sent	The number of tasks for the batch that are sent for processing.
Tasks Working	The number of tasks for the batch that are currently being processed.
Last Sync	The last time that the batch data was written to disk.
Creation Date	Date and time that the batch was created.
Last Modified	Date and time when the batch was last modified.
Priority	The batch priority.
Child Hold	The check box is checked if a hold has occurred.
Server ID	Serial number of the server where the batch resides.
Child Error	The check box is checked if an error has occurred.
Status Message	Displays the status of the batch. This value is set in the *IPP* using the IA Value <*SetASCII*> with key `$batch=<batchID>/status`.
Locks	Count of locks present on the batch.

Element	Description
Chart: Displays the installed processes or module steps in a process depending on the user's selection. The bars on the chart provide quantitative data for the displayed processes or steps: • *Red hatch bar*: Count of batches in error, hold, or priority 0. Count of tasks in error. • *Gray bar*: Count of batches or tasks in ready, working, or sent status. • *White bar*: Count of batches or tasks with any status other than the statuses represented by the Red hatch bar and the Gray bar.	
Modules *table*: Displays the modules connected for all installed processes or specific processes depending on the user's selection.	
Status bar at the bottom of the pane	Displays the logged in user name.

Related Topics

"Understanding the Components of the Batch Traffic Pane" on page 164

"Viewing All Batches in the System" on page 166

"Viewing Batches for a Specific Installed Process" on page 168

"Exporting a Batch" on page 181

"Configuring a Batch Step in Setup Mode" on page 169

"Customizing Information Tables Using the Column Manager" on page 112

10.4.1.1 Modules Table - Batch Traffic Pane

The modules table in the **Batch Traffic** pane displays information about the module connections currently active in the system. When no batches are selected, the table displays all connected modules. When a batch is selected, the connected modules for the batch steps are displayed. This information is for the module connections only and does not provide specific insight into the selected batch. Right-click a module to view additional information, disconnect the module, or refresh the module list.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Table 10-6: Modules Table - Batch Traffic Pane

Element	Description
Available columns in the **Connected modules** table:	
Module	Full name of the module.

Element	Description
Server	Server name where module is connected.
Workstation	Name of the workstation where module is running.
User	Name of the user name connected to the module.
Department	Name of the department(s) specified when the module was started.
Tasks	Number of unfinished tasks the module is currently processing.
Last Response (seconds)	Time period since the module last responded to the server.
Executable	Name of the module executable file.
Server Group	Name of the ScaleServer group to which the module is connected.
Server ID	Serial number of the server.
UUID	Unique ID for the connection.

Related Topics

"Viewing Module Connections and Disconnecting Modules" on page 149

"Viewing, Adding, Modifying, and Deleting Modules" on page 150

"Viewing and Defining Access Control for Modules" on page 151

"Customizing Information Tables Using the Column Manager" on page 112

10.4.2 Admin Review

Select **Admin Review** from the navigational panel to view batches that have errors, holds or both. For more information, see "Locating and Fixing Batch Problems" on page 194.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Table 10-7: Admin Review Pane

Element	Description
Admin Review pane	Displays batches in an error or hold state and enables the user to fix the batch errors. The **Admin Review** pane is divided into three panes: Batches table (top table), Chart, and the modules table (bottom table). To understand how the tables interact in the window, see "Understanding the Components of the Batch Traffic Pane" on page 164.
Batches table (top table in the right pane)	Displays a list of batches that contain errors or holds. For a description of the columns in the table, see Batch Traffic topic, specifically the "Available columns in the batches table" section of the table.
Chart (lower left area in the right pane)	Displays the installed processes or module steps in a process depending on the user's selection. **Note:** This chart displays processes or module steps information for all processes, not just those processes associated with batches that are in error or hold. When no processes or batches are selected, the chart displays all processes. When a process or batch is selected, the chart displays the steps associated with the selection. The bars on the chart provide quantitative data for the displayed processes or steps: • *Red hatch bar*: Count of batches in error, hold, or priority 0. Count of tasks in error. • *Gray bar*: Count of batches or tasks in ready, working, or sent status. • *White bar*: Count of batches or tasks with any status other than the statuses represented by the Red hatch bar and the Gray bar.
Modules table (lower right area in the right pane)	Displays the modules connected for all installed processes or specific processes depending on the user selection. For a description of the columns in the table, see "Connections" on page 285 topic, specifically the "Available columns in the Connected modules table" section of the table.

Related Topics

"Retriggering a Batch Step" on page 195

"Customizing Information Tables Using the Column Manager" on page 112

"Viewing All Batches for a Process, Module, or Server" on page 196

"Intelligent Capture Permissions List" on page 381

10.4.3 Systems

This section discusses the options available in the **Systems** pane of the **Intelligent Capture Administrator** window. Options include:

Table 10-8: Systems Pane

Element	Description
Servers area	
View Servers	Displays the **Servers** pane and lists all the Intelligent Capture Servers added to the system. Options include adding new Intelligent Capture Servers, viewing or modifying the server settings, and deleting Intelligent Capture Servers from the system.
View ScaleServer Groups	Displays the **ScaleServer Groups** pane and lists all the ScaleServer groups added to the system. Options include adding new ScaleServer groups, viewing or modifying the ScaleServer group settings, viewing the Intelligent Capture Servers added to a ScaleServer groups, and deleting ScaleServer groups from the system.
Processes area	
View Processes	Displays the **Processes** pane and lists all the processes installed on the system. Options include adding processes, installing upgraded processes, viewing or modifying the process settings, viewing the module steps for a selected process, specifying the *ACL* for the process, adding a batch based on a process, configuring a module step in setup mode, viewing and modifying IA Values and indexed IA Values for a process, and deleting a process from the system.
Modules area	

Element	Description
View Modules	Displays the **Modules** pane and lists all the client modules in the system. Options include adding new client modules, viewing or modifying module settings, specifying the *ACL* for each added client module, and deleting a client module from the system.
View Monitor	Displays the **Monitor** pane and lists the client modules that are currently processing batches on the Intelligent Capture Server. For more information, see Monitor pane on page 97.
View Module Connections	Displays the **Connections** pane and lists all the modules that are currently connected to the system. Connected modules can be monitored for system activity. Options include disconnecting and connecting client modules.
Departments area	
View Departments	Displays the **Departments** pane and lists all the departments added to the system. Options include adding new departments, specifying the *ACL* for each department, viewing or modifying the department settings, and deleting departments. Note that departments may not be deleted if they are in use; that is, defined within any resident process or batch.

10.4.3.1 Servers

The **Servers** pane lists the Intelligent Capture Servers defined in the system.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Page Refresh Rates automatically refresh this page. If auto refresh occurs while performing administrative tasks on one of the screens, any work being performed can be disrupted. When performing administrative tasks on this screen, use the **Auto Refresh** link on the particular pane to turn off auto refresh. When finished, click the link again to switch auto refresh back on.

Table 10-9: Servers Pane

Element	Description
Registered servers table	Lists the servers added to the system. The following client-server data encryption icons might be displayed: •  Encryption is enabled for server. •  Encryption is enabled for the server in a ScaleServer group. •  Restart is required for encryption to take effect on the corresponding server.
Filter	Lists the Intelligent Capture Servers in the system. Users can select from the list and view information for a specific server or ScaleServer Group.
Add	Click to add an Intelligent Capture Server to the system.
Settings	Click to view the settings of the selected Intelligent Capture Server and set client-server data encryption. **Note:** Viewing and editing server settings is only available in Intelligent Capture Administrator 7.5 and later.
Delete	Click to delete the selected Intelligent Capture Server from the system.
Available columns in the **Registered servers** table:	
Serial Number	The license ID of the Intelligent Capture Server.
Name	Intelligent Capture Server name.
Service Name	The service name of the server.
Connected	The connection status of the Intelligent Capture Server.
Secured	Whether network encryption between client modules and Intelligent Capture Server is enabled.
Free Space (MB)	Free disk space on the server in megabytes.

Element	Description
Free Space (%)	Percentage of free disk space on the server.
ScaleServer Group	Name of the ScaleServer group that the Intelligent Capture Server is attached to.
Version	Version of the server installed on the machine.

Related Topics

"Adding and Connecting Intelligent Capture Servers" on page 116

"Activating Intelligent Capture Servers" on page 117

"Managing Client-Server and Batch Staging File Data Encryption" on page 139

"Customizing Information Tables Using the Column Manager" on page 112

10.4.3.2 ScaleServer Groups

The **ScaleServer Groups** pane displays the list of ScaleServer groups defined in the system and the Intelligent Capture Servers associated with each ScaleServer group.

Table 10-10: ScaleServer Groups Pane

Element	Description
Registered ScaleServer groups table	Lists the ScaleServer groups defined in the system.
Add	Click to add a new ScaleServer group.
Settings	Click to modify the selected ScaleServer group, including setting client-server data encryption. The following client-server data encryption icons might be displayed: •  Encryption is enabled for the server in a ScaleServer group. •  Restart is required for encryption to take effect on the corresponding server.
Delete	Click to delete the selected ScaleServer group.
Available columns in the **Registered ScaleServer groups** table:	

Element	Description
Name	Lists the names of all ScaleServer groups defined in the system.
Servers Attached	Number of Intelligent Capture Servers attached to the ScaleServer group.
Attached servers for the selected ScaleServer groups	Lists all Intelligent Capture Servers attached to the selected ScaleServer group. The available columns in the table lists the various server settings. For a description of the various columns, see "Available columns in the Registered servers" table in the Servers topic.

Related Topics

"Adding and Connecting ScaleServer Groups" on page 128

"Viewing or Modifying ScaleServer Settings" on page 130

"Viewing ScaleServer Groups" on page 126

"Listing Intelligent Capture Servers for each ScaleServer Group" on page 127

"Managing Client-Server and Batch Staging File Data Encryption" on page 139

"Customizing Information Tables Using the Column Manager" on page 112

10.4.3.3 Processes

The **Processes** pane displays the list of processes installed on the system and the module steps associated with each process.

Notes

- The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.
- **Page Refresh Rates** automatically refresh this page. If auto refresh occurs while performing administrative tasks on one of the screens, any work being performed can be disrupted. When performing administrative tasks on this screen, use the **Auto Refresh** link on the particular pane to turn off auto refresh. When finished, click the link again to switch auto refresh back on.

Table 10-11: Processes Pane

Element	Description
Filter	Specify the Intelligent Capture Server to filter on. The list of processes is filtered to display those processes installed on the selected Intelligent Capture Server.
Processes table	List the processes installed on the system.
Add	Click to install a process on an Intelligent Capture Server.
Settings	Click to view or modify the settings of the selected process.
Delete	Click to delete the selected process.
Available columns in the **Processes** table:	
Name	Name of the process.

Element	Description
Legacy	Checked if the process was created using Process Developer. Unchecked if the process was created using Intelligent Capture Designer. Some menu items are disabled for Intelligent Capture Designer processes because of their multi-file structure. Instead you should use Intelligent Capture Designer because it has extensive functionality for deploying and maintaining its processes on Intelligent Capture Servers. For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*. If the process was created in Intelligent Capture Designer, then the following functionality and context menu items are disabled: • Adding processes. • Upgrading processes. • Deleting processes unless all associated batches are deleted from the Intelligent Capture Server. • Renaming processes. • **Add Upgraded Process** • **Copy** – **Process** – **Settings to File** – **Settings** – **Single Setup Value** • **Paste** – **Settings from File** – **Settings** – **Single Setup Value**
Process ID	Process ID.
Total Tasks	The total number of tasks in batches based on this process. This is the sum of tasks that have been sent from the Intelligent Capture Server to a module instance, tasks that in the working state, and tasks that are ready to be sent for the process. It does not include tasks whose Priority is 0. To determine the number of pending tasks only, use **Tasks Queued**.

Element	Description
Batches Ready	The total number of batches ready to execute for the process.
Batches with Errors	The total number of batches for this process that are in the error state.
Batches on Hold	The total number of batches for this process that are in the on-hold state.
Batches Not Ready	The total number of batches for this process that are in the “Not Ready” state.
Batches Stopped	The total number of batches for this process that are stopped. Batches are stopped if their Priority is 0 (zero) or if either their error or hold status, or both, is set.
Batches Working	The total number of batches currently executing for this process.
Server	Name of the Intelligent Capture Server where the process is installed.
Tasks with Errors	The total number of tasks for this process that indicate an error state.
Tasks Queued	The total number of pending tasks for this process.
Total Batches	The total number of current batches in the system that are based on the process.
Priority	The process priority.
Batches With Priority 0	The total number of batches at priority 0 (zero) for this process. Processes at priority level 0 do not execute. A Priority of 0 usually indicates that the process code has detected some kind of error.
Batches Completed	The total number of batches for this process that are in the “Done” state.
Batches Sent	The total number of batches for this process that are in the “Sent” state.
Tasks Offline	The total number of tasks for this process that are in “offline” state.
Description	The process description.
Compile Time	The date and time when the process was compiled.
Intelligent Capture Process Developer Version	The version of Process Developer used to develop the process.
Original CaptureFlow	The name of the CaptureFlow used to install this process.

Element	Description
CaptureFlow Version ID	The version of the CaptureFlow used to install this process.
VBA Version	The version of Visual Basic that was used to create the process.
Process Compiler Version	Version of Process Developer that was used to compile the process.
Available columns in the **Process steps** table: Lists the module steps associated with the process selected from the **Processes** table:	
Step ID	The step ID.
Name	Name of the module step in the process.
Trigger	Trigger level for the module step as defined in the process.
Departments	The department defined for the module step in the process.
Module	The client module associated with the step.
Executable	Name of the executable file for the module associated with the step.

Related Topics

"Adding a Batch" on page 170

"Configuring a Process Step in Setup Mode" on page 157

"Viewing and Defining Access Control for a Process" on page 160

"Copying Step, Process, and Batch Settings" on page 197

"Customizing Information Tables Using the Column Manager" on page 112

10.4.3.4 Modules

The **Modules** pane displays information about the modules recognized in the system.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Page Refresh Rates automatically refresh this page. If auto refresh occurs while performing administrative tasks on one of the screens, any work being performed can be disrupted. When performing administrative tasks on this

screen, use the **Auto Refresh** link on the particular pane to turn off auto refresh. When finished, click the link again to switch auto refresh back on.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-12: Modules Pane

Element	Description
Modules table	Displays information about the modules in the system.
Filter	Limits the displayed modules to the selected server.
Add	Displays the **Add Module** window used to define a new module. In the **Add Module** window, the fields include: • **Name**: The module's name. • **Executable**: The name of the module's executable file. **Note:** Do not include ".exe" in the file name. • **Launch name**: The launch name assigned to the module. • **Related to process** check box: Indicates that the module is related to a process.
Settings	Displays the **Module Settings** window used to view and modify module settings. In the **Module Settings** window, the fields include: • **Display Name**: A user-specified name for the module. • **MDF Name**: The name of the module's MDF file. • **EXE/DLL Name**: The name of the EXE file or DLL file associated with the module. **Note:** Do not include ".exe" or any extension in the EXE/DLL name. • **Related to process** check box: Indicates that the module is related to a process.
Delete	Deletes the selected modules.
Batches using the selected modules	Lists the batches associated with the selected modules.
Processes using the selected modules	Lists the processes associated with the selected modules.
Available columns in the **Modules** table:	

Element	Description
Name	Module name.
Total Tasks	Total number of tasks for the module. This is the sum of the tasks that have been sent from the Intelligent Capture Server to a module instance, tasks that are in the working state, and tasks that are ready to be sent for the module). To determine the number of pending tasks only, use **Tasks Queued**.
Tasks Active	Number of tasks in the active state for this module. This includes tasks that are in the Ready, Sent, or Working state.
Tasks Queued	Number of tasks that are in the Ready state for this module.
Tasks with Errors	Number of tasks in the error state for this module.
Tasks Not ready	Number of tasks in the NotReady state for this module.
Department	Department names that apply to the module.
Process Related	Indicates that the module is related to a process if selected.
System	Indicates that the module is recognized by the system if selected.
Tasks Working	Number of tasks in the working state for this module.
Tasks Offline	Number of tasks that are offline for this module.
Tasks Completed	Number of tasks in the done state for this module.
Tasks Sent	Number of tasks in the sent state for this module.
Batches	Number of batches associated with the module.
Server	The server the module step is connected to.
Server ID	The server ID.
Processes	Number of processes associated with the module.
Executable	The module executable name.
Launch Name	Name of the executable that is used to start the module.

Related Topics

"Running Unattended Modules as Windows Services" on page 152

"Viewing Module Connections and Disconnecting Modules" on page 149

"Viewing, Adding, Modifying, and Deleting Modules" on page 150

"Viewing and Defining Access Control for Modules" on page 151

"Connections" on page 285

"Customizing Information Tables Using the Column Manager" on page 112

"Intelligent Capture Permissions List" on page 381

10.4.3.5 Connections

The **Connections** pane displays information about the module connections currently active in the system.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Page Refresh Rates automatically refresh this page. If auto refresh occurs while performing administrative tasks on one of the screens, any work being performed can be disrupted. When performing administrative tasks on this screen, use the **Auto Refresh** link on the particular pane to turn off auto refresh. When finished, click the link again to switch auto refresh back on.

Table 10-13: Connections Pane

Element	Description
Connected modules table	Displays information about the module connections in the system.
Filter	Limits the displayed module connections in the system.
Disconnect	Disconnects the selected module connections. **Note:** The module connection is reestablished only when the module is restarted.
Batches using the selected modules	Lists the batches associated with the selected module connections.

Element	Description
Available columns in the **Connected modules** table:	
Module	Full name of the module.
Server	Server name where module is connected.
Workstation	Name of the workstation where module is running.
User	Name of the user name connected to the module.
Department	Name of the department(s) specified when the module was started.
Tasks	Number of unfinished tasks the module is currently processing.
Last Response (seconds)	Time period since the module last responded to the server.
Executable	Name of the module executable file.
Server Group	Name of the ScaleServer group to which the module is connected.
Server ID	Serial number of the server.
UUID	Unique ID for the connection.

Related Topics

"Running Unattended Modules as Windows Services" on page 152

"Viewing Module Connections and Disconnecting Modules" on page 149

"Viewing, Adding, Modifying, and Deleting Modules" on page 150

"Viewing and Defining Access Control for Modules" on page 151

"Customizing Information Tables Using the Column Manager" on page 112

"Intelligent Capture Permissions List" on page 381

10.4.3.6 Departments

The **Departments** pane displays the list of departments defined the system

Table 10-14: Departments Pane

Element	Description
Name	Name of the department.
Add	Click to add a new department.
Delete	Click to delete a department. Departments that are in use (specified by any resident process or batch) may not be deleted.

Related Topics

"Adding and Deleting Departments" on page 147

"Viewing the List of Departments" on page 147

"Viewing and Defining Access Control for Departments" on page 148

10.4.4 Licensing / Security

This section discusses the options available in the **Licensing / Security** pane of the **Intelligent Capture Administrator** window. Options include:

Table 10-15: Licensing / Security Pane

Element	Description
Licensing area	
License Codes	Displays the **License Codes** pane and lists all license codes installed with a license file or manually entered into the system. Options include adding new license codes manually, importing license codes from a license file, viewing or modifying the license code settings, and deleting expired license codes from the system.
Module Licenses	Displays the **Module Licenses** pane and lists the licensed modules on each Intelligent Capture Server.
Server Activations	Displays the **Server Activations** pane and lists all Intelligent Capture Servers in the system and provides the server activation status. Also, enables activation of Intelligent Capture Servers.

Element	Description
Page Count Report	Displays **Page Count Report** pane, which lists the page count usage of Intelligent Capture Servers. See "Page Count Report" on page 292.
Security area	
Roles	Displays the **Roles** pane and lists all roles defined in the system. Options include adding new roles, modifying existing role settings and deleting a selected role.
Security Options	Displays the **Security** pane.

10.4.4.1 License Codes

The **License Codes** pane displays the license codes added to the system. The following information is displayed: Copyright (c) EMC Corporation All Rights Reserved

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Table 10-16: License Codes Pane

Element	Description
License Codes table	Lists the license codes in the system.
Import License	Click to add license codes from a license (*LIC*) file.
Delete Expired	Click to delete expired license codes.
Add	Click to add a license code manually.
Settings	Click to view or modify the license code settings of the selected license code.
Delete	Click to delete a selected license code.
Available columns in the **License Codes** table:	
Name	The server name, module executable, or group name that is licensed by the license code.
Server	The Intelligent Capture Server to which the license code applies.
Connections	Number of connections allowed to the **Name**.

Element	Description
Pages	Number of pages that the license can process.
Valid until	Expiration date of the license in <*YYMMDD*> format.
Issue date	The date that the license was issued in <*YYMMDD*> format.
Enter by	Date by which license must be entered to be usable.
Features	The list of feature codes licensed by the license code.
Disables	String containing the features that are disabled by this license code.
Status	The status of license code.
License Code	The actual license code string. For a description of license codes and the features they include, see "Server Licenses" on page 42.

Related Topics

"Importing License Codes from a License File" on page 124

"Adding License Codes Manually" on page 125

"Viewing or Modifying License Code Settings" on page 125

"Viewing License Codes by Module" on page 123

"Customizing Information Tables Using the Column Manager" on page 112

10.4.4.2 Module Licenses

The **Module Licenses** pane displays a list of licensed modules on each Intelligent Capture Server. The following information about each module is displayed:

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Table 10-17: Module Licenses Pane

Element	Description
Module Licenses table	Lists the licensed modules on each Intelligent Capture Server.
Available columns in the **Module Licenses** table:	
Executable	The executable name of the module without the file extension.
Used	Number of instances of the module that are connected to the Intelligent Capture Server.
Available	Number of remaining instances of this module that are licensed to connect to the Intelligent Capture Server.
Percent Copies Used	Percentage of licenses for this module that are currently in use.
Pages Used	Number of pages that have already been processed by this module using the current set of license codes.
Pages Available	Total number of pages that can be used. To get the remaining pages, the pages used must be subtracted from the pages available.
Percent Pages Used	Percentage of page licenses that have been used for the module on the Intelligent Capture Server.
Features	The list of feature codes licensed by the license code.
Server	Name of the Intelligent Capture Server on which the license code is installed.

Related Topics

"Importing License Codes from a License File" on page 124

"Adding License Codes Manually" on page 125

"Viewing or Modifying License Code Settings" on page 125

"Viewing License Codes Installed on the System" on page 122

"Customizing Information Tables Using the Column Manager" on page 112

10.4.4.3 Server Activations

The **Server Activations** pane assigns an activation code to an Intelligent Capture Server and enables users to activate the Intelligent Capture Servers when using a software activation key.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Table 10-18: Server Activations Pane

Element	Description
Server Activations table	Lists the servers in the system and their activation status.
Install activation file	Specify or **Browse** for the server activation file (*CAF* file) for the Intelligent Capture Server.
To activate a server, go to My Support	Link to My Support (https://support.opentext.com) to request for an Intelligent Capture Server activation code.
Activate Server	Click to display the **Activate Server** window and provide the activation code to activate the server.
Available columns in the **Server Activations** table:	
Server	The name of the Intelligent Capture Server.
File	Status of whether an activation file is installed for the Intelligent Capture Server.
Server Serial Number	The serial number of the activated server.
State	The activation state of the Intelligent Capture Server which includes the validity of the server activation and the expiring activation information.
Server ID	The unique Server ID of the Intelligent Capture Server.
Grace Period	The date that the server started the grace period.

Related Topics

"Activating Intelligent Capture Servers" on page 117

"Customizing Information Tables Using the Column Manager" on page 112

10.4.4.4 Page Count Report

Table 10-19: Page Count Report Pane

Element	Description
Server ID	The server ID of the Intelligent Capture Server.
Server Serial Number	The serial number of the Intelligent Capture Server.
Server	Name of the server.
Create Audit File	Creates an audit file of page count usage. The audit file is for technical services use only.
View Usage	Displays the usage pane that displays the number of pages that have been used for each license on each day for the past 15 months. You can click **Export to CSV** to create a CSV file and save it.

10.4.4.5 Roles

The **View Roles** link from the **Licensing / Security** navigation displays the **Roles** pane, that displays a list of all defined roles.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-20: Roles Pane

Element	Description
Roles table	Displays the **Name** and optional **Description** of the roles defined in the system.
Add	Displays the **Add Role** pane used to define a new role.
Settings	Displays the **Role Settings** pane used to view and modify role settings.
Delete	Deletes the selected role.
Available columns in the **Roles** table:	
Name	The role name.
Description	An optional description for the role.

Related Topics

"Adding Users and Groups to Roles" on page 142

"Defining Roles, Role Members, and Role Permissions" on page 132

"Configuring Roles" on page 131

"Add Roles and Role Settings" on page 266

"Viewing Roles" on page 131

"Intelligent Capture Permissions List" on page 381

10.4.5 Reports / Logs

The **Reports / Logs** pane provides access to reporting, logging, and purging of events and actions stored in the Intelligent Capture Database. For more information on reports and logs, see Managing Reports and Logs.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-21: Reports / Logs Pane

Element	Definition
Reports	
View Reports	Displays the **Reports** pane containing a list of reports currently defined in the system. Reports can be added, modified, deleted or used to generate report output from the **Reports** pane. The three most recently run or modified reports are also listed below the **View Reports** link.
View Report Definitions	Displays the **Report Definitions** pane containing a list of currently defined report definitions. Definitions can be added, modified, or deleted from the **Report Definitions** pane.
Purges	
View Purges	Displays the **Purges** pane containing the currently defined purges in the system. Purges can be added, modified, deleted or run from the **Purges** pane.
View Purge Definitions	Displays the **Purge Definition** pane containing a list of purge definitions currently defined in the system. Definitions can be added, modified, or deleted from the **Purge Definition** pane.
Logs	

Element	Definition
View Logs	Displays the **Logs** pane containing a list of logged events or actions. Logs can be viewed or deleted from the **Logs** pane.
View Log View Filters	Displays the **Log View Filters** pane containing a list of defined log view filters to view a subset of logs. The three most recently run or modified log filters are also listed.
View Log Rules	Displays the **Log Rules** pane containing a list of log rules defining what events or actions will generate a log. Log rules can be added, modified, or deleted from the **Log Rules** pane.

Related Topics

"Intelligent Capture Permissions List" on page 381

10.4.5.1 Reports

The **Reports** pane displays all reports collected in the Intelligent Capture Database. Reports provide a way to monitor most components of Intelligent Capture. The **Reports** pane enables generation of reports, as well as creation, deletion, and modification of reports.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-22: Reports Pane

Element	Description
Generate Report	Displays the **Reports Results** window that shows the results of the selected report.
Add	Displays the **Add Report** pane where new reports are created.
Save As	Makes a copy of the selected report in the **Add Report** pane, where you can make modifications and save the new report.
Settings	Displays the settings for the selected report in the **Report Settings** pane.

Element	Description
Delete	Deletes the selected reports.
Available columns in the **Reports** table:	
Name	The name of the report.
Definition Name	Then name of the report definition the report is based on.
Description	The description of the report.
Creation Date	The date and time when the report was created.
Modification Date	The date and time when the report was last modified.
Last Modified By	The user that last modified the report.

Related Topics

"Creating or Modifying a Report" on page 235

"Creating or Modifying a Report Definition" on page 233

"Generating and Viewing Reports in Crystal Reports Viewer" on page 236

"Report Definitions" on page 295

"Report Details" on page 431

"Understanding Report Definitions" on page 232

"Managing Reports and Logs" on page 205

"Viewing Report Definitions" on page 234

"Intelligent Capture Permissions List" on page 381

"Customizing Information Tables Using the Column Manager" on page 112

10.4.5.2 Report Definitions

The **Report Definition** pane enables creation, editing, and deletion of the report definitions, containing the tunable arguments for the report, the actual Crystal Reports project file, and a sample image of the report output. This pane lists all report definitions that are stored in the Intelligent Capture Database.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-23: Report Definitions Pane

Element	Description
Add	Displays the **Add Report Definition** pane where new report definitions are created.
Add Report	Displays the **Add Report** pane where the user can create a report.
Save As	Makes a copy of the selected report in the **Add Report Definition** pane, where you can make modifications and save the new report definition.
Settings	Displays the settings for the selected report definition in the **Add Report Definition** pane.
Delete	Deletes the selected report definition.
Available columns in the **Report Definitions** table:	
Name	The report definition name.
Crystal Reports File	The **Crystal Reports** file used to generate the report.
Stored Procedure	The name of the stored procedure used to generate the report.
Read Only	Read only reports are those put in the system upon generation of the database. Custom reports are not read only.
Description	The description of the report.
Parameters File	The name of the parameters *XML* file.
Sample Image Filename	The file name for the sample image for the report definition.

Related Topics

"Creating or Modifying a Report" on page 235

"Creating or Modifying a Report Definition" on page 233

"Generating and Viewing Reports in Crystal Reports Viewer" on page 236

"Reports" on page 294

"Understanding Report Definitions" on page 232

"Managing Reports and Logs" on page 205

"Viewing Report Definitions" on page 234

"Customizing Information Tables Using the Column Manager" on page 112

"Intelligent Capture Permissions List" on page 381

10.4.5.3 Purges

The **Purges** pane lists all purges stored in the Intelligent Capture Database. The **Purges** pane enables creation, editing, and deleting of purges.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-24: Purges Pane

Element	Description
Run Purge	Runs the selected purge.
Add	Displays the **Add Purge** pane where purges are created or modified.
Save As	Makes a copy of the selected purge in the **Add Purge** pane where new purges are created.
Settings	Displays the **Purge Settings** pane where the settings for the selected purge are displayed.
Delete	Deletes the selected purge.
Available columns in the **Purges** table:	
Name	The purge name.
Definition Name	The name of the **Purge Definition** used for the purge.
Last Successful Run	The date and time stamp of the last successfully completed run of the purge.
Schedule Option	The schedule option for the purge.
Start Time	The date and time stamp of when the purge should be started.
Schedule Days	Any combination can be set and defines which days of the week the purge should run.

Element	Description
Description	The description of the purge.
Creation Date	The date and time stamp when the purge was created.
Modification Date	The date and time stamp when the purge was modified.
Last Modified By	The user name (in the form Domain\User) of who last modified the purge.
Last Attempt	The date and time stamp of the last attempted run of the purge.
Last Error Code	The error number for the last unsuccessful run of the purge.
Running	When selected, the purge is running.

Related Topics

"Creating a Purge Definition" on page 248

"Creating a Purge" on page 249

"Purge Definitions" on page 298

"Purging the Intelligent Capture Database" on page 247

"Understanding Purging" on page 246

"Managing Reports and Logs" on page 205

"Viewing Purge Definitions" on page 250

"Viewing Purges" on page 251

"Customizing Information Tables Using the Column Manager" on page 112

"Intelligent Capture Permissions List" on page 381

10.4.5.4 Purge Definitions

Purge definitions are used to create purges that run a scheduled stored procedure to purge old report data.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-25: Purge Definitions Pane

Element	Description
Add	Displays the **Add Purge Definition** pane where purge definitions are created or modified.
Add Purge	Displays the **Purge Settings** pane where purges are created or modified.
Save As	Makes a copy of the selected purge definition and displays the **Add Purge Definition** where new purge definitions are created.
Settings	Displays the **Purge Definition Settings** pane where the settings for the selected purge definition are displayed.
Delete	Deletes the selected purge definition.
Available columns in the **Purge Definitions** table:	
Name	The name of the purge definition.
Stored Procedure	The name of the stored procedure to run for the purge.
Read Only	Read only purges are those put in the system upon generation of the database. Custom purge definitions are not read only.
Description	The description of the purge definition.
Parameters File	The name of the *XML* parameters file.

Related Topics

"Creating a Purge Definition" on page 248

"Creating a Purge" on page 249

"Purges" on page 297

"Purging the Intelligent Capture Database" on page 247

"Understanding Purging" on page 246

"Managing Reports and Logs" on page 205

"Viewing Purge Definitions" on page 250

"Viewing Purges" on page 251

"Customizing Information Tables Using the Column Manager" on page 112

"Intelligent Capture Permissions List" on page 381

10.4.5.5 Logs

The **Logs** pane displays all logs generated by the system. The type of logs generated are controlled by **Log Rules**, which can be static system rules or user-defined custom rules. All log rules are disabled by default. Log rules must be enabled if logs must be generated by the system.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Page Refresh Rates automatically refresh this page. If auto refresh occurs while performing administrative tasks on one of the screens, any work being performed can be disrupted. When performing administrative tasks on this screen, use the **Auto Refresh** link on the particular pane to turn off auto refresh. When finished, click the link again to switch auto refresh back on.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-26: Logs Pane

Element	Description
Filter	Select the type of logs to display, including custom log view filters.
Details	Displays the **Log Details** window providing details of the selected log. **Note:** If two or more logs are selected, the **Log Details** window will only provide details for the first selected log.
Delete	Deletes the selected logs.
Available columns in the **Logs listed by selected filter** table:	
Batch ID	The batch ID that uniquely identifies the batch that was in context from which this log originated. This may be blank.

Element	Description
Batch Name	The name of the batch that was in context from which this log originated. This may be blank. **Note:** The **Batch Name** column does not display the name of the batch, but instead displays the name of the process on which the batch is based.
DLL Name	The name of the *DLL* from which the log originated. This may be blank if it did not come from a *DLL*.
Log Category	The name of the category for the log.
Executable	The name of the executable from which the log originated.
Log Code	Log code.
Log Date	The date and time that the log was created.
Log Type	The log type.
Workstation Name	The name of the workstation from which the log originated.
Message	The log message. **Note:** In a log rule, if information messages (indicated by selecting **FilterAllDebugInfos** from the **Filter definition** list) are logged to **AuditToDBSink**, **ErrorToDBSink**, or **GeneralEventLogSink**, then the **Logs** pane will not display all the log messages.
Message Category	Three letter acronym for the message *DLL* that the log message uses.
Module Step	Name of the module step from which the log originated.
Node ID	The node ID that was in context from which this log originated. This may be blank.
Node Level	The node level that was in context from which this log originated. This may be blank.
Process ID	The process flow ID that uniquely identifies the batch that was in context from which this log originated. This may be blank.
Process Name	The name of the process that was in context from which this log originated. This may be blank.

Element	Description
OS Process ID	The process ID for the log as listed in the Task Manager in Windows.
Storage Date	The date and time that the log was stored in the database.
OS Thread ID	The *OS* assigned Thread ID from which the log originated.
Task Module	The name of the module running the task when this log originated.
Task Workstation	The workstation running the task when this log originated.
Task User	The user running the task when this log originated. This is encrypted if the server includes a feature code of "Q".
User Name	The name of the user from which the log originated.

Related Topics

"Deleting Logs Manually" on page 210

"Exporting Logs" on page 211

"Setting the Log Refresh Rate" on page 212

"Understanding Logs" on page 206

"Viewing a List of Logs" on page 208

"Viewing Log Details" on page 209

"Customizing Information Tables Using the Column Manager" on page 112

"Intelligent Capture Permissions List" on page 381

10.4.5.6 Log View Filters

Log view filters refine log lists to a user-defined subset of logs. These are used in the **Logs** pane by selecting the filter from the **Log** pane **Filter** list box.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-27: Log View Filters Pane

Element	Description
View Results	Displays the results of the log view filter in the **Logs** pane.
Add	Displays the **Add Log View Filter** pane where purges are created or modified.
Save As	Makes a copy of the selected log view filter and displays the **Add Log View Filter** window, where new log view filters are created.
Settings	Displays the **Log View Filter Settings** window for the selected log view filter.
Delete	Deletes the selected log view filter.
Available columns in the **Log View Filters** table:	
Name	The log view filter name.
Description	The log view filter description.
Creation Date	The date the log was created.

Related Topics

"Creating a Log View Filter" on page 213

"Log View Filter Settings and Add Log View Filter" on page 325

"Understanding Log View Filters" on page 212

"Managing Reports and Logs" on page 205

"Viewing Log View Filter Results" on page 214

"Customizing Information Tables Using the Column Manager" on page 112

"Intelligent Capture Permissions List" on page 381

10.4.5.7 Log Rules

Log rules provide a way to facilitate capture of system log information. The **Log Rules** pane displays a list of all logging rules including system and custom logging rules. Users can view the details of the selected logging rule, and enable, disable, edit or delete them from here. This also enables creation of a logging rule based on an existing rule or creation of a logging rule with totally new parameters. If the list of logging rules has more than one page, page numbers will display.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide.

Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Table 10-28: Log Rules Pane

Element	Description
Filter	Select the **Log Rule Filter** to limit the display to only the types selected: **All**, **System**, or **Custom**.
Add	Opens the **Add Log Rule** pane.
Save As	Makes a copy of the selected rule and opens the **Add Log Rule** pane.
Settings	Displays the **Log Rule Settings** pane for the selected log rule.
Delete	Deletes the selected rules.
Available columns in the **Registered Log Rules** table:	
Creation Date	Date and time when this logging rule was created.
Culture Code	The culture code for description string.
Data	Log rule data definition name.
Data Definition Description	Log rule data definition description.
Description	Description of this logging rule from Tbl_LocalText.
Enabled	Determines if this rule is enabled.
Exclude	Determines if the logging rule is blocked.
Filter	Log rule filter name.
Filter Definition Description	Log rule filter definition description.
Name	Name to represent this logging rule.
Read Only	Indicates the read only status of the rule.
Scope Component	The specific component to monitor. If blank, the logging rule considers all components.
Scope User	The specific user to monitor. If blank, the logging rule considers all users.
Scope Workstation	The specific workstation to monitor. If blank, the logging rule considers all workstations.
Sink	Log rule sink name.
Sink Definition Description	Log rule sink definition description.

Related Topics

"Creating or Copying a Log Rule" on page 219

"Defining Log Rule Filter Definitions" on page 221

"Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218

"Log Rule Data Definition Settings" on page 318

"Log Rule Filter Definition Settings and Add Log Rule Filter Definition" on page 319

"Log Rule Settings and Add Log Rule" on page 323

"Log Rule Sink Definition" on page 329

"Understanding Log Rules" on page 215

"Managing Reports and Logs" on page 205

"Viewing Log Rule Settings" on page 217

"Viewing Log Rules and Log Rule Settings" on page 216

"Customizing Information Tables Using the Column Manager" on page 112

"Intelligent Capture Permissions List" on page 381

10.4.6 Find a Batch

The **Find a Batch** pane enables users to search for batches quickly. Users can retrieve batches based on search parameters specified in the batch filters. Select **Batch Finder** from the navigation panel to access this pane.

Table 10-29: Find a Batch Pane

Element	Description
Find a Batch pane	Displays the main search pane.
Find	Click to perform a simple search for batches.
Last Results	Displays the results of batch searches and batch filters in the right pane. For more information, see Batch Finder Results.
Filters	Displays the filters and options to create new filters, copy filters, and edit filters. For more information, see Batch Filters.
Advanced Search	Enables users to find batches based on detailed search criteria. For more information, see Batch Finder (New Search).

Related Topics

"Specifying Batch Search Filters" on page 190

"Viewing and Modifying Batch Search Filters" on page 192

"Displaying Batch Search Results" on page 193

10.4.6.1 Batch Finder Results

Access the **Last Results** option from the **Batch Finder** panel to view the **Batch Finder Results** pane.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Table 10-30: Batch Finder Results Pane

Element	Description
Modify Search	Enables users to change the search criteria by displaying the **Batch Finder** pane. To understand the search elements, see "Batch Finder" on page 307.
Settings	Displays the **Batch Settings** window.
Delete	Deletes the selected batch filter.
Batch Finder Results: Displays batch search results in the following tables. To understand how the tables interact in the window, see "Understanding the Components of the Batch Traffic Pane" on page 164.	
Batches table (top table)	Displays the list of batches. The Batches table is filtered based on the user selection.
Chart	Displays the installed processes or module steps in a process depending on the user's selection.
Modules table (bottom table)	Displays the modules connected for all installed processes or specific processes depending on the user selection.

Related Topics

"Specifying Batch Search Filters" on page 190

"Viewing and Modifying Batch Search Filters" on page 192

"Displaying Batch Search Results" on page 193

10.4.6.2 Batch Filters

The **Batch Filters** pane displays the list of saved batches search filters. For more information, see "Viewing and Modifying Batch Search Filters" on page 192.

Table 10-31: Batch Filters Pane

Element	Description
Name	Specifies the name of the filter.
Filtering	Displays a summary of the search filters.
Description	Specifies the description of the search filter.
View Results	Select a filter and click **View Results** to display the **Batch Finder Results** pane that lists the batches that meet the search criteria specified in the filter.
Add	Adds a new batch filter.
Save As	Saves a new batch search filter.
Settings	Displays the **Batch Finder** pane with the settings of the selected batch search filter.
Delete	Deletes the selected batch filters.

Related Topics

"Specifying Batch Search Filters" on page 190

"Viewing and Modifying Batch Search Filters" on page 192

"Displaying Batch Search Results" on page 193

10.4.6.3 Batch Finder

The **Batch Finder** pane enables users to specify advanced search criteria for batch search filters. For more information, see "Searching for Batches" on page 189.

Table 10-32: Batch Finder Pane

Element	Description
Filter Name for this Search	Specifies the **Filter name** and **Description** of the filter.

Element	Description
Batch Properties to Match	Selected check boxes and options determine the search criteria. • **Name**: Specify the name of the batch to search for. • **Description**: Type the description of the batch. • **Server**: Select the Intelligent Capture Server to search. The batches are searched for in the selected Intelligent Capture Server. The default is the current Intelligent Capture Server name. • **Process**: Select the process associated with the batch. • **Status**: Specify the batch status. • **Priority less than or equal to**: Specify a batch priority. The filter searches for batches with a priority less than the number selected in this list box. • Select the appropriate **Batch was created** option: – **Anytime**: The search will not filter based on batch creation date and time. The default. – **At least this many days ago**: Search displays batches whose creation date and time occurred before the specified number of days in the past. – **Before this date**: The search filters the available batches based on batch creation date and time. – **Batch contains value**: The search filters the available batches based on the contents of a searchable IA Value. Searchable IA Values are IA Values of a process that have been indexed. Select one of these options to specify a searchable IA Value to use in the search: ○ **In any indexed value**: Searches all searchable IA Values for the selected text. ○ **In value**: Select the IA Value from the list box to use in the search. The list box displays all the searchable IA Values in the system.

Element	Description
Run Search	Searches for batches that match the search filter criteria. For more information, see Displaying batch search results.
OK	Saves the current search as a filter.

Related Topics

"Specifying Batch Search Filters" on page 190

"Viewing and Modifying Batch Search Filters" on page 192

"Displaying Batch Search Results" on page 193

10.4.7 Options

Set preferences for the Intelligent Capture Administrator from the **Options** pane.

Table 10-33: Options Pane

Element	Description
Default Settings	Specifies the default Intelligent Capture Administrator preferences. For example: the refresh rate for the panes, the window displayed when the user logs in to the Intelligent Capture Administrator, and how to set up modules without consuming a license.
My Preferences	The Intelligent Capture Administrator settings displayed at the user's login. Settings specified in **My Preferences** override the **Default Settings**.

Related Topics

"Specifying Intelligent Capture Administrator Default Settings" on page 110

"Setting Preferences for Your Work Environment" on page 111

10.4.7.1 Default Settings

Default Settings apply to all users accessing Intelligent Capture Administrator.

See Specifying Intelligent Capture Administrator settings

Table 10-34: Default Settings Pane

Element	Description
Display Options: Sets the display options for Intelligent Capture Administrator.	
Start Page	Sets the default pane. The pane is displayed when the user logs on to Intelligent Capture Administrator. The default startup pane is the **Batch Traffic** pane.
Maximum number of rows in table lists	Sets the number of lines displayed in each table. The default is 100.
Maximum number of batches	Sets the number of batches to display and work with in Intelligent Capture Administrator. The default is 5000.
Maximum number of logs	Sets the number of logs to display. The default is 5000.
Page Refresh Rates: Sets the page refresh rate. **Note: Page Refresh Rates** automatically refresh the specified panes. If auto refresh occurs while performing administrative tasks on one of the panes, any work being performed can be disrupted. When performing administrative tasks on one of these panes, use the **Auto Refresh** link on the particular pane to turn off auto refresh. When finished, click the link again to switch auto refresh back on.	
Screen Name	The screen on which the refresh rate will be applied.
Default Refresh Rate	Specifies the frequency to update the selected window.
Recommended Refresh Rate	A static value indicating the recommended rate. This value optimizes refresh versus performance.
Module Setup Options: Specifies options when running a module in setup mode.	
Restricted	Specifies the module setup option as **Restricted** which does not consume a license.
Unrestricted	Specifies the module setup option as **Unrestricted** which uses a license in setup mode.
Apply Recommended Settings	Resets each setting to the default settings.
OK	Saves the settings.
Cancel	Discards the changes.

Related Topics

"Logging In to Intelligent Capture Administrator" on page 109

"Setting Preferences for Your Work Environment" on page 111

"Intelligent Capture Permissions List" on page 381

10.4.7.2 My Preferences

User's can specify their Intelligent Capture Administrator preferences in the **My Preferences** pane. For more information, see Setting preferences for your work environment.

Table 10-35: My Preferences Pane

Element	Description
Display Options: Specifies the user's display preferences.	
Start Page	Sets the default Intelligent Capture Administrator pane to display when the user logs on to Intelligent Capture Administrator. The default startup pane is the **Batch Traffic** pane.
Maximum number of rows in table lists	Sets the number of lines displayed in each table. The default is 100.
Maximum number of batches	Sets the number of batches to display and work with in Intelligent Capture Administrator. The default is 5000.
Maximum number of logs	Sets the number of logs to display. The default is 5000.
Page Refresh Rates: Sets the page refresh rates for the specified panes.	
Screen Name	The screen on which the refresh rate will be applied.
Current Refresh Rate	Specifies the frequency to update the selected window.
Recommended Refresh Rate	A static value indicating the recommended rate. This value optimizes refresh versus performance.
Note: Page Refresh Rates automatically refresh the pane. If auto refresh occurs while performing administrative tasks on one of the panes, any work being performed can be disrupted. When performing administrative tasks on one of these panes, use the **Auto Refresh** link on the particular pane to turn off auto refresh. When finished, click the link again to switch auto refresh back on.	
Module Setup Options: Specifies options when running a module in setup mode.	

Element	Description
Restricted	Specifies the module setup option as **Restricted** which does not consume a license.
Unrestricted	Specifies the module setup option as **Unrestricted** which uses a license in setup mode.
Apply Recommended Settings	Resets each setting to the recommended (factory) values.
Apply Default Settings	Resets each setting to the current **Default Settings** values.
OK	Saves the settings.
Cancel	Discards the changes.

Related Topics

"Logging In to Intelligent Capture Administrator" on page 109

"Specifying Intelligent Capture Administrator Default Settings" on page 110

"Intelligent Capture Permissions List" on page 381

10.4.8 Web Services

The **Web Services** pane enables users to manage the Web Services subsystem, including viewing, adding, and deleting web services and web hostings, as well as defining global options.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-36: Web Services Pane

Element	Description
View Services	View, define, and delete individual web services. A web service is defined by selecting a Web Services Description Language (*WSDL*) file, parsing, naming, and describing it, and then specifying how to map a *`Correlation ID`* to facilitate asynchronous operation.
View Hostings	View, define, and delete web service hostings. Each hosting is an instance of a web server that makes the selected web services available to workstations connecting using the corporate intranet or the public Internet.

Element	Description
View Web Services Settings	View and configure global options for the Web Services subsystem.

Related Topics

"Intelligent Capture Permissions List" on page 381

"Web Services" on page 104

"Managing Web Services and Hosting" on page 251

10.4.8.1 Services

The **Services** pane displays a list of web services that have been registered in the Intelligent Capture Web Services subsystem, their hosting status and service attributes, and the service attributes for hostings that expose each service. It also provides the ability to add, delete, and change the settings of web services.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-37: Services Pane

Element	Description
Add	Displays the **New Service Setup Wizard** window.
Delete	Displays the **Remove Service** window. This window lists the processes and batches that are dependent on the web service you are about to delete. Review the list before proceeding. If you feel it is safe to delete the web service, click **OK**. Otherwise, click **Cancel** to return to the **Services** screen without deleting the web service.

Element	Description
Settings	Displays the **Service Properties** window. In this window, select either **General Options** or **Mapping Options** from the **View** list: • **General Options** enable you to view the web service name and to view or edit the web service description. • **Mapping Options** enable you to view or edit the mapping of web service methods to Correlation IDs. With the exception of the wizard's **Back** and **Next** buttons, this window is identical to the **New Service Setup Wizard: Correlation Mapping** window. Unavailable unless a Web Service is selected in the **Services** table.
Refresh List	Updates the information displayed in the **Hostings** table. Click this button when you suspect that another administrator may have added, removed, or changed one or more web services.
Service Name	Displays the registered name of the web service (which may or may not be the original name of the web service).
Description	Displays the description, if any, specified by the user who registered the web service.
Hostings: Click the **+** button to expand the sublist for each listed web service to display the following read-only information:	
Computer	Displays the machine name or *IP* address of the computer that is providing this hosting. The **Computer** field can only contain characters that are valid in a Microsoft Windows computer name or an *IP* address.
Status	Displays the hosting status: ⇧ (up) or ⇩ (down).
Virtual Directory	Displays the virtual directory where the web service is hosted.
Port	Displays the port that is listening for requests for this web service.
SSL	Indicates whether the web service is using Secure Sockets Layer (*HTTPS*) for communication with clients.
Description	Displays the description, if any, specified by the user who registered the hosting.

Related Topics

"Intelligent Capture Permissions List" on page 381

"Configuring Hostings" on page 256

"Hostings" on page 315

"Web Services Settings" on page 316

10.4.8.2 Hostings

The **Hostings** pane displays a list of web service hostings that have been registered in the Intelligent Capture Web Services subsystem, their hosting status and service attributes, and the service attributes for the web services that each hosting exposes. It also provides the ability to add, delete, and change the settings of web service hostings.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-38: Hostings Pane

Element	Description
Add	Displays the **New Hosting Setup Wizard** window.
Delete	Deletes selected web service hosting from the system.
Settings	Displays the **Hosting Properties** window in which you can view the details of the selected hosting, as well as register and unregister web services on the hosting. With the exception of the wizard's **Back** and **Next** buttons, this window is identical to the **New Hosting Setup Wizard: Set Services** window. Unavailable unless a hosting is selected in the Hostings table.
Name	Displays the name of the hosting as specified when the hosting was defined.
Status	Displays the hosting status: ⬆ (up) or ⬇ (down).
Description	Displays the description, if any, specified by the user who defined the hosting.
Web Services: Click the **+** button to expand the sublist for each listed hosting to display the following read-only information:	

Element	Description
Service	Displays the registered name of the web service (which may or may not be the original name of the web service).
Virtual Directory	Displays the virtual directory where the web service is hosted.
Port	Displays the port that is listening for requests for this web service.
SSL	Indicates whether the web service is using Secure Sockets Layer (*HTTPS*) for communication with clients.
Description	Displays the description, if any, specified by the user who registered the web service.

Related Topics

"Intelligent Capture Permissions List" on page 381

"Configuring Hostings" on page 256

"Services" on page 313

"Web Services Settings" on page 316

10.4.8.3 Web Services Settings

The **Web Services Settings** pane displays the global options for the Intelligent Capture Web Services subsystem.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-39: Web Services Settings Pane

Element	Description
WS Hosting connection: attempt interval (sec)	Specifies the interval, in seconds, at which the Web Services Coordinator attempts to connect to the Web Service Hosting service.
Incoming web request timeout (sec)	Specifies the time, in seconds, after which the Web Services Coordinator deletes web service requests that have not been processed. The default value is 86,400 seconds (24 hours).
TCP port for connections to Web Services Coordinator	Specifies the *TCP* port number that the Web Services Input module and the Intelligent Capture Administrator use to connect to the Web Services Coordinator.

Caution

Do not attempt to connect one instance of the Web Services Hosting service to multiple Web Services Coordinator instances. Doing so is not a supported configuration and will result in a sharing conflict, as each Web Service Coordinator attempts to reconfigure the common hosting instance with is own rules.

Related Topics

"Intelligent Capture Permissions List" on page 381

"Defining Web Services Settings" on page 260

"Services" on page 313

"Hostings" on page 315

10.5 Intelligent Capture Administrator Logon

The Intelligent Capture Administrator **Logon** window is used to login to the Intelligent Capture Administrator.

Table 10-40: Intelligent Capture Administrator Logon Window

Element	Description
Username and **Password**	The credentials of the user logging into the Intelligent Capture Administrator.
Domain	The **Domain** of the user.
Logon	Logon to Intelligent Capture Administrator.

Related Topics

"Logging In to Intelligent Capture Administrator" on page 109

"Specifying Intelligent Capture Administrator Default Settings" on page 110

"Intelligent Capture Permissions List" on page 381

10.6 Log Rule Data Definition Settings

Log rule data definitions specify additional data to pass with the log. Generally this is used in audit and statistic log rules to define specific data related to the context of the modules associated with the event being logged.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-41: Log Rule Data Definition Settings Window

Element	Description
Name	The name for the data definition. This name will appear in the **Log Rule Settings** or **Add Log Rule** windows.
Description	An optional description of the data definition. This description will appear in the **Log Rule Settings** or **Create a Custom Log Rule** windows.
Available columns in the Log Rule Data Definition Settings table:	
Name	The name of the data definition parameter. Edited by double-clicking.
Custom Data Value	The data value to apply to the data definition parameter, such as IA Values. Edited by double-clicking.
Add	For adding a data definition parameter.
Delete	For deleting the selected data definition parameter.

Note: Predefined system **Data definitions** cannot be changed or deleted. User created **Data definitions** can be deleted, but only when they are not in use by any log rule. To delete user created definitions:

- Open the log rules using the definition to be deleted.
- Select a different definition than the one to be deleted.
- Save the log rule.
- Edit any other log rule, select the definition to be deleted, and click delete.
- Reset the correct definition for the open log rule and click **OK**.

Related Topics

"Creating or Copying a Log Rule" on page 219

"Defining Log Rule Filter Definitions" on page 221

"Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218

"Log Rule Filter Definition Settings and Add Log Rule Filter Definition" on page 319

"Log Rule Settings and Add Log Rule" on page 323

"Log Rules" on page 303

"Log Rule Sink Definition" on page 329

"Understanding Log Rules" on page 215

"Viewing Log Rule Settings" on page 217

"Viewing Log Rules and Log Rule Settings" on page 216

"Intelligent Capture Permissions List" on page 381

10.7 Log Rule Filter Definition Settings and Add Log Rule Filter Definition

Filter definitions determine when a log is created, and under what conditions the log will be created.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-42: Log Rule Filter Definition Settings and Add Log Rule Filter Definition Windows

Element	Description
Name	Type a unique name for the filter definition.
Description	Include an optional description
Setting	Select the type of setting to be configured, **Log Type and Codes**, **Processes and Modules**, or **Workstations and Users**. The bottom of the pane changes to reflect the selection.

Element	Description
Log Type and Codes	**Log Type and Codes** is the mechanism by which the user can edit filter name, description, log type, stack dump, log codes and logging categories when users are creating a logging rule filter or modifying an existing one. The available options are: • **Log type**: **Error**, **Warning**, **Audit**, **Statistic** and **Debug** • **Log codes**: The contents of the log code differs depending on the selected log type. A complete list of client module error and log codes is listed in *OpenText Intelligent Capture - Module Reference (ECPCORE-CMD)*. • **Available Categories / Selected Categories**: The combined list of the categories is from all logging categories in the database. The selected categories are part of the log rule filter definition.

Element	Description
Processes and Modules	**Processes and Modules** enables the user to edit filter name, description, process, steps, module attributes, and modules. This includes the following options: • **Available Processes / Selected Processes**: The available and selected processes installed on the Intelligent Capture Server. For processes, if the **Scope component** specified in the log rule is an Intelligent Capture module or the Intelligent Capture Server, a process can be added to the filter. This will limit the log to only events that happen when tasks for that process are being processed by the module or server. Specifying a process setting when the **Scope component** is not a module or the server, will result in the rule not matching any logs sent by the **Scope component**. Multiple processes can be specified. • **Available Steps / Selected Steps**: The list of step names are from the selected processes. The filter will apply only if there are selected steps. If no steps are selected, logs will not be filtered by steps. If any steps are selected, only log events that came from any one of the selected steps will be stored. • **Available Module Attributes / Selected Module Attributes**: This is a fixed list including the values: **Attended**, **Unattended**, **Ocr**, **Index**, **CreatePage**, **Scan**. The attributes setting will limit the log to only events sent by the server when tasks from the module are logged. • **Available Modules / Selected Modules**: For modules, if the **Scope component** for the rule is the Intelligent Capture Server, the module setting will limit the log to only events sent by the server when tasks from the module are logged. If Module is specified for Scope Components other than the Server, this setting will be ignored. Multiple modules can be specified.

Element	Description
Workstations and Users	**Workstations and Users** enables the user to specify the logging subsystem to only log events from specified workstations, users, or both. • **Workstation(s)**: For workstations, if the **Scope component** for the rule is the Intelligent Capture Server, the **Workstations** setting will limit the log to only events sent by the server when tasks from the modules running on the workstation are logged. If **Workstation** is specified for **Scope component** other than the Intelligent Capture Server, this setting will be ignored. Multiple workstations can be specified, separated by a semicolon (;). • **User(s)**: User names must be specified in the form domain\user. For users, if the **Scope Component** for the rule is the Intelligent Capture Server, the **Users** setting will limit the log to only events sent by the server when tasks from the modules executed by the user are logged. If **User** is specified for **Scope Component** other than the Intelligent Capture Server, this setting will be ignored. Multiple users can be specified, separated by a semicolon (;).

Note: Predefined system **Filter definitions** cannot be changed or deleted. User created **Filter definitions** can be deleted, but only when they are not in use by any log rule. To delete user created definitions:

- Open the log rules using the definition to be deleted.
- Select a different definition than the one to be deleted.
- Save the log rule.
- Edit any other log rule, select the definition to be deleted, and click delete.
- Reset the correct definition for the open log rule and click **OK**.

Related Topics

"Creating or Copying a Log Rule" on page 219

"Defining Log Rule Filter Definitions" on page 221

"Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218

"Log Rule Data Definition Settings" on page 318

"Log Rule Settings and Add Log Rule" on page 323

"Log Rules" on page 303

"Log Rule Sink Definition" on page 329

"Understanding Log Rules" on page 215

"Viewing Log Rule Settings" on page 217

"Viewing Log Rules and Log Rule Settings" on page 216

"Intelligent Capture Permissions List" on page 381

10.8 Log Rule Settings and Add Log Rule

Log rules define what kind of logs will be logged, when it will be logged, where it will go and how it will be formatted. This pane enables creation of new log rules or view settings of existing system log rules, or view/edit an existing user defined log rule.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-43: Log Rule Settings and Add Log Rule Windows

Element	Description
Name	A unique name for the log rule.
Description	An optional description of the log rule.
Status	Select **Enabled** to activate this log rule or clear the check box to disable. Selecting **Block logs that meet this criteria** disregards logs that meet these criteria.
Scope component	Pre-populated with all module names in the `Tbl_Module` table in the Intelligent Capture Database and the scope components from existing log rules (components that users have previously typed in). This can be blank, in which case the rule applies to all modules and services.
Scope user	Pre-populated with all entries from the `Tbl_Identity` table in the Intelligent Capture Database and all scope users from existing log rules (ones that users have previously typed in). This can be blank, in which case the rule applies to all users.

Element	Description
Scope workstation	Pre-populated with all workstation names in the `Tbl_AuditErrorLog` table in the Intelligent Capture Database and the scope workstations from the existing log rules (ones that users have previously typed in). This can be blank, in which case the rule applies to all workstations.
Filter definition	Defines when to create a log based on parameters such as processes, modules, workstations and users.
Data definition	Defines what additional data to include with the log.
Sink definition	Defines the configuration of a log sink. This includes where the log is written and how it is written including any connection information and the format of the log output. **Note:** In a log rule, if information messages (indicated by selecting **FilterAllDebugInfos** from the **Filter definition** list) are logged to **AuditToDBSink**, **ErrorToDBSink**, or **GeneralEventLogSink**, then the **Logs** pane will not display all the log messages.

Note: Predefined system **Filter definitions**, **Data definitions**, or **Sink definitions** cannot be changed or deleted. User created **Filter definitions**, **Data definitions**, or **Sink definitions** can be deleted, but only when they are not in use by any log rule. To delete user created definitions:

- Open the log rules using the definition to be deleted.
- Select a different definition than the one to be deleted.
- Save the log rule.
- Edit any other log rule, select the definition to be deleted, and click delete.
- Reset the correct definition for the open log rule and click **OK**.

Related Topics

"Creating or Copying a Log Rule" on page 219

"Defining Log Rule Filter Definitions" on page 221

"Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218

"Log Rule Data Definition Settings" on page 318

"Log Rule Filter Definition Settings and Add Log Rule Filter Definition" on page 319

"Log Rules" on page 303

"Log Rule Sink Definition" on page 329

"Understanding Log Rules" on page 215

"Viewing Log Rule Settings" on page 217

"Viewing Log Rules and Log Rule Settings" on page 216

"Intelligent Capture Permissions List" on page 381

10.9 Log View Filter Settings and Add Log View Filter

Log view filters limit the type of logs displayed based on their characteristics. The **Add Log View Filter** and **Log Filter Settings** windows title changes depending on whether a new log filter is being created or an existing log filter is being modified. In either of these windows, set the filter name, description, and any or all of the filter types when creating a log filter or modifying an existing one. The available filter types are: **Date/Time**, **Log Type and Codes**, **Processes and Batches**, and **Workstations and Modules**. When selecting one of the filter types, the **Settings** area of the window changes, enabling definition of the selected type

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-44: Log View Filter Settings and Add Log View Filter Windows

Element	Description
Name	Give the log view filter a name.
Description	Give the log view filter an optional description.
Filtering	You can specify any combination of: • **Date/Time** specifies the display of logs from a particular time period. • **Log Type and Codes** specifies the display of logs based on type, codes, and category of log. • **Processes and Batches** specifies the display of logs based on processes, steps, and batches. • **Workstations and Modules** specifies the display of logs based on workstations and modules.
Date/Time	Specifies the display of logs from a particular time period.

Element	Description
Log Type and Codes	**Log Type and Codes** is the mechanism by which the user can edit log view filter name, description, log type, log codes and logging categories when users are creating a logging rule filter or modifying an existing one. the available options are: • **Log Type and Log Codes**: **Error**, **Warning**, and **Audit** • **Available Log Codes / Selected Log Codes**: The contents of the log code differs depending on the selected log type. The log view filter will apply only if there are selected log codes. If no log codes are selected, logs will not be filtered by log codes. • **Available Categories / Selected Categories**: The combined list of the categories is from all logging categories in the log database. The log view filter will apply only if there are selected categories. If no log categories are selected, logs will not be filtered by category.

Element	Description
Processes and Batches	**Processes and Batches** enables the user to edit filter name, description, process, steps, module attributes, and modules. This includes the following options: • **Available Processes / Selected Processes**: The available and selected processes installed on the Intelligent Capture Server. The log view filter will apply only if there are selected processes. If no processes are selected, logs will not be filtered by processes. If any processes are selected, only log events generated by one of the selected processes are stored. • **Available Steps / Selected Steps**: The list of step names are from the selected processes. The log view filter will apply only if there are selected steps. If no steps are selected, logs will not be filtered by steps. If any steps are selected, only log events that came from any one of the selected steps will be stored. • **List one or more batch names, separated by a semi-colon**: Specify one or more batch names, with the batch name separated by a semicolon.  **Caution** Batches with ";" and "|" in the batch name cannot be filtered. The log view filter will apply only if there are batches with the specified names. Logs from any of the specified batches will be returned. • **Process ID**: The process ID. If blank, the log view filter is not applied on this field. • **Batch ID**: The batch ID. If blank, the log view filter is not applied on this field. • **Node level**: The node level from 0 to 7. If blank, the log view filter is not applied on this field. • **Node ID**: The node ID. If blank, the log view filter is not applied on this field.

Element	Description
Workstations and Modules	**Workstations and Modules** enables the user to specify the logging subsystem to only log events from specified workstations, users, or both. • **Available Workstations / Selected Workstations**: The log view filter will apply only if there are selected workstations. If no workstations are selected, logs will not be filtered by workstations. If any workstations are selected, only logs that came from any one of the selected workstations will be returned. • **Available Users / Selected Users**: The log view filter will apply only if there are selected users. If no users are selected, logs will not be filtered by users. If any users are selected, only logs that came from any one of the selected users will be returned. • **OS process ID**: The *OS* process ID. If blank, the log view filter will not be applied on this field. • **OS thread ID**: The *OS* thread ID. If blank, the log view filter will not be applied on this field. • **EXE name**: The executable name. If blank, the log view filter will not be applied on this field. • **DLL name**: The *DLL* name. If blank, the log view filter will not be applied on this field.

Related Topics

"Creating a Log View Filter" on page 213

"Log View Filters" on page 302

"Understanding Log View Filters" on page 212

"Viewing Log View Filter Results" on page 214

"Intelligent Capture Permissions List" on page 381

10.10 Log Rule Sink Definition

Defines the configuration of a log sink. It determines where the log is written and how it is written, including any connection information and the output format. The exact format and content of the sink properties will depend on the type of sink being configured.

Sink definitions specify the destination where the log is written. Intelligent Capture Administrator supports the following sinks:

- Event sink: Writes application logs to the Windows Event Log.
- File sink: Writes the log to a file on the machine running the **Scope Component**. Entries logged to the File Sink that are longer than 511 bytes may be truncated. Truncated entries end with "…".
- Database sink: Writes the log to a table in the database.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-45: Log Rule Sink Definition Window

Element	Description
Name	The name for the sink definition.
Description	An optional description of the sink definition.
Destination	Specify both the **Sink type** and the **Destination** (the location of the specified sink).
Destination Setting File	This field is required for a new sink definition if defining a database, text file, or event log sink. If a new file is selected, it will be validated to determine both if it is a valid *XML* file and if it contains valid destination settings schema parameters. The schema for the destination settings file is provided in "FileSinkFormat XML" on page 425.
Format Configuration File	This field is required for a new sink definition if defining a database or text file log sink. This field is ignored for Event Log. If a new file is selected, it will be validated to determine both if it is both a valid *XML* file and if it contains valid format configuration schema parameters. The schema for the format configuration file is provided in "FileSinkFormat XML" on page 425.

Note: Predefined system **Sink definitions** cannot be changed or deleted. User created **Sink definitions** can be deleted, but only when they are not in use by any log rule. To delete user created definitions:

- Open the log rules using the definition to be deleted.
- Select a different definition than the one to be deleted.
- Save the log rule.
- Edit any other log rule, select the definition to be deleted, and click delete.
- Reset the correct definition for the open log rule and click **OK**.

Related Topics

"Creating or Copying a Log Rule" on page 219

"Defining Log Rule Filter Definitions" on page 221

"Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218

"Log Rule Data Definition Settings" on page 318

"Log Rule Filter Definition Settings and Add Log Rule Filter Definition" on page 319

"Log Rule Settings and Add Log Rule" on page 323

"Log Rules" on page 303

"Understanding Log Rules" on page 215

"Viewing Log Rule Settings" on page 217

"Viewing Log Rules and Log Rule Settings" on page 216

"Intelligent Capture Permissions List" on page 381

10.11 New Hosting Setup Wizard: Define Workstation

The **New Hosting Setup Wizard** defines a new web service hosting on a specified computer. The **Define Workstation** pane is the first of three panes that comprise the wizard.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-46: New Hosting Setup Wizard: Define Workstation Window

Element	Description
Hosting name	The workstation name or *IP* address of the workstation that will be an Intelligent Capture Web Services host. Type a valid computer name or *IP* address in this field. The **Hosting Name** must be under 1000 characters and may only contain characters that are valid in a Microsoft Windows computer name or an *IP* address.
Description	Specifies a description for the hosting. Type a description in this field.
Next	Displays the **New Hosting Setup Wizard: Set services** window.

Related Topics

"Intelligent Capture Permissions List" on page 381

"New Hosting Setup Wizard: Set Services" on page 331

"New Hosting Setup Wizard: Register Hosting" on page 332

"Hostings" on page 315

10.12 New Hosting Setup Wizard: Set Services

The **New Hosting Setup Wizard** defines a new web service hosting on a specified computer. The **Set services** pane is the second of three panes that comprise the wizard.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-47: New Hosting Setup Wizard: Set Services Window

Element	Description
Hosting name	The machine name or address of the computer that will be an Intelligent Capture Web Service host. This is a read-only field. To change the computer name, click **Back** to return to the **Define workstation** pane.
Available services to register on this hosting	

Element	Description
Service Name	The service name of each of the web services that have been defined in the Web Services subsystem. Click to select a service to register in this hosting.
Description	A description of this hosting.
Register	Registers the selected web service in this hosting. If successful, removes the selected web service from the table and adds the assigned *URL* to the **Registered services** table.
Unregister	Removes the selected registered service from the **Registered services** table. When unregistered, the web service is not available from this hosting.
Registered services	
URL	Displays the *URL* assigned to each web service that has been registered on this hosting.
Back	Returns to the **New Hosting Setup Wizard: Define workstation** window.
Next	Displays the **New Hosting Setup Wizard: Register hosting** window.

Related Topics

"Intelligent Capture Permissions List" on page 381

"New Hosting Setup Wizard: Define Workstation" on page 330

"New Hosting Setup Wizard: Register Hosting" on page 332

"Hostings" on page 315

10.13 New Hosting Setup Wizard: Register Hosting

The **New Hosting Setup Wizard** defines a new web service hosting. The **Register hosting** pane is the last of three panes that comprise the wizard. This pane enables you to review the hosting definition prior to registering the hosting.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-48: New Hosting Setup Wizard: Register Hosting Window

Element	Description
Hosting information list	Displays the workstation name of the computer on which the hosting is being registered followed by each web service that will be published on the new hosting.
Back	Returns to the **New Hosting Setup Wizard: Set services** window.
OK	Registers the hosting and publishes the specified web services, closes the wizard, and returns to the **Hostings** window.

Related Topics

"Intelligent Capture Permissions List" on page 381

"New Hosting Setup Wizard: Define Workstation" on page 330

"New Hosting Setup Wizard: Set Services" on page 331

"Hostings" on page 315

10.14 Install Process

The **Install Process** window installs processes onto the Intelligent Capture Server. After a process is installed, each module step associated with the process can be configured in setup mode.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-49: Install Process Window

Element	Description
Name	Name of the process. The name must be unique within the list of existing processes. The process name can be a maximum of 128 characters.
Process IAP file, including path	The full path name of the process file.
Set the priority for new batches to the server default	Select to specify that batches created with this process should inherit priority from the server's default priority.

Element	Description
Priority for batches based on this process	If the **Set the priority for new batches to the server default** check box is cleared, type the processing priority for the batches in this field. The priority can be any value from 1-99. The default priority is 50.
Install to servers	Determines the Intelligent Capture Servers where the process is installed. The **Servers Available** list box lists all the servers in the system. The **Servers Selected** list box lists the servers where the process is installed.
Description	Description of the process.
OK	Installs the process onto the selected server.

Related Topics

"Intelligent Capture Administrator Component Interactions and User interface Language" on page 92

"Monitoring Intelligent Capture" on page 96

"Configuring a Process Step in Setup Mode" on page 157

"Viewing and Defining Access Control for a Process" on page 160

"Copying Step, Process, and Batch Settings" on page 197

"Intelligent Capture Permissions List" on page 381

10.15 New Service Setup Wizard: Define Service

The **New Service Setup Wizard** defines a new web service. The **Define service** pane is the first of three panes that comprise the wizard.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-50: New Service Setup Wizard: Define Service Window

Element	Description
Select WSDL	Specifies the name of the Web Service Description Language (*WSDL*) file to use in the web service definition. Type a path and file name in this field, or click **Browse** to display a standard **Choose File** window, then navigate to and open the *WSDL* file.

Element	Description
Parse	Click to parse the selected *WSDL* file. If successful, the **Select WSDL** field is cleared and the parsed Service Name is displayed in the **Service** field. If parsing is unsuccessful, the wizard displays an error message near the top of the pane.
Service	Displays the Service Name(s) parsed from the selected *WSDL* file. If multiple Service Names were parsed, select the Service Name from this list box.
Keep original	Uses the Service Name displayed in the **Service** list box.
Set different name	Uses a different name in place of the parsed Service Name. Type the new name into the adjacent field. The specified Service Name may contain only characters that are valid within an *HTTP* header string.
Description	Specifies a description for the web service. Type the description text into this field.
Next	Displays the **New Service Setup Wizard: Correlation Mapping** window.

Related Topics

"Intelligent Capture Permissions List" on page 381

"New Service Setup Wizard: Correlation Mapping" on page 335

"New Service Setup Wizard: Register Service" on page 337

"Services" on page 313

10.16 New Service Setup Wizard: Correlation Mapping

The **New Service Setup Wizard** defines a new web service. The **Correlation mapping** pane is the second of three panes that comprise the wizard. This pane enables you to define a *`Correlation ID`* to use in work flows that require multiple, independent web service requests. The *`Correlation ID`* links together the responses that are stored in the Intelligent Capture Database as each independent request is processed, and prevents a task from being processed until all required inputs are available. The *`Correlation ID`* can be mapped either to the *SOAP* header or to a selected parameter of a selected method. Each method in a web service can have a separate *`Correlation ID`* mapping.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-51: New Service Setup Wizard: Correlation Mapping Window

Element	Description
Methods table	
Name	Displays the names of the web service methods that were parsed from the *WSDL* file specified in the **Define service** pane, one method name per row. Select a method name and then specify the *`Correlation ID`* mapping.
Mapped	Indicates whether the method is mapped to a *`Correlation ID`*. If a mapping has been defined, the **Mapped** column displays a red check mark ( ).
Mapping controls	
No Correlation ID	Specifies no *`Correlation ID`* mapping for the selected web service method. This is an appropriate setting for methods that do not require asynchronous processing.
Correlation ID is Located in SOAP Header	Specifies that the selected method is mapped to a *SOAP* header *`Correlation ID`*. Type the name of the *SOAP* header in the adjacent field. *SOAP* header parameter identifiers may contain only letters (A-Z, a-z), numerals (0-9) and '_' symbol, and must not begin with a numeral.
Correlation ID is Located in Method Parameter	Specifies that the selected method is mapped to a method parameter Correlation ID. The adjacent list displays all parameters of the selected method, and pre-selects the parameter, if any, that contains a *`Correlation ID`*. Select one or more methods to map.
Back	Returns to the **New Service Setup Wizard: Define service** window.
Next	Displays the **New Service Setup Wizard: Register Service** window.

Note: If the Web Services Input module will be using this service to create batches (as the first module step in a process), do not map a *`Correlation ID`*. (Only methods that do not have a *`Correlation ID`* mapped to them will be present in the Web Services Input module's **Mapped method** list. If all methods are mapped, then the service will not be present in the Web Services Input module's **Service for mapping** list. Both lists display in theWS Input module setup window.)

Conversely, if the Web Services Input module will be using this service to add data to an existing batch (in a position other than the first module step in a process), you must map at least one method to a *Correlation ID*. (Only methods that have a *Correlation ID* mapped to them will be present in the Web Services Input module's **Mapped method** list. If no methods are mapped, then the service will not be present in the **Service for mapping** list. Both lists display in the WS Input module setup window.)

Related Topics

"Intelligent Capture Permissions List" on page 381

"New Service Setup Wizard: Define Service" on page 334

"New Service Setup Wizard: Register Service" on page 337

"Services" on page 313

10.17 New Service Setup Wizard: Register Service

The **New Service Setup Wizard** defines a new web service. The **Register Service** pane is the last of three panes that comprise the wizard. This pane enables you to review the web service definition and *Correlation ID* mapping prior to registering the service.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-52: New Service Setup Wizard: Register Service Window

Element	Description
Review Service Registration Settings	Displays the specified Service Name and *Correlation ID* mapping that were specified in the **Define service** and **Correlation mapping** panes.
Back	Returns to the **New Service Setup Wizard: Correlation mapping** window.
OK	Registers the web service with the specified settings, closes the wizard, and returns to the **Services** window.

Related Topics

"Intelligent Capture Permissions List" on page 381

"New Service Setup Wizard: Define Service" on page 334

"New Service Setup Wizard: Correlation Mapping" on page 335

"Services" on page 313

10.18 Print

The **Print** link is located in the right top corner of all of the Intelligent Capture Administrator windows and panes.

Table 10-53: Print Window

Element	Description
Print	Use the default print features.
Print a table:	
Frame at the (top/bottom/left/right)	Prints the indicated frame only.
Selected rows	Prints only the selected rows in the table.
Current page	Prints only the rows within the current page.
Page range	Prints the rows specified in the page range.
All Pages	Prints all of the rows in the table.

Related Topics

"Customizing Information Tables Using the Column Manager" on page 112

10.19 Select User or Group

The **Select User or Group** window enables selection of users or groups from the system directory that the current user has access to. When selecting users or groups for use in other windows (e.g., the **Access Control List** window), the **Select Users or Groups** window enables you to run a filter to find the specific individuals or groups.

Depending on granted permissions, some of these options may be disabled in Intelligent Capture Administrator.

Table 10-54: Select User or Group Window

Element	Description
Use domain or workstation filter	Select the check box and choose the domain in which to search. The domains list is populated with domains available to currently logged-in user.
Use name filter (Use* for a wild card search)	Select the check box and type the names to search for. This text box uses .NET regular expression syntax.

Element	Description
Maximum number of results	Select the check box and type the maximum number of users or groups to display in the **Result List**.
Include built-in security principals	Select the check box to include the built-in security principals of the operating system.
Results List	The list of users or groups based on the specified search criteria.

Related Topics

"Intelligent Capture Permissions List" on page 381

10.20 Values

The **Values** window displays the IA Values associated with a process or a module.

Note: The **Available Columns** listings described in this table can be displayed or hidden in Intelligent Capture Administrator by right-clicking the column header in the table pane and then selecting the columns to display or hide. Depending on the defined configuration columns display, not all of the columns described in this topic may be seen.

Table 10-55: Values Window

Element	Description
Tree view: Displays various nodes that enable navigation through the various IA Value types for the selected process or module. The IA Values list on the right displays the actual IA Values for the selected tree node.	
Step Values	Contains a subnode for each module step in the process. Selecting a module step node displays the global setup values for the module associated with the selected module step.
Default Node Level Values	Contains a subnode for each level (0-7). Selecting a subnode displays the default IA Values defined in the *MDF* file for the selected level. After a default value has been set, nodes created after that point will not be affected by subsequent changes to the default value. **Note:** Changes to a default value propagate to existing nodes if the default value has never been set prior to creating the nodes.

Element	Description
Non-nodal Values	Global IA Values for the process or step.
IA Values list (right area): Displays the following information about the IA Values for the tree node selected from the **Process/Module** tree view. Depending on the tree node selected, some of these columns may not apply.	
Filter	Specify the step to filter on. The list of IA Values is filtered to display only those IA Values associated with the selected step.
Value Name	IA Value name.
Value Type	IA Value type.
Setting	Value set for the IA Value.
Input	Selected if the IA Value is an Input IA Value (variable that is used as input data).
Output	Selected if the IA Value is an Output IA Value (variable that is used as output data).
Trigger	Selected if the IA Value is a Trigger IA Value (variable that is used to notify an Intelligent Capture Server that a task is ready for processing).
Prefetch	Selected if the IA Value is a Prefetch IA Value (file that is sent with the task).
Prime	Selected if the IA Value is a Prime IA Value (variable that is sent with the task).
Step	The name of the module step if the IA Value is associated with a module.
Level Name	The level name where the module step IA Value exists.
Level Number	Tree level number of the module step IA Value.

Related Topics

"Adding a Batch" on page 170

"Configuring a Process Step in Setup Mode" on page 157

"Viewing and Defining Access Control for a Process" on page 160

"Copying Step, Process, and Batch Settings" on page 197

"Customizing Information Tables Using the Column Manager" on page 112

Chapter 11

Intelligent Capture Administrator Reference

The topics within this section contain reference information useful while using Intelligent Capture Administrator.

11.1 Intelligent Capture Server Parameters

This section describes Intelligent Capture Server parameters:

Note: Viewing and editing server settings is only available in Intelligent Capture Administrator 7.5 and later.

Table 11-1: List of Intelligent Capture Server Parameters

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
BatchInitThreads	Number of batches that the Intelligent Capture Server will load at the same time during startup.	*RW*	4	1	50

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
BatchMaxAddressSpaceK	Maximum amount of virtual address space that the Intelligent Capture Server allows batches to use. When this limit is reached, the server will unload batches (starting with those least recently used) to keep the server from running out of memory. The default (recommended) and maximum values for this setting depend on the operating system type and the /3GB memory switch. For optimal performance, it is recommended that this parameter be set to 0.5 GB less than the machine's physical memory. For example, if a machine has 16 GB of	*RW*	3145728 KB (3.0 GB)	32768 KB (32 MB)	Dependent on the operating system.

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
	physical memory, then this parameter would be 16252928 (15.5 GB).				

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
BatchMaxLoaded	Maximum number of batches that can be loaded at a time. At a minimum, set this value equal to the number of active batches or connected modules, whichever is less. **Note:** The limit specified by "Batch MaxAddressSpaceK" takes precedence over the limit specified by "Batch MaxLoaded". For example, if "Batch MaxLoaded" is set to 65, and 20 batches are loaded that reach the	*RW*	100,000,000	1	Max. integer

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
	limit specified by "Batch MaxAddressSpaceK", then the Intelligent Capture Server will not load a 21st batch (even though "Batch MaxLoaded" is set to allow the loading of up to 65 batches). Instead, the Server will unload one of the 20 batches, then load another batch, keeping the total at 20.				

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
BatchMaxVBProjectsLoaded	Maximum number of Visual Basic (*VB*) projects loaded at any given time. The Intelligent Capture Server loads up the projects until this limit is reached, at which time it will free the last used *VB* project.	*RW*	100	1	1000
BatchShrink	Shrinks batch and process files when closing. This requires slightly less disk space at the cost of slowing the server down.	*RW*	0 (False)	0	1

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
BatchSync	Maximum number of seconds that the Intelligent Capture Server waits before saving batch and process files to its disk. If the Intelligent Capture Server must be restarted due to a power failure, critical software failure, or other abnormal termination, then the state of the batch is restored using information committed to disk during the last commit.	*RW*	300 seconds	1 second	Max. integer

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
BatchSyncMaxTime	Maximum amount of time spent syncing a set of batches. If set to 0 (the default) the server spends as much time as necessary to sync batches. Setting to a non-zero value may result in the batches not being synced as frequently as specified in the "BatchSync" parameter.	*RW*	0 *msecs*	0	Max. integer

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
CanPauseWhileDebugging	Determines if the Intelligent Capture Server can be paused while a batch is being debugged in Process Developer. If set to 1 (default), then the server can pause during debugging and will disconnect any instances of Process Developer. If set to zero, the Intelligent Capture Server cannot be paused during debugging.	*RW*	1 (True)	0	1
ClientPing	Number of seconds a client module must be unresponsive before the Intelligent Capture Server pings it.	*RW*	60 seconds	1	Max. integer

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
ClientTimeout	Number of seconds a client module must be unresponsive before the Intelligent Capture Server forcefully disconnects it.	*RW*	300 seconds	1 second	Max. integer
ClusterReconnectTime	Number of milliseconds this Intelligent Capture Server will wait until it attempts to reconnect to a server to which it does not have a connection. If it fails, then it will try again in "ClusterReconnectTime".	*RW*	60000 msecs	5000 msecs	Max. integer
ClusterTimeout	The period that the Intelligent Capture Server will wait for a response when communicating with another server in a ScaleServer group.	*RW*	10000 msecs	100 msecs	Max. integer

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
ConsoleLCID	This is the locale ID in its decimal form. For example, 1033 specifies English-USA, and 2052 specifies Chinese-PRC. This setting is used by the server to determine the language in which to display messages on the console.	*RW*	At first start-up, the server checks if the *Locale* parameter has been specified for Intelligent Capture applications in `win.ini` file. If it is specified, then **ConsoleLCID** is set to that value in the database. You may reset this value using the Intelligent Capture Administrator. The default value for **ConsoleLCID** is taken from **Windows Regional Options (Formats and Standards)**.	-	-

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
CSThresholdDebugInMS	Debug threshold for which the server will log when processing threads are blocked. Any thread that is blocked (or blocking) for this long will log a record in the Intelligent Capture Server debug log file.	RW	2000 msec	0	Max. integer

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
DebugLevel	Error checking level for basic Intelligent Capture Server operations. We recommend using the default value of 1, although setting this value to zero may slightly increase the performance of the Intelligent Capture Server. The Intelligent Capture Server checks for errors after basic functions occur, including locking, unlocking, allocating, and reallocating memory and freeing disk space.	*RW*	1	0	1
DefaultBatchPriority			1	1	1
DisableCrypto	The server disables the encrypting that protects IA Values across the network.	*RW*	0 (False)	0	1

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
DisableIPV4	Disables listening for connections on IPv4 network. If both "DisableIPv4 " and "DisableIPv6 " are enabled, then the Intelligent Capture Server will not be able to receive any client connections.	R	0 (False)	0	1
DisableIPV6	Disables listening for connections on IPv6 network. If both "DisableIPv4 " and "DisableIPv6 " are enabled, then the Intelligent Capture Server will not be able to receive any client connections.	R	0 (False)	0	1

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
DiskReserveK	Specifies the amount of extra disk space (in KB) to reserve on the volume pointed to by "RootDir". The Intelligent Capture Server will stop processing and send a notification to the client modules after the available disk space on this volume falls below the amount determined by "BatchMaxAddressSpaceK" or "DiskReserveK".	*RW*	1536000 *KB* (1.5*GB*)	256 KB	Max. integer
EnforceVersionCheck	Enforces XPP process version to be the same as its CodeBehind DLLs.	R	1 (Enabled)	0	1

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
EventLogLevel	Determines the events that are recorded to the Windows Event Log. To determine which events are logged, use the following values. These values and the sum of these values are the only valid logging combinations: • 1/0x01: Errors • 2/0x02: Warnings • 4/0x04: Informati on • 8/0x08: Audit successes • 16/0x10: Audit failures • 128/0x80: Successes The default value is: 128 Successes + 16 Audit failures + 2 Warnings + 1 Errors = 147.	*RW*	147 (0x93)	0	0xFFFFFFFF

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
FileTraceBackupFileCount	Number of copies of the Intelligent Capture Server debug log file to save. Each time the server is started, a new debug log is created and older logs are deleted depending on the value of this setting.	*RW*	10	1	100

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
FileTraceLevel	Controls the logging that goes to the Intelligent Capture Server log file, `debug.out`. The following values can be added together to attain different logging levels: • 1: Miscellaneous • 2: Net • 4: Console • 8: Information • 16: Warning • 32: Error • 64: Fatal The default is: 64 Fatal + 32 Error + 16 Warning + 4 Console = 116	*RW*	116 (0x74)	0	0xFFFFFFFF

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
HideUserIdentity	If enabled, this parameter hides the user identity in logs or reports that are generated. This parameter cannot be turned off if the Intelligent Capture Server license includes a feature code "Q" .	*RW*	0 (False)	0	1
IOThreadCount	The number of main processing threads that will run simultaneously on the server. If it is set to 0 (default) then the server will choose a value that is 5 times the number of physical CPU cores for the machine.	R	0	0	Max. integer

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
LLVFatalErrorEnable	Controls whether lock level violations are considered fatal or not. If this setting is disabled (0), any lock level violation will produce a crash dump file and terminate the server. By default, these violations are tracked but do not terminate the server.	RW	1 (True)	0	1

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
LogScriptQueueLengthInterval	Specifies the period (in minutes) for which the maximum queue lengths in each of the VBA and VB.Net hosts are calculated and reported in the `debug.out` file. After the maximum queue lengths are calculated for the period and then reported, they are reset to 0 such that the maximum values in the next period can be calculated. The default is 10 minutes. **Note:** At any single time, more than 1 item of work is usually queued for processing by one of these hosts. Examples of the entries in the `debug.out` file	R/W	10 (Minutes)		

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
	would appear as follows: `VBNet Max Queue Length: 2 VBA Max Queue Length: 1 1 1` The number of values reported correlates to the `MaxVBNetHost` and `MaxVBAHost` parameters. Because this reporting is a low overhead operation, this parameter might be set to a number lower than the default (for more frequent reporting); however, under a heavy load, the reported value would not change significantly from one period to the next.				

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
MaxDebugOutMaxK	Maximum allowed size in KB, of the Intelligent Capture Server debug log file. After the file reaches the maximum size, debug messages begin overwriting the oldest debug messages in the file. A value of 0 indicates unlimited size for the file.	*RW*	1000000 KB (1 GB)	0	Max. integer

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
MaxVBAHost	Specifies the number of simultaneous, out-of-process 32-bit VBA engines to be used for processing VBA-based batches (any IPP, or XPP built in Intelligent Capture 7.1 or earlier). If running VBA-based batches, it is recommended that you set this parameter to 3. Increasing it beyond that would increase overall CPU usage but might not yield any measurable improvement in performance. **Note:** If you are processing only batches based on XPPs compiled under Intelligent Capture 7.5,	RW	3	1	100

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
	this setting is not relevant because VBA would not be used.				

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
MaxVBNetHosts	Specifies the number of simultaneous, in-process .NET-based CaptureFlow processing hosts used to process XPPs compiled under Intelligent Capture 7.5 or later. All Intelligent Capture 7.5 (and later) XPPs use compiled .NET code assemblies on the Intelligent Capture Server to perform CaptureFlow logic execution (value assignments, conditional expression evaluation for flow routing or other assignments, as well as customer-written CaptureFlow scripting). With additional VBNetHosts, several batches can be processed simultaneously. Although	RW	3	1	100

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
	the default value is 1, it is recommended that you set this parameter to at least 3 or to about half of the number of CPU cores on your machine. For more information, see the *Performance and Tuning Guide*.				
PagesToBorrow	The number of pages that an Intelligent Capture Server can borrow from another server in a ScaleServer group when the Intelligent Capture Server runs out of its own pages. The server borrows pages in multiples of this value rather than a single page at a time.	*RW*	1000 pages	100	100000

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
RequireLatestClient	Ensures that the client module version matches the version of Intelligent Capture Server that is running. Setting this value to 1 disallows any client modules to connect that use a client *DLL* prior to the release of the Intelligent Capture Server. Typically this only allows compatibility enforcement of major product revisions, for example, requiring 7.0 client modules with Intelligent Capture 7.0 . Setting this value to 0 enables an older or current client module version to connect to the Intelligent Capture Server.	*RW*	0 (False)	0	1

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
RootDir	Root directory in which to place all the Intelligent Capture Server and Intelligent Capture related files, such as batches and processes. By default, this folder is set to: `c:\IAS`. **Note:** Turn off any virus checking of this folder since it results in performance degradation of Intelligent Capture.	R	`c:\IAS`	N/A	N/A
SecurityPackage	Determines the security package to be used. By default, this is set to "Negotiate". Other acceptable values include: • *NTLM* • Kerberos	R	Negotiate	N/A	N/A

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
StringTraceLevel	Level at which string tracing occurs when running the Intelligent Capture Server as an application. This parameter controls the level of logging displayed at the Intelligent Capture Server command prompt. The following values can be added together to attain different logging levels: • 1: Miscellaneous • 2: Net • 4: Console • 8: Information • 16: Warning • 32: Error • 64: Fatal The default is: 64 Fatal + 32 Error + 16 Warning + 4 Console = 116	*RW*	116 (0x74)	0	0xFFFFFFFF

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
TaskFinishOnTaskClear	Controls whether the task finish event processing will occur when a module calls `TaskClear` instead of `TaskFinish`. The setting is a string value that specifies one or more modules for which the new behavior should apply. Modules are specified by their short name and must be comma separated with no additional spaces. If a listed module issues a `TaskClear` call, the server will fire a task finish event the same as it does for `TaskFinish` and corresponding entries will be created in the Reports Task tables.	R	Blank	N/A	N/A

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
TcpIpPort	The *TCP/IP* port name or port number of the Intelligent Capture Server.	R	10099	N/A	N/A

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
TcpIpAddress	The TCP/IP address for the IPv4 protocol. • This parameter supports Microsoft Cluster configuration and is used primarily so that the Intelligent Capture Server is restricted to listen to the specific IPv4 protocol address configured for the cluster. • If used to support cluster configuration, this value must be set to a single cluster-defined IP address for the Intelligent Capture Server. If this value is not set and left blank, then this protocol will not be	R/W	Blank.	N/A	N/A

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
	used for the cluster configuration. • If this protocol is not used in a cluster configuration, then it must be left blank so that the server can listen to all IP addresses on the computer. By default it is assumed that the server is not configured for a cluster environment and must be left blank so that it can listen to all IP addresses on the computer.				

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
TcpIpv6Address	The TCP/IP address for the IPv6 protocol. • This parameter supports Microsoft Cluster configuration and is used primarily so that the Intelligent Capture Server is restricted to listen to the specific IPv6 protocol address configured for the cluster. • If used to support cluster configuration, this value must be set to a single cluster-defined IP address for the Intelligent Capture Server. If this value is not set and left blank, then this protocol will not be	R	Blank.	N/A	N/A

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
	used for the cluster configuration. • If this protocol is not used in a cluster configuration, then it must be left blank so that the server can listen to all IP addresses on the computer. By default it is assumed that the server is not configured for a cluster environment and must be left blank so that it can listen to all IP addresses on the computer.				

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
TrackDailyPageCountUsage	For counting with limited page count licenses, logs the page count usage per day (24 hours). The data is available through performance counters (`IA:Server_Intelligent Capture_Licenses`) and in the Administration Console.	*RW*	1 (Enabled)	0	1
TriggerIfEmpty	When this is set to the default, tasks that have no children nodes are considered triggered.	*RW*	1 (True)	0	1

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
ValuesBackupTime	The frequency at which the `value.idx` file is automatically backed up as `values.bak`. When the server next restarts, if it detects a problem with the current `values.idx`, it copies `values.bak` as `values.idx`, and attempts to start again.	*RW*	3600 seconds	0	Max. integer

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
VBARoundRobin	Enables (`1`) or disables (`0`) a simple round-robin assignment of new batches to VBA processing hosts. For example, if `VBARoundRobin = 1` and `MaxVBAHost = 3`, then 3 hosts are spawned and batches are assigned to each host in alternating order as follows: • Host 1 Batches: 1, 4 , 7, 10 • Host 2 Batches: 2, 5, 8, 11 • Host 3 Batches: 3, 6, 9, 12 If `VBARoundRobin = 0` and `MaxVBAHost = 3`, then new batches are assigned to the VBA host that appears to be the least busy at that instant. It is recommended that you set this	R	1 (Enabled)	0	1

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
	parameter to 1 because round robin assignment, in general, balances the load more effectively. **Notes** • VBNet batches (compiled under Intelligent Capture 7.5 or later) are always assigned to VB.Net hosts in a round-robin sequence. • After a batch is assigned to a particular VBA host,				

Server Parameter Name	Description	Read/ Write (R/W)	Default Value	Min. Value	Max. Value
	then it continues to be processed by the same host for as long as the batch remains in memory.				

11.2 Intelligent Capture Permissions List

Intelligent Capture Administrator assigns permissions to control access to Intelligent Capture functionality within the Intelligent Capture Administrator itself and all client modules. If users do not have the appropriate permissions, then they will not be able to perform necessary operations. The following is a list of the security permissions in Intelligent Capture.

Note: The prefix of the permission determines the component to which the permission applies:

- *AC*: Applies to using the functionality in Intelligent Capture Administrator.
- <*Module name*>: Applies to using the functionality in the specific module.
- Server: Applies to connecting to the Intelligent Capture Server and accessing the functionality of the Intelligent Capture Server.
- System: Applies to using the specific functionality in all client modules.

Table 11-2: Intelligent Capture Permissions

Permission	Description
AC.GlobalOptionsModify	Modify the global **Default Settings** set in Intelligent Capture Administrator from the **Options** navigation panel.
AC.GlobalOptionsRead	View the global options set.

Permission	Description
AC.LicenseModify	Add and remove licenses from the system.
AC.LicenseRead	View the licenses and module licenses installed in the system.
AC.Login	The permission to log in to Intelligent Capture Administrator.
AC.LogModify	Delete logs from the system.
AC.LogRead	View logs created by components of the system, create and use log view filters, and view log rules.
AC.LogRuleModify	Create rules defining which log events get saved in the system and where they get saved to.
AC.PreventBatchDelete	Prevent user from deleting a batch.
AC.PurgeExecute	Execute configured purges manually.
AC.PurgeModify	Modify configured purges and purge definitions.
AC.PurgeRead	View configured purges and purge definitions.
AC.ReportExecute	Run configured reports to get results in the Crystal Reports viewer.
AC.ReportModify	Modify configured reports and report definitions.
AC.ReportRead	View configured reports and report definitions.
AC.WSHostingModify	Add, modify, delete web services hostings and their settings.
AC.WSHostingRead	View web services hostings and their settings.
AC.WSModify	Add, modify, delete web services and their settings.
AC.WSRead	View web services and their settings.
Desktop.ExecuteAccess	Log in to the Completion module.
Desktop.RunAllBatches	Enables the operator to view and select the **All batches** option when getting work in the Completion module.
Desktop.RunSingleBatch	Enables the operator to select a single batch when getting work in the Completion module.
DocumentumAdvancedExport.Login	Log in to the Documentum Advanced Export module.

Permission	Description
DWebClient.Login	In conjunction with other permissions, enables an operator to perform the following tasks in the Intelligent Capture Web Client: • Logging in • Creating batches • Processing all batches • Processing a single batch • Administering REST and Intelligent Capture Web Client licensing (from the **License Administration** page) For information about the required permissions, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.
DWebClient.runSingleBatch	In conjunction with other permissions, enables an operator to process a single batch in the Intelligent Capture Web Client. For information about the required permissions, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.
Identification.ExecuteAccess	Log in to the Identification module.
Identification.RunAllBatches	Enables the operator to view and select the **All batches** option when getting work in the Identification module.
Identification.RunSingleBatch	Enables the operator to select a single batch when getting work in the Identification module.
ImageConverter.Login	Log in to the Image Converter module, version 6.5 or 6.5 SP1. This permission is not used nor required for the 7.0 version of Image Converter.
NuanceOCR.Login	Log in to NuanceOCR.
RescanPlus.ChangeScanConfig	Change the scanning configuration in RescanPlus.
RescanPlus.Login	Log in to RescanPlus.
RescanPlus.ReorderImages	Add, move, and delete images in RescanPlus.
RescanPlus.SetupInstance	Set up a RescanPlus step.
RescanPlus.ShowBatchesWithoutTasks	Displays **Show only batches with ready tasks** check box for the RescanPlus operator.
RescanPlus.RunAll	Enables the operator to run all batches in RescanPlus.

Permission	Description
ScanPlus.AllowOpenReleasedBatches	Enables displaying released batches in the ScanPlus batch list.
ScanPlus.ChangeScanConfig	Change the scanning configuration defined in ScanPlus.
ScanPlus.Login	Log in to ScanPlus.
ScanPlus.ReorderImages	Add, move, and delete images in ScanPlus.
ScanPlus.SetupInstance	Set up a ScanPlus step.
Server.Copy.Batch.to.Server	Copy batches to the Intelligent Capture Server using the Copy module or Intelligent Capture Administrator.
Server.Create.Batch	Create batches to the server.
Server.Debug	Obtain server debug information. This permission is needed to start a debugging session in Process Developer to debug a batch.
Server.Install.Process	Install processes on the server. This permission also enables users to install scripts created using the CaptureFlow Script Editor.
Server.Log.Message	Obtain server log messages.
Server.Login	Log in to the Intelligent Capture Server.
Server.Read.Module.Data	Read module data from the server.
Server.SetLogContext	Set server log context data. For internal use only.
Server.Write.Module.Data	Write module data to the server.
System.BatchModify	Modify batch data. This includes scanning, indexing, image enhancement, and other operations that modifies batch data.
System.BatchRead	View the batches in the system along with their state and settings. **Note:** Intelligent Capture Administrator users with the **System.BatchRead** permission can read protected values associated with a batch even if they have not been assigned the **System.ReadProtectedValues** permission. However, for users running client modules, being able to read protected values requires the **System.ReadProtectedValues** permission.

Permission	Description
System.ModifyProtectedValues	Modify protected IA Values.
System.ProcessModify	Add, modify, delete Intelligent Capture processes and to deploy scripts to the system. This permission is also required for users to establish a connection between Intelligent Capture Designer and the Server.
System.ProcessRead	View the Intelligent Capture processes installed in the system and view their settings. **Note:** Intelligent Capture Administrator users with the **System.ProcessRead** permission can read protected values associated with a process even if they have not been assigned the **System.ReadProtectedValues** permission. However, for users running client modules, being able to read protected values requires the **System.ReadProtectedValues** permission.
System.ReadProtectedValues	Read protected IA Values.
System.SecurityModify	Write *ACL* security data. This permission is required to make any security changes to the roles, process, batch, and department ACLs.
System.SecurityRead	Read *ACL* security data.
System.ServerModify	Update connection settings for servers, add and modify ScaleServer groups.
System.ServerRead	View the servers installed in the Intelligent Capture Database, as well as the ScaleServer groups in the system. This permission is required for any client attempting to connect to a ScaleServer group.
WebServices.WSInput.Login	Log in to the Web Services Input module.
WebServices.WSOutput.Login	Log in to the Web Services Output module.

Related Topics

"Understanding Permissions" on page 134

"Permissions for Running in Production Mode" on page 135

11.3 Predefined Roles

Intelligent Capture Administrator enables administrators to configure roles and assign permissions to individuals responsible for performing tasks in Intelligent Capture Administrator. The following is a list of the predefined roles for Intelligent Capture, that are listed in the **Roles** pane.

Table 11-3: Intelligent Capture Predefined Roles

Role	Description
Administrators	Includes all Intelligent Capture permissions. Only users in this role are granted complete access to Intelligent Capture Server objects such as batches and process.
System Monitor	Includes all Intelligent Capture permissions needed to operate the Intelligent Capture Administrator in a read-only mode for monitoring the status of the system. No default members are assigned to this role.
Module Operator	Includes the common Intelligent Capture permissions required to work with modules. No default members are assigned to this role.
Index Operator	Includes Completion permissions. To use this role, a member must be assigned to both the **Module Operator** and **Index Operator** roles. No default members are assigned to this role.
Scan Operator	Includes all ScanPlus and RescanPlus permissions and the **Server.Create.Batch** permission. To use this role, a member must be assigned to both the **Module Operator** and **Scan Operator** roles. No default members are assigned to this role.
DocumentumExport Operator	Includes the permissions required to work with the Documentum Advanced Export Module, including **DocumentumAdvancedExport.Login**, **System.ReadProtectedValues**, and **System.ModifyProtectedValues**. To use this role, a member must be assigned to both the **Module Operator** and **DocumentumExport Operator** roles. No default members are assigned to this role.
eInput Operator	Includes all eInput permissions and the **Server.Create.Batch** permission. To use this role, a member must be assigned to both the **Module Operator** and **Scan Operator** roles. No default members are assigned to this role.

Related Topics

"Defining Roles, Role Members, and Role Permissions" on page 132

"Adding Users and Groups to Roles" on page 142

"Configuring Roles" on page 131

"Add Roles and Role Settings" on page 266

"Viewing Roles" on page 131

11.4 System Log Rules

Log rules determine what data is logged, when the data is logged, and where the data is logged. Intelligent Capture includes several system log rules. These log rules cannot be modified.

Note: System log rules are disabled by default. To log data defined by the log rule, make sure the log rule is enabled. For information on how to enable or disable a log rule, see "Enabling and Disabling Log Rules, and Blocking Logs Based on Log Rules" on page 218.

This section contains details of all the system log rules included with Intelligent Capture.

11.4.1 AllDebugInfos Rule

The **AllDebugInfos** log rule logs general debugging information to the `DebugLog.log` file. On Windows 7, this file is located by default in the directory: `$CommonApplicationData$\EMC\InputAccel\DebugLog`

Table 11-4: Details about the AllDebugInfos Log Rule

Log Description	Logs general debugging information from all modules.
Log Type (type of information logged)	Debug information.
Scope Component (the Intelligent Capture component that is logged)	Not applicable.
Filter Definition (determines the events that trigger the log rule)	FilterAllDebugInfos
Data Definition (determines the data that is logged)	DataAllDebugInfos
Sink Definition (determines the log destination)	DebugSink
Enabled/Disabled by Default	Disabled

11.4.2 AllErrors Rule

The **AllErrors** log rule logs all errors from all client modules. These errors can be viewed in Intelligent Capture Administrator.

Table 11-5: Details about the AllErrors Log Rule

Log Description	Logs all errors from all client modules.
Log Type (type of information logged)	Error
Scope Component (the Intelligent Capture component that is logged)	Not applicable.
Filter Definition (determines the events that trigger the log rule)	FilterAllErrors
Data Definition (determines the data that is logged)	DataAllErrors
Sink Definition (determines the log destination)	ErrorToDBSink
Enabled/Disabled by Default	Disabled

11.4.3 AllLogLibraryDebugInfos Rule

The **AllLogLibraryDebugInfos** log rule logs all DebugInfo logs from the Logging library to the `LOGDebug.log` file. This rule can be used as a template to create custom debug logging rules. On Windows 7, the `LOGDebugLog.log` file is located by default in the directory: `$CommonApplicationData$\EMC\InputAccel\DebugLog`

Table 11-6: Details about the AllLogLibraryDebugInfos Log Rule

Log Description	Logs debug information from the Logging library.
Log Type (type of information logged)	Debug information.
Scope Component (the Intelligent Capture component that is logged)	`Emc.InputAccel.Logging.Log` (Logging library)
Filter Definition (determines the events that trigger the log rule)	FilterAllDebugInfos
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	LOGDebugSink
Enabled/Disabled by Default	Disabled

11.4.4 AllLogLibraryErrors Rule

The **AuditAllLogLibraryEvents** log rule logs all log errors. These errors can be viewed in Intelligent Capture Administrator.

Table 11-7: Details about the AllLogLibraryErrors Log Rule

Log Description	Logs all log errors.
Log Type (type of information logged)	Error
Scope Component (the Intelligent Capture component that is logged)	`Emc.InputAccel.Logging.Log` (Logging library)
Filter Definition (determines the events that trigger the log rule)	FilterAllErrors
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	ErrorToDBSink
Enabled/Disabled by Default	Disabled

11.4.5 AllLogLibraryWarnings Rule

The **AllLogLibraryWarnings** log rule logs all log warnings. These warnings can be viewed in Intelligent Capture Administrator.

Table 11-8: Details about the AllLogLibraryWarnings Log Rule

Log Description	Logs all log warnings.
Log Type (type of information logged)	Warning
Scope Component (the Intelligent Capture component that is logged)	`Emc.InputAccel.Logging.Log` (Logging library)
Filter Definition (determines the events that trigger the log rule)	FilterAllWarnings
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	ErrorToDBSink
Enabled/Disabled by Default	Disabled

11.4.6 AllServerWarnings Rule

The **AllServerWarnings** log rule logs all warnings from the Intelligent Capture Server. These warnings can be viewed in Intelligent Capture Administrator.

Table 11-9: Details about the AllServerWarnings Log Rule

Log Description	Logs all warnings from the Intelligent Capture Server.
Log Type (type of information logged)	Warning
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterAllServerWarnings
Data Definition (determines the data that is logged)	DataAllErrors
Sink Definition (determines the log destination)	ErrorToDBSink
Enabled/Disabled by Default	Disabled

11.4.7 AllWarnings Rule

The **AllWarnings** log rule logs all warnings from all client modules. These warnings can be viewed in Intelligent Capture Administrator.

Table 11-10: Details about the AllWarnings Log Rule

Log Description	Logs all warnings from all client modules.
Log Type (type of information logged)	Warning
Scope Component (the Intelligent Capture component that is logged)	Not applicable.
Filter Definition (determines the events that trigger the log rule)	FilterAllWarnings
Data Definition (determines the data that is logged)	DataAllErrors
Sink Definition (determines the log destination)	ErrorToDBSink
Enabled/Disabled by Default	Disabled

11.4.8 AuditAdminConsoleEvents Rule

The **AuditAdminConsoleEvents** log rule logs all events from Intelligent Capture Administrator. These events can be viewed in Intelligent Capture Administrator.

Table 11-11: Details about the AuditAdminConsoleEvents Log Rule

Log Description	Logs all events from Intelligent Capture Administrator.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	ADMINCSL (Intelligent Capture Administrator).
Filter Definition (determines the events that trigger the log rule)	*FilterAllEvents*
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.9 AuditAdminConsoleSECEvents Rule

The **AuditAdminConsoleSECEvents** log rule logs at-rest security events from Intelligent Capture Administrator. These events can be viewed in Intelligent Capture Administrator.

Table 11-12: Details about the AuditAdminConsoleSECEvents Log Rule

Log Description	Logs at-rest security events from Intelligent Capture Administrator.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	ADMINCSL (Intelligent Capture Administrator).
Filter Definition (determines the events that trigger the log rule)	*FilterAllEvents*
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.10 AuditSECEvents Rule

The **AuditSECEvents** log rule logs all events from the Security library. These events can be viewed in Intelligent Capture Administrator.

Table 11-13: Details about the AuditSECEvents Log Rule

Log Description	Logs all events from the Security library
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	SEC (Security component)
Filter Definition (determines the events that trigger the log rule)	FilterAllEvents
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.11 AuditServerBatchCategoryEvents Rule

The **AuditServerBatchCategoryEvents** log rule logs all Batch category events from the Intelligent Capture Server. These events can be viewed in Intelligent Capture Administrator.

Table 11-14: Details about the AuditServerBatchCategoryEvents Log Rule

Log Description	Logs all events from the server that belong to the Batch category.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterServerBatchCategoryEvents
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.12 AuditServerConfigFileCategoryEvents Rule

The **AuditServerConfigFileCategoryEvents** log rule logs all ConfigFile category events from the Intelligent Capture Server. These events can be viewed in Intelligent Capture Administrator.

Table 11-15: Details about the AuditServerConfigFileCategoryEvents Log Rule

Log Description	Logs all events from the server that belong to the ConfigFile category.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterServerConfigFileCategoryEvents
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.13 AuditServerConnectionCategoryEvents Rule

The **AuditServerConnectionCategoryEvents** log rule logs all Connection category events from the Intelligent Capture Server. These events can be viewed in Intelligent Capture Administrator.

Table 11-16: Details about the AuditServerConnectionCategoryEvents Log Rule

Log Description	Logs all events from the server that belong to the Connection category.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterServerConnectionCategoryEvents
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.14 AuditServerEventCategoryEvents Rule

The **AuditServerEventCategoryEvents** log rule logs all Server category events from the Intelligent Capture Server. These events can be viewed in Intelligent Capture Administrator.

Table 11-17: Details about the AuditServerEventCategoryEvents Log Rule

Log Description	Logs all events from the server that belong to the Server category.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterServerEventCategoryEvents
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.15 AuditServerNodeCategoryEvents Rule

The **AuditServerNodeCategoryEvents** log rule logs all Node category events from the Intelligent Capture Server. These events can be viewed in Intelligent Capture Administrator.

Table 11-18: Details about the AuditServerNodeCategoryEvents Log Rule

Log Description	Logs all events from the server that belong to the Node category.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterServerNodeCategoryEvents
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.16 AuditServerNodeVerboseCategoryEvents Rule

The **AuditServerNodeVerboseCategoryEvents** log rule logs all NodeVerbose category events from the Intelligent Capture Server. These events can be viewed in Intelligent Capture Administrator.

Note: These events are logged only if the Reporting feature is licensed on the Intelligent Capture Server.

Table 11-19: Details about the AuditServerNodeVerboseCategoryEvents Log Rule

Log Description	Logs all events from the server that belong to the NodeVerbose category.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterServerNodeVerboseCategoryEvents
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.17 AuditServerProcessCategoryEvents Rule

The **AuditServerProcessCategoryEvents** log rule logs all Process category events from the Intelligent Capture Server. These events can be viewed in Intelligent Capture Administrator.

Table 11-20: Details about the AuditServerProcessCategoryEvents Log Rule

Log Description	Logs all events from the server that belong to the Process category.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterServerProcessCategoryEvents
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	AuditToDBSink

Enabled/Disabled by Default	Disabled

11.4.18 AuditServerSecurityCategoryEvents Rule

The **AuditServerSecurityCategoryEvents** log rule logs all Security category events from the Intelligent Capture Server. These events can be viewed in Intelligent Capture Administrator.

Table 11-21: Details about the AuditServerSecurityCategoryEvents Log Rule

Log Description	Logs all events from the server that belong to the Security category.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterServerSecurityCategoryEvents
Data Definition (determines the data that is logged)	DataServerSecurityCategoryEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.19 AuditServerStageFileCategoryEvents Rule

The **AuditServerStageFileCategoryEvents** log rule logs all StageFile category events from the Intelligent Capture Server. These events can be viewed in Intelligent Capture Administrator.

Table 11-22: Details about the AuditServerStageFileCategoryEvents Log Rule

Log Description	Logs all events from the server that belong to the StageFile category.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterServerStageFileCategoryEvents
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.20 AuditServerStepCategoryEvents Rule

The **AuditServerStepCategoryEvents** log rule logs all Step category events from the Intelligent Capture Server. These events can be viewed in Intelligent Capture Administrator.

Table 11-23: Details about the AuditServerStepCategoryEvents Log Rule

Log Description	Logs all events from the server that belong to the Step category.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterServerStepCategoryEvents
Data Definition (determines the data that is logged)	DataAllEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.21 AuditServerTaskCategoryEvents Rule

The **AuditServerTaskCategoryEvents** log rule logs all Task category events from the Intelligent Capture Server. These events can be viewed in Intelligent Capture Administrator.

Table 11-24: Details about the AuditServerTaskCategoryEvents Log Rule

Log Description	Logs all events from the server that belong to the Task category.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterServerTaskCategoryEvents
Data Definition(determines the data that is logged)	DataAllEvents
Sink Definition(determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.22 AuditServerValueCategoryEvents Rule

The **AuditServerValueCategoryEvents** log rule logs all Value category events from the Intelligent Capture Server. These events can be viewed in Intelligent Capture Administrator.

Table 11-25: Details about the AuditServerValueCategoryEvents Log Rule

Log Description	Logs all events from the server that belong to the Value category.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	Server (Intelligent Capture Server component).
Filter Definition (determines the events that trigger the log rule)	FilterServerValueCategoryEvents
Data Definition (determines the data that is logged)	DataServerValueEvents
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.4.23 CaptivaBatchDeleteReason

This log rule logs all BatchDeleteReason events from Intelligent Capture Administrator. These events can be viewed in Intelligent Capture Administrator.

Enabling this log rule also enables prompting the user to enter a reason when deleting a batch.

Table 11-26: Details about the CaptivaBatchDeleteReason Log Rule

Log Description	Logs all BatchDeleteReason events from Intelligent Capture Administrator.
Log Type (type of information logged)	Audit
Scope Component (the Intelligent Capture component that is logged)	ADMINCSL (Intelligent Capture Administrator).
Filter Definition (determines the events that trigger the log rule)	FilterBatchDeleteReason
Data Definition (determines the data that is logged)	*DataAllEvents*
Sink Definition (determines the log destination)	AuditToDBSink
Enabled/Disabled by Default	Disabled

11.5 System Filter Definitions

Filter definitions determine the events that trigger a log rule. Intelligent Capture includes several predefined system filter definitions that are used with the system log rules.

This section contains details of all the filter definitions used with the system log rules.

11.5.1 FilterAllDebugInfos Filter Definition

The **FilterAllDebugInfos** filter definition filters all debug information for the selected scope component, scope user, and scope workstation.

Table 11-27: Details about the FilterAllDebugInfos Filter Definition

Filter Description	Filters all debug information.
Log Type (type of information filtered)	Debug information.
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Any

11.5.2 FilterAllErrors Filter Definition

The **FilterAllErrors** filter definition filters all errors for the selected scope component, scope user, and scope workstation.

Table 11-28: Details about the FilterAllErrors Filter Definition

Filter Description	Filters all errors.
Log Type (type of information filtered)	Error
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Any

11.5.3 FilterAllEvents Filter Definition

The **FilterAllEvents** filter definition filters all events for the selected scope component, scope user, and scope workstation.

Table 11-29: Details about the FilterAllEvents Filter Definition

Filter Description	Filters all events.
Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any

Categories (the categories that are filtered)	Any

11.5.4 FilterAllServerWarnings Filter Definition

The **FilterAllServerWarnings** filter definition filters all warnings for the selected scope component, scope user, and scope workstation. It is used with the **AllServerWarnings** predefined log rule to filter all server warnings. This definition is identical to the **FilterAllWarnings** filter definition. If you are creating a custom log rule and want to use this filter definition to filter on Server warnings, you must set the **Scope Component** of the log rule to **Server**.

Table 11-30: Details about the FilterAllServerWarnings Filter Definition

Filter Description	Filters all warnings.
Log Type (type of information filtered)	Warning
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Any

11.5.5 FilterAllWarnings Filter Definition

The **FilterAllWarnings** filter definition filters all warnings for the selected scope component, scope user, and scope workstation.

Table 11-31: Details about the FilterAllWarnings Filter Definition

Filter Description	Filters all warnings.
Log Type (type of information filtered)	Warning
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Any

11.5.6 FilterBatchCreate Filter Definition

The **FilterBatchCreate** filter definition filters all events related to batch creation and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **ReportBatchCreate** log rule.

Table 11-32: Details about the FilterBatchCreate Filter Definition

Filter Description	Filters all events related to batch creation.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	10
Log Code Events (events that are filtered)	*BatchCreate*

Categories (the categories that are filtered)	Any

11.5.7 FilterBatchDelete Filter Definition

The **FilterBatchDelete** filter definition filters all events related to batch deletion and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **CaptivaBatchDelete** log rule.

Table 11-33: Details about the FilterBatchDelete Filter Definition

Filter Description	Filters all events related to batch deletion.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	11
Log Code Events (events that are filtered)	*BatchDelete*
Categories (the categories that are filtered)	Any

11.5.8 FilterBatchDeleteReason Filter Definition

The **FilterBatchDeleteReason** filter definition filters all events related to batch deletion reasons and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **CaptivaBatchDeleteReason** log rule.

Table 11-34: Details about the FilterBatchDeleteReason Filter Definition

Filter Description	Filters all events related to batch deletion reasons.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	1409
Log Code Events (events that are filtered)	*BatchDeleteReason*
Categories (the categories that are filtered)	Any

11.5.9 FilterBatchRename Filter Definition

The **FilterBatchRename** filter definition filters all events related to batch renaming and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **ReportBatchRename** log rule.

Table 11-35: Details about the FilterBatchRename Filter Definition

Filter Description	Filters all events related to batch renaming.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	19

Log Code Events (events that are filtered)	*BatchRename*
Categories (the categories that are filtered)	Any

11.5.10 FilterNodeCreate Filter Definition

The **FilterNodeCreate** filter definition filters all events related to node creation and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **ReportNodeCreate** log rule.

Table 11-36: Details about the FilterNodeCreate Filter Definition

Filter Description	Filters all events related to node creation.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	100
Log Code Events (events that are filtered)	*NodeCreate*
Categories (the categories that are filtered)	Any

11.5.11 FilterNodeDelete Filter Definition

The **FilterNodeDelete** filter definition filters all events related to node deletion and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **ReportNodeDelete** log rule.

Table 11-37: Details about the FilterNodeDelete Filter Definition

Filter Description	Filters all events related to node deletion.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	101
Log Code Events (events that are filtered)	*NodeDelete*
Categories (the categories that are filtered)	Any

11.5.12 FilterServerBatchCategoryEvents Filter Definition

The **FilterServerBatchCategoryEvents** filter definition filters all events from the server that belong to the Batch category. This filter can be applied to a scope component, scope user, and scope workstation.

Table 11-38: Details about the FilterServerBatchCategoryEvents Filter Definition

Filter Description	Filters all events from the server that belong to the Batch category.

Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Batch
Batch Category Events (events that are filtered)	• BatchLoad • BatchUnload • BatchSync • BatchRollback • BatchCreate • BatchDelete • BatchPriorityChange • BatchStatusChange • BatchStatusMessageChange • BatchDescriptionChange • BatchRename

11.5.13 FilterServerConfigFileCategoryEvents Filter Definition

The **FilterServerConfigFileCategoryEvents** filter definition filters all events from the server that belong to the ConfigFile category. This filter can be applied to a scope component, scope user, and scope workstation.

Table 11-39: Details about the FilterServerConfigFileCategoryEvents Filter Definition

Filter Description	Filters all events from the server that belong to the ConfigFile category.
Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	ConfigFile
ConfigFile Category Events (events that are filtered)	• ConfigFileWrite • ConfigFileDelete • ConfigFileRead

11.5.14 FilterServerConnectionCategoryEvents Filter Definition

The **FilterServerConnectionCategoryEvents** filter definition filters all events from the server that belong to the Connection category. This filter can be applied to a scope component, scope user, and scope workstation.

Table 11-40: Details about the FilterServerConnectionCategoryEvents Filter Definition

Filter Description	Filters all events from the server that belong to the Connection category.
Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Connection
Connection Category Events (events that are filtered)	• ModuleConnect • ModuleDisconnect

11.5.15 FilterServerEventCategoryEvents Filter Definition

The **FilterServerEventCategoryEvents** filter definition filters all events from the server that belong to the Server category. This filter can be applied to a scope component, scope user, and scope workstation.

Table 11-41: Details about the FilterServerEventCategoryEvents Filter Definition

Filter Description	Filters all events from the server that belong to the Server category.
Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Server
Server Category Events (events that are filtered)	• ServerStart • ServerStop • ServerPause • ServerContinue • ServerAddScaleServer • ServerRemoveScaleServer • ServerReady • ServerWIPLoadDone

11.5.16 FilterServerNodeCategoryEvents Filter Definition

The **FilterServerNodeCategoryEvents** filter definition filters all events from the server that belong to the Node category. This filter can be applied to a scope component, scope user, and scope workstation.

Table 11-42: Details about the FilterServerNodeCategoryEvents Filter Definition

Filter Description	Filters all events from the server that belong to the Node category.
Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Node
Node Category Events (events that are filtered)	• NodeCreate • NodeDelete • NodeMoveBegin • NodeMoveEnd

11.5.17 FilterServerNodeVerboseCategoryEvents Filter Definition

The **FilterServerNodeCategoryEvents** filter definition filters all events from the server that belong to the NodeVerbose category. This filter can be applied to a scope component, scope user, and scope workstation.

Table 11-43: Details about the FilterServerNodeVerboseCategoryEvents Filter Definition

Filter Description	Filters all events from the server that belong to the NodeVerbose category.
Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	NodeVerbose
NodeVerbose Category Events (events that are filtered)	• NodeFinishLevel0 • NodeFinishLevel1 • NodeFinishLevel2 • NodeFinishLevel3 • NodeFinishLevel4 • NodeFinishLevel5 • NodeFinishLevel6 • NodeFinishLevel7

11.5.18 FilterServerProcessCategoryEvents Filter Definition

The **FilterServerProcessCategoryEvents** filter definition filters all events from the server that belong to the Process category. This filter can be applied to a scope component, scope user, and scope workstation.

Table 11-44: Details about the FilterServerProcessCategoryEvents Filter Definition

Filter Description	Filters all events from the server that belong to the Process category.
Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Process
Process Category Events (events that are filtered)	• ProcessInstall • ProcessDelete • ProcessPriorityChange • ProcessDescriptionChange • ProcessRename • ProcessLoad • ProcessUnload

11.5.19 FilterServerSecurityCategoryEvents Filter Definition

The **FilterServerSecurityCategoryEvents** filter definition filters all events from the server that belong to the Security category. This filter can be applied to a scope component, scope user, and scope workstation.

Table 11-45: Details about the FilterServerSecurityCategoryEvents Filter Definition

Filter Description	Filters all events from the server that belong to the Security category.
Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Security
Security Category Events (events that are filtered)	• SecurityPermissionChange • SecurityCheckFailed

11.5.20 FilterServerStageFileCategoryEvents Filter Definition

The **FilterServerStageFileCategoryEvents** filter definition filters all events from the server that belong to the StageFile category. This filter can be applied to a scope component, scope user, and scope workstation.

Table 11-46: Details about the FilterServerStageFileCategoryEvents Filter Definition

Filter Description	Filters all events from the server that belong to the StageFile category.
Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	StageFile
StageFile Category Events (events that are filtered)	• StageFileWrite • StageFileDelete • StageFileRead

11.5.21 FilterServerStepCategoryEvents Filter Definition

The **FilterServerStepCategoryEvents** filter definition filters all events from the server that belong to the Step category. This filter can be applied to a scope component, scope user, and scope workstation.

Table 11-47: Details about the FilterServerStepCategoryEvents Filter Definition

Filter Description	Filters all events from the server that belong to the Step category
Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Step
Step Category Events (events that are filtered)	• StepSetDepartment

11.5.22 FilterServerTaskCategoryEvents Filter Definition

The **FilterServerTaskCategoryEvents** filter definition filters all events from the server that belong to the Task category. This filter can be applied to a scope component, scope user, and scope workstation.

Table 11-48: Details about the FilterServerTaskCategoryEvents Filter Definition

Filter Description	Filters all events from the server that belong to the Task category.
Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Task
Task Category Events (events that are filtered)	• TaskSent • TaskWorkStart • TaskFinish

11.5.23 FilterServerValueCategoryEvents Filter Definition

The **FilterServerValueCategoryEvents** filter definition filters all events from the server that belong to the Value category. This filter can be applied to a scope component, scope user, and scope workstation.

Table 11-49: Details about the FilterServerValueCategoryEvents Filter Definition

Filter Description	Filters all events from the server that belong to the Value category.
Log Type (type of information filtered)	Audit
Log Codes (the log codes that are filtered)	Any
Categories (the categories that are filtered)	Value
ValueCategory Events (events that are filtered)	• ValueCreate • ValueSet

11.5.24 FilterStageFileRead Filter Definition

The **FilterStageFileRead** filter definition filters all events related to reading the stage file and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **ReportStageFileRead** log rule.

Table 11-50: Details about the FilterStageFileRead Filter Definition

Filter Description	Filters all events related to reading the stage file.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	170
Log Code Events (events that are filtered)	StageFileRead
Categories (the categories that are filtered)	Any

11.5.25 FilterStageFileWrite Filter Definition

The **FilterStageFileWrite** filter definition filters all events related to writing the stage file and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **ReportStageFileWrite** log rule.

Table 11-51: Details about the FilterStageFileWrite Filter Definition

Filter Description	Filters all events related to writing the stage file.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	171
Log Code Events (events that are filtered)	StageFileWrite
Categories (the categories that are filtered)	Any

11.5.26 FilterTaskFinishCreatePage Filter Definition

The **FilterTaskFinishCreatePage** filter definition filters all events related to when a new page is created and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **ReportTaskFinishCreatePage** log rule.

Table 11-52: Details about the FilterTaskFinishCreatePage Filter Definition

Filter Description	Filters all events related to creating a page.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	130

Log Code Events (events that are filtered)	NodeFinishedTask_Level0
Categories (the categories that are filtered)	Any

11.5.27 FilterTaskFinishDonePage Filter Definition

The **FilterTaskFinishDonePage** filter definition filters all events related to when a page is done processing and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **ReportTaskFinishDonePage** log rule.

Table 11-53: Details about the FilterTaskFinishDonePage Filter Definition

Filter Description	Filters all events related to when a page is done processing.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	130
Log Code Events (events that are filtered)	NodeFinishedTask_Level0
Categories (the categories that are filtered)	Any

11.5.28 FilterTaskFinishIndexTask Filter Definition

The **FilterTaskFinishIndexTask** filter definition filters all events related to when an indexing task is finished processing and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **ReportTaskFinishIndexTask** log rule.

Table 11-54: Details about the FilterTaskFinishIndexTask Filter Definition

Filter Description	Filters all events related to when an indexing task finishes processing.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	123
Log Code Events (events that are filtered)	TaskFinish
Categories (the categories that are filtered)	Any

11.5.29 FilterTaskFinishOcrPage Filter Definition

The **FilterTaskFinishOcrPage** filter definition filters all events related to when an *OCR* task is finished processing and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **ReportTaskFinishOcrPage** log rule.

Table 11-55: Details about the FilterTaskFinishOcrPage Filter Definition

Filter Description	Filters all events related to when an *OCR* task on a page finishes processing.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	130
Log Code Events (events that are filtered)	NodeFinishedTask_Level0
Categories (the categories that are filtered)	Any

11.5.30 FilterTaskFinishPage Filter Definition

The **FilterTaskFinishPage** filter definition filters all events related to when a page is finished processing (with a success or error) and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **ReportTaskFinishPage** log rule.

Table 11-56: Details about the FilterTaskFinishPage Filter Definition

Filter Description	Filters all events related to when a page is finished processing.
Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	130
Log Code Events (events that are filtered)	NodeFinishedTask_Level0
Categories (the categories that are filtered)	Any

11.5.31 FilterTaskFinishTask Filter Definition

The **FilterTaskFinishTask** filter definition filters all events related to when any task is finished processing and can be applied to a scope component, scope user, and scope workstation. This filter definition is used in the **ReportTaskFinishTask** log rule.

Table 11-57: Details about the FilterTaskFinishTask Filter Definition

Filter Description	Filters all events related to when any task finishes processing.

Log Type (type of information filtered)	Statistic
Log Codes (the log codes that are filtered)	123
Log Code Events (events that are filtered)	TaskFinish
Categories (the categories that are filtered)	Any

11.6 System Data Definitions

Data definitions determine the data that is logged. Intelligent Capture includes several system data definitions that are used with the system log rules.

This section contains details of all the data definitions used with the system log rules.

11.6.1 DataAllDebugInfos Data Definition

The **DataAllDebugInfos** data definition logs data related to debug information from all client modules. This data definition is used in the **AllDebugInfos** log rule.

Table 11-58: Details about the DataAllDebugInfos Data Definition

Data Definition Description	Logs data from all client modules debug information.
Data logged	All information related logs

11.6.2 DataAllErrors Data Definition

The **DataAllErrors** data definition logs data related to all errors from all client modules. This data definition is used in the **AllErrors** log rule.

Table 11-59: Details about the DataAllErrors Data Definition

Data Definition Description	Logs data related to all errors from all client modules.

Additional Data Logged	• **Batch ID** • **Batch Name** • **Log Date** • **Module Step** • **Node ID** • **Node Level** • **Process ID** • **Process Name** • **Workstation Name** • **Task Module** • **Task User**

11.6.3 DataAllEvents Data Definition

The **DataAllEvents** data definition logs data related to all events from all client modules. This data definition is used in the **AuditAllEvents** log rule.

Table 11-60: Details about the DataAllEvents Data Definition

Data Definition Description	Logs data related to all events from all client modules.
Additional Data Logged	• **Batch ID** • **Batch Name** • **Log Date** • **Module Step** • **Node ID** • **Node Level** • **Process ID** • **Process Name** • **Workstation Name** • **Task Module** • **Task User**

11.6.4 DataBatchCreate Data Definition

The **DataBatchCreate** data definition logs data related to creating a batch. This data definition is used in the **ReportBatchCreate** log rule.

Table 11-61: Details about the DataBatchCreate Data Definition

Data Definition Description	Logs data related to creating a batch.
Additional Data Logged	• **Batch Name** • **Batch ID** • **Batch Creation Date and Time** • **Process Name** • **Process ID** • **Server Name** • **Task Module** • **Task User**

11.6.5 DataBatchDelete Data Definition

The **DataBatchDelete** data definition logs data related to deleting a batch. This data definition is used in the **ReportBatchDelete** log rule.

Table 11-62: Details about the DataBatchDelete Data Definition

Data Definition Description	Logs data related to deleting a batch.
Additional Data Logged	• **Batch ID** • **Batch Deletion Date and Time** • **Server Name** • **Task Module** • **Task User**

11.6.6 DataBatchRename Data Definition

The **DataBatchDelete** data definition logs data related to renaming a batch. This data definition is used in the **ReportBatchRename** log rule.

Table 11-63: Details about the DataBatchRename Data Definition

Data Definition Description	Logs data related to renaming a batch.
Additional Data Logged	• **Batch Name** • **Batch ID**

11.6.7 DataDefault Data Definition

The **DataDefault** data definition logs data from all logs except logs generating from the Intelligent Capture Server.

Table 11-64: Details about the DataDefault Data Definition

Data Definition Description	Logs data related to all logging except logs generating from the Intelligent Capture Server.
Additional Data Logged	All logging data except for logs generated from the Intelligent Capture Server.

11.6.8 DataNodeCreate Data Definition

The **DataNodeCreate** data definition logs data related to node creation. This data definition is used in the **ReportNodeCreate** log rule.

Table 11-65: Details about the DataNodeCreate Data Definition

Data Definition Description	Logs data related to node creation.
Additional Data Logged	• **Batch ID** • **Node Creation Date and Time** • **Node Level** • **Node ID** • **Node Ordinal** • **Server Name** • **Task Workstation** • **Task Module** • **Task User**

11.6.9 DataNodeDelete Data Definition

The **DataNodeCreate** data definition logs data related to node deletion. This data definition is used in the **ReportNodeDelete** log rule.

Table 11-66: Details about the DataNodeDelete Data Definition

Data Definition Description	Logs data related to node deletion.

Additional Data Logged	• **Batch ID** • **Node Deletion Date and Time** • **Node Level** • **Node ID** • **Node Ordinal** • **Server Name** • **Task Workstation** • **Task Module** • **Task User**

11.6.10 DataServerSecurityCategoryEvents Data Definition

The **DataServerSecurityCategoryEvents** data definition logs data from the Intelligent Capture Server belonging to the Security Category. This data definition is used in the **ReportNodeDelete** log rule.

Table 11-67: Details about the DataServerSecurityCategoryEvents Data Definition

Data Definition Description	Logs data from the Intelligent Capture Server belonging to the Security category.
Additional Data Logged	• **Batch ID** • **Batch Name** • **Log Date** • **Module Step** • **Node ID** • **Node Level** • **Process ID** • **Process Name** • **Sub Token 1** (insertion strings) • **Sub Token 2** (insertion strings) • **Workstation Name** • **Task Module** • **Task User**

11.6.11 DataServerValueEvents Data Definition

The **DataServerValueEvents** data definition logs data from the Intelligent Capture Server belonging to the Value Category.

Table 11-68: Details about the DataServerValueEvents Data Definition

Data Definition Description	Logs data from the Intelligent Capture Server belonging to the Value category.
Additional Data Logged	• **Batch ID** • **Batch Name** • **Log Date** • **Module Step** • **Node ID** • **Node Level** • **Process ID** • **Process Name** • **Sub Token 1** (insertion strings) • **Workstation Name** • **Task Module** • **Task User**

11.6.12 DataStageFileRead Data Definition

The **DataStageFileRead** data definition logs data from the Intelligent Capture Server belonging to the StageFile Category. Data is logged when a stage file is viewed or read. This data definition is used in the **ReportStageFileRead** log rule.

Table 11-69: Details about the DataStageFileRead Data Definition

Data Definition Description	Logs data from the Intelligent Capture Server belonging to the StageFile category
Additional Data Logged	• **Batch ID** • **Node Level** • **Node ID** • **Node Ordinal** • **Sent Date** • **Server Name** • **Stage File Number** • **Workstation Name** • **Task Module** • **Task User**

11.6.13 DataStageFileWrite Data Definition

The **DataStageFileWrite** data definition logs data from the Intelligent Capture Server belonging to the StageFile Category. Data is logged when a stage file is written or updated. This data definition is used in the **ReportStageFileWrite** log rule.

Table 11-70: Details about the DataStageFileWrite Data Definition

Data Definition Description	Logs data from the Intelligent Capture Server belonging to the StageFile category.
Additional Data Logged	• **Batch ID** • **Node Level** • **Node ID** • **Node Ordinal** • **Written Date** • **Server Name** • **Stage File Number** • **Workstation Name** • **Task Module** • **Task User**

11.6.14 DataTaskFinishCreatePage Data Definition

The **DataTaskFinishCreatePage** data definition logs data from the Intelligent Capture Server belonging to the Task Category. Data is logged when a task finishes creating a page. This data definition is used in the **ReportTaskFinishCreatePage** log rule.

Table 11-71: Details about the DataTaskFinishCreatePage Data Definition

Data Definition Description	Logs data from the Intelligent Capture Server belonging to the Task category for when a task finished creating a page.
Additional Data Logged	• **Batch ID** • **Node ID** • **Page Time** • **Source** • **Task Module** • **Task ID**

11.6.15 DataTaskFinishDonePage Data Definition

The **DataTaskFinishDonePage** data definition logs data from the Intelligent Capture Server belonging to the Task Category. Data is logged when processing of a page is completed. This data definition is used in the **ReportTaskFinishDonePage** log rule.

Table 11-72: Details about the DataTaskFinishDonePage Data Definition

Data Definition Description	Logs data from the Intelligent Capture Server belonging to the Task category for when task processing of a page is completed.
Additional Data Logged	• **Batch ID** • **Node ID**

11.6.16 DataTaskFinishIndexTask Data Definition

The **DataTaskFinishIndexTask** data definition logs data from the Intelligent Capture Server belonging to the Task Category. Data is logged when processing of an indexing task is completed. This data definition is used in the **ReportTaskFinishIndexTask** log rule.

Table 11-73: Details about the DataTaskFinishIndexTask Data Definition

Data Definition Description	Logs data from the Intelligent Capture Server belonging to the Task category for when indexing task processing is completed.
Additional Data Logged	• **Batch ID** • **Character Count** • **Document Count** • **Field Count** • **Key Time** • **Task Module** • **Task ID**

11.6.17 DataTaskFinishOcrTask Data Definition

The **DataTaskFinishOcrTask** data definition logs data from the Intelligent Capture Server belonging to the Task Category. Data is logged when processing of an *OCR* task on a page is completed. This data definition is used in the **ReportTaskFinishOcrPage** log rule.

Table 11-74: Details about the DataTaskFinishOcrTask Data Definition

Data Definition Description	Logs data from the Intelligent Capture Server belonging to the Task category for when *OCR* task on a page is completed.
Additional Data Logged	• **Character Count** • **Node ID** • **Rejected Count** • **Task Module** • **Task ID**

11.6.18 DataTaskFinishPage Data Definition

The **DataTaskFinishPage** data definition logs data from the Intelligent Capture Server belonging to the Task Category. Data is logged when processing of a page is completed, either successfully or with an error. This data definition is used in the **ReportTaskFinishPage** log rule.

Table 11-75: Details about the DataTaskFinishPage Data Definition

Data Definition Description	Logs data from the Intelligent Capture Server belonging to the Task category for when processing of a page (either with success or error) is completed.
Additional Data Logged	• **Node ID** • **Node Ordinal** • **Page Result** • **Page Time** • **Task Module** • **Task ID**

11.6.19 DataTaskFinishTask Data Definition

The **DataTaskFinishTask** data definition logs data from the Intelligent Capture Server belonging to the Task Category. Data is logged when a task finishes processing. This data definition is used in the **ReportTaskFinishTask** log rule.

Table 11-76: Details about the DataTaskFinishTask Data Definition

Data Definition Description	Logs data from the Intelligent Capture Server belonging to the Task category for when processing of a task is completed.
Additional Data Logged	• **Batch ID** • **Module Step** • **Page Count** • **Task Result** • **Return Value** • **Server Name** • **Task End Date** • **Workstation Name** • **Task Module** • **Task Start Date** • **Task Time on Server** • **Task Time Value** • **Task User** • **Task ID** • **Trigger ID** • **Trigger Level** • **Trigger Level Name** • **Trigger Ordinal**

11.7 System Sink Definitions for Client Modules and Components

Sink definitions determine where the data for the log rule is logged. Intelligent Capture includes several predefined system sink definitions. Data can be logged to the Intelligent Capture Database, the Windows Event Log, or a log file in the directory: `<<ApplicationData>>\EMC\InputAccel\` where *<<ApplicationData>>* a user-defined variable, depending on the location of the user's local `ApplicationData` folder.

Table 11-77: Details about predefined debug sinks

Sink Name	Description	Logged To
AdminLibDebugSink	Logs debug information for Intelligent Capture Administrator	Log file: `ACDebugLog.log`.
AuditToDBSink	Logs audit information to the Intelligent Capture Database	Logs to the `Tbl_AuditErrorLog` table in the Intelligent Capture Database.
CLTDebugSink	Logs debug information for the Intelligent Capture Client component	Log file: `CLTDebugLog.log`.
DebugSink	Logs all debug information	Log file: `DebugLog.log`.
DEMDebugSink	Logs debug information for Documentum Advanced Export client module	Log file: `DEMDebugLog.log`.
ErrorToDBSink	Logs all Error and warning logs	Logs to the `Tbl_AuditErrorLog` table in the Intelligent Capture Database.
GeneralEventLogSink	Logs audit information to the Windows Event Log	Logs to the Windows Event Log.
GeneralFileSink	Logs information to the file sink	Log file: `YYYYMMDD_InputAccel.log` where YYYYMMDD is the date of the log.
ICVDebugSink	Logs information for Image Converter client module	Log file: `ICVDebugLog.log`.
LOGDebugSink	Logs debug log information	Log file: `LOGDebugLog.log`
LOGEventLogSink	Logs audit logs to the Windows Event Log	Logs to the Windows Event Log.
NFSDebugSink	Logs information for the notification service.	Log file: `NFSDebugLog.log`
NUADebugSink	Logs information for NuanceOCR client module	Log file: `NUADebugLog.log`
RSCDebugSink	Logs information for RescanPlus client module	Log file: `RSCDebugLog.log`
SCNDebugSink	Logs information for ScanPlus client module	Log file: `SCNDebugLog.log`
SECDebugSink	Logs information from the Security Library	Log file: `SECDebugLog.log`
SinkBatchCreate	Sink for the **ReportBatchCreate** reporting log rule	Logs to the Intelligent Capture Database.

Sink Name	Description	Logged To
SinkBatchDelete	Sink for the **ReportBatchDelete** reporting log rule	Logs to the Intelligent Capture Database.
SinkBatchRename	Sink for the **ReportBatchRename** reporting log rule	Logs to the Intelligent Capture Database.
SinkNodeCreate	Sink for the **ReportNodeCreate** reporting log rule	Logs to the Intelligent Capture Database.
SinkNodeDelete	Sink for the **ReportNodeDelete** reporting log rule	Logs to the Intelligent Capture Database.
SinkStageFileRead	Sink for the **ReportStageFileRead** reporting log rule	Logs to the Intelligent Capture Database.
SinkStageFileWrite	Sink for the **ReportStageFileWrite** reporting log rule	Logs to the Intelligent Capture Database.
SinkTaskFinishCreatePage	Sink for the **ReportTaskFinishCreatePage** reporting log rule	Logs to the Intelligent Capture Database.
SinkTaskFinishDonePage	Sink for the **ReportTaskFinishDonePage** reporting log rule	Logs to the Intelligent Capture Database.
SinkTaskFinishIndexTask	Sink for the **ReportTaskFinishIndexTask** reporting log rule	Logs to the Intelligent Capture Database.
SinkTaskFinishOcrPage	Sink for the **ReportTaskFinishOcrPage** reporting log rule	Logs to the Intelligent Capture Database.
SinkTaskFinishPage	Sink for the **ReportTaskFinishPage** reporting log rule	Logs to the Intelligent Capture Database.
SinkTaskFinishTask	Sink for the **ReportTaskFinishTask** reporting log rule	Logs to the Intelligent Capture Database.
WSCDebugSink	Logs information forWeb Services Coordinator	Log file: `WSCDebugLog.log`
WSIDebugSink	Logs information for WS Input client module	Log file: `WSIDebugLog.log`
WSODebugSink	Logs information for WS Output client module	Log file: `WSODebugLog.log`

11.7.1 XML Schema for the Logging Sink Definitions

Users may specify their own sink definitions that specify where log data will be written. If users require sink definitions in addition to the sytstem sinks, then users can write both destination and formatting XML files that control where and how the log data is written. When a log rule is created, the sink XML is verified against the relevant sink schema.

This section provides the XML schema and the schema elements for the three supported sink destinations.

Related Topics

"Defining Log Rule Filter Definitions" on page 221

"Log Rule Settings and Add Log Rule" on page 323

"Log Rule Sink Definition" on page 329

"Specifying Log Rule Sink Definition" on page 228

"Understanding Log Rules" on page 215

11.7.1.1 EventSinkDestination XML

User created *<EventSinkDestination>*.xml files contain methods to write the log data to the *NT* Event Log. Users can create *XML* files to define the event sink for their environment. When a log rule is created, the XML is verified against the event sink schema, and must use the following format. When specifying LogName only Application is supported at this time. Applications may not write entries to the Security or System log.

Table 11-78: EventSinkDefinition XML Schema

Schema Elements	Description
<EventSinkDestination>.xml	
<?xml version="1.0" encoding="utf-8" ?> <!--Sample XML for the Athena Event Sink destination --> <EventSinkDestination xmlns="http://www.emc.com/InputAccel/Logging"> <MachineName>*<localhost>*</MachineName> <LogName>Application</LogName> <Source>*<GEN>*</Source> </EventSinkDestination>	
MachineName	Optional. The name of the computer on which the event source is registered. A null or empty value will default to "localhost". Any other name will be interpreted as a valid *NT* machine name.

Schema Elements	Description
`LogName`	The name of the event log to which the source writes entries. The value "Application" will write subsequent entries to the appropriate system log. This parameter is required. Only "Application" is supported at this time. Applications may not write entries to the Security or System log.
`Source`	The source name of the event source. This source must exist as an event source for the specified LogName in the registry of the MachineName machine. This name may be specified by using the 3-character acronym of the Intelligent Capture component doing the logging or may be actual source name to be used.

Related Topics

"Defining Log Rule Filter Definitions" on page 221

"DbSinkFormat XML" on page 428

"FileSinkDestination XML" on page 429

"FileSinkFormat XML" on page 425

"Specifying Log Rule Sink Definition" on page 228

"Understanding Log Rules" on page 215

"XML Schema for the Logging Sink Definitions" on page 424

11.7.1.2 FileSinkFormat XML

User created *<FileSinkFormat>*`.xml` files contain information controlling how information is presented in the output file. When the log rule is created the xml entered by the user is verified against the Intelligent Capture `FileSinkFormat` schema, so it must follow this format.

Table 11-79: FileSinkFormat XML Schema

Schema Elements	Description
<FileSinkFormat>`.xml`	

Schema Elements	Description
<?xml version="1.0" encoding="utf-8" ?> <!--Sample XML for the InputAccel File Sink Format--> <FileSinkFormat xmlns="http://www.emc.com/InputAccel/Logging"> <Header> <Content><*Text*></Content> </Header> <Line> <Content><*{0} - {1}*></Content> <SubParam><*Log.LogDateTime*></SubParam> <SubParam><*Log.LogMessage*></SubParam> </Line> <Line INDENT="<*4*>"> <Content><*{0}*></Content> <SubParam><*Log.LogStack*></SubParam> </Line> </FileSinkFormat>	
`Header`	For specifying header information that will appear as the first lines of the file. `Header` lines are written once only and must be defined in the SinkDefinition for the log that writes the first log to the file. This setting is ignored for subsequent writes.
`Line`	Each log request will write at least one line to the output file. The `Line` element allows the user to optionally add additional information from the log data into the log. Each `Line` element consists of one `Content` element and zero or more `SubParam` elements for the insertions. Use the `INDENT` attribute to indent the line.
`Content`	`Content` elements (in either the `Header` or `Line` elements) define a constant string to be written. Data can be inserted into the string using the SubParam elements and an insertion specification {n}. The Content strings will be checked for localization according to the locale of the machine on which `Emc.InputAccel.Logging.Sinks.File.dll` is running.

Schema Elements	Description
`SubParam`	`SubParam` elements define the data to be inserted into the preceding `Content` element string. • These strings may contain constants or may specify some data that will be passed with the log. • The text in the strings will not be localized. • If a reference to a log field is made, the field will be converted into a string. • Dates and numbers will be represented according to the regional settings of the local machine. • If the insertion string is *`Log.LogStack`*, the line will be repeated for each log in the log stack. The log stack data will be presented as a comma separated list of data. The data reported will be: "LogDateTime, LogType, LogCode, Message". **Note:** `SubParam` entries logged to the File Sink that are longer than 511 bytes may be truncated. Truncated entries end with "…".

Related Topics

"Defining Log Rule Filter Definitions" on page 221

"DbSinkFormat XML" on page 428

"EventSinkDestination XML" on page 424

"FileSinkDestination XML" on page 429

"Specifying Log Rule Sink Definition" on page 228

"Understanding Log Rules" on page 215

"XML Schema for the Logging Sink Definitions" on page 424

11.7.1.3 DbSinkFormat XML

User created *<DbSinkFormat>*.xml files contain information controlling the filename, location and basic structure of the output log file. When the log rule is created, the *XML* entered by the user is verified against the DbSinkDestination.xsd schema so it must follow this format.

Table 11-80: DbSinkFormat XML Schema

Schema Elements	Description
<DbSinkFormat>.xml	
<?xml version="1.0" encoding="utf-8" ?> <!--Sample XML for the InputAccel Db Sink format--> <DbSinkFormat xmlns="http://www.emc.com/InputAccel/Logging" TYPE="DB"> <Command>*<spLogBatchCreate>*</Command> <Parameters> <ParamName>*<serverId>*</ParamName> <ParamValue>*<LOG.ServerId>*</ParamValue> <ParamName>*<serverName>*</ParamName> <ParamValue>*<LOG.ServerName>*</ParamValue> <ParamName>*<batchName>*</ParamName> <ParamValue>*<LOG.BatchName>*</ParamValue> <ParamName>*<batchUuid>*</ParamName> <ParamValue>*<LOG.BatchUUID>*</ParamValue> <ParamName>*<createTime>*</ParamName> <ParamDate>*<LOG.CreateTime>*</ParamDate> <ParamName>*<Process>*</ParamName> <ParamValue>*<LOG.Process>*</ParamValue> <ParamName>*<moduleExe>*</ParamName> <ParamValue>*<LOG.ModuleExe>*</ParamValue> <ParamName>*<operator>*</ParamName> <ParamValue>*<LOG.Operator>*</ParamValue> </Parameters> </DbSinkFormat>	
Command	Specifies the name of a stored procedure to be called to log the data.
ParamName	The name of one of the parameters to the stored procedure named in the Command element. The value of the parameter named in ParamName can be a string, a number or a date.

Schema Elements	Description
`ParamValue`	Contains the value to be passed for the parameter named in the `ParamName` element preceding it. It can contain an optional type attribute that defines the type of value to expect. • `String`: A String object. This is the default if no type attribute is found. • `Date`: A .NET DateTime object or a string that can represent a date. If it is a string, it will be converted to a DateTime object before passing it to the command. • `Datebinary`: A 64-bit integer that represents a date. This data will be converted to a .NET DateTime object before passing it to the command. • `Number`: An integer object or a string that represents an integer object. If it is a string, it will be converted to an Int32 object before passing it to the command.

Related Topics

"Defining Log Rule Filter Definitions" on page 221

"EventSinkDestination XML" on page 424

"FileSinkDestination XML" on page 429

"FileSinkFormat XML" on page 425

"Specifying Log Rule Sink Definition" on page 228

"Understanding Log Rules" on page 215

"XML Schema for the Logging Sink Definitions" on page 424

11.7.1.4 FileSinkDestination XML

User created *<FileSinkDestination>*`.xml` files contain information controlling the filename, location and basic structure of the output log file. When the log rule is created the *XML* entered by the user, it is verified against the `FileSinkDestination.xsd` schema so it must follow this format.

Table 11-81: FileSinkDestination XML Schema

Schema elements	Description
<FileSinkDestination>.xml	
<xml version="1.0" encoding="utf-8" ?> <!--Sample XML for the InputAccel File Sink Destination format--> <FileSinkDestination xmlns="http://www.emc.com/InputAccel/Logging"> <Path CREATEPATH="*<true>*" OVERWRITE="0">*<$CommonApplicationData$|EMC|InputAccel|>*</Path> <FileName>*<@d_InputAccel>*</FileName> <Structure MAXSIZE="*<0>*" SKIPHEADER="*<yes>*"></Structure> </FileSinkDestination>	
Path	The path for the file to be written. Path names within $$ are translated to local system settings and acceptable folder names are defined by .NET Environment. SpecialFolder . Can contain two optional attributes: • CREATEPATH - Determines the path will be created if it does not exist. Valid settings are “true” and “false” or “1” and “0”. The default is “false” or “0.” • OVERWRITE - If the file already exists, overwrite it. Valid settings are “1” and “0”. If the file exists and OVERWRITE=“0” or does not exist, an indexer will be appended to the filename. For example, if “FileName.log”, “FileName1.log” and “FileName2.log” exist, the new file will be named “FileName3.log”.
FileName	The name of the file to be written, without the “.log” extension. The following substitution characters can be embedded in the string. When the file is created they will be replaced with the appropriate strings: • @d: Substitutes the current in a sortable format. Example: “@dLogs” when written by the FileSink on 1/20/2007 becomes “20070120Logs.log” • @t: Substitutes the current time in a sortable format. For example, @d_@tLogs written by the FileSink on 1/20/2007 at 3:15 *PM* becomes “20070120_1515Logs.log”. This is the time the file was first opened, not the time the first log was written.

Schema elements	Description
<FileSinkDestination>.xml	
Structure	Describes elements of the file. • MAXSIZE – the maximum size in bytes. 0 is unlimited. **Note:** If the size of the log file exceeds the size indicated in MAXSIZE, then the log file is wrapped, where the first entries are overwritten with the latest entries. • SKIPHEADER – when wrapping back to the beginning of the file, does not overwrite the header information.

Related Topics

"Defining Log Rule Filter Definitions" on page 221

"DbSinkFormat XML" on page 428

"FileSinkFormat XML" on page 425

"Specifying Log Rule Sink Definition" on page 228

"Understanding Log Rules" on page 215

"XML Schema for the Logging Sink Definitions" on page 424

11.8 Report Details

Intelligent Capture installs predefined reports to perform common tasks. The reports use report definitions to specify the stored procedures that collect data from the Intelligent Capture Database and *XML* and *RPT* files that design the reports. You can also create custom reports based on these report definitions and stored procedures. The following topics list the log rules that need to be enabled before generating each predefined report and list the predefined reports and their associated parameters and stored procedures.

Note: The batch creation dates displayed in reports are in UTC, however records selected for batch reports are filtered on dates in terms of local database time. In some cases this can lead to discrepancies between the expected results and the actual reported results. Reports include data for complete days, extending from the configured beginning date to ending date, but the difference between the displayed creation date in UTC, and the corresponding creation date in local database time can extend from one day to another. Users configuring the beginning and ending dates for a report might expect the reported results to correspond exactly with the batch creation dates

displayed in Intelligent Capture Administrator, but that will not always be the case. The specific records actually selected by a report query will depend on various factors, such as the time zone in which the database is located with respect to UTC, and the time of the day a particular batch may have been created.

11.8.1 Predefined Report Details

Intelligent Capture installs the following predefined reports for performing common tasks.

11.8.1.1 Batch Reconciliation Reports

Batch Reconciliation Reports can be considered a summary version of the File Audit Trail Detail Report. It shows the number of pages created, deleted and done over a period of time. This report can be viewed at a variety of summary levels, Daily, Weekly, Monthly and the granularity of the detail rows vary accordingly. For example, a Batch Reconciliation Report shows each batch processed on a given day for each process, the number of pages created, and deleted. The number of pages done plus the number of pages deleted should equal the number of pages created. If it does not, the batch is marked with an asterisk. If the user chooses to filter the report to "Uncompleted Batches in Process", only the batches marked with an asterisk will appear on the report.

Note: Pages complete a process when they route to the IADone module. IADone must be included in the *IPP* for the pages to be considered done.

Log rules to be enabled for Batch Reconciliation Detail Report

- ReportBatchCreate
- ReportBatchRename
- ReportNodeCreate
- ReportNodeDelete
- ReportTaskFinishDonePage

Log rules to be enabled for Batch Reconciliation Summary Report

- ReportBatchCreate
- ReportNodeCreate
- ReportNodeDelete
- ReportTaskFinishDonePage

Parameters to be selected for this report:

Table 11-82: Parameters in the Batch Reconciliation Reports

Parameter	Description
Date range for report period	The date range is inclusive.
Processes	Processes to be included in the report.
Servers	Servers to be included in the report. These are the servers that created the batches.
Report Organization	Select the report organization. The report can be organized by date and then process, or by process first and then the date.
Batch Filter	Select to indicate the type of batches to include in the report.
Sort Column	Select the column to be used to sort the detail rows. The detail rows can be sorted by the processing time or the batch name.
Sort Order	Select the sort order of the detail rows. The report can display the detail rows in ascending or descending order.
Summary Level – (Summary report only)	Select the option to indicate how the data must be summarized. The report can display data summarized by the day, week, or month. The Processing Date column on the Summary report changes accordingly

For each page level node created or deleted by a module or done (IADone module only) by a module, the data to log is:

- Server ID
- Server Name
- Batch name
- Batch ID
- Node ID
- Node Action – Created or Deleted
- Done – True or False

Columns for the report are:

Table 11-83: Columns in the Batch Reconciliation Reports

Column	Description
Batch name	Name of the batch.

Column	Description
Not done	Uncompleted batches are marked with "*". A batch is completed when all page nodes have the Done status set.
Pages created	Total number of pages created for the batch.
Pages deleted	Total number of pages deleted during batch processing.
Pages to IADone	Total number of pages that have completed the workflow.
Time for Batch(s)	Time in seconds from the batch creation until the last page node was marked as Done. Batches that have not completed do not show this value. Note that the Total rows for this value are the average times, not the total times.
Time for Batch (m)	Time in minutes from the batch creation until the last page node was marked as Done. Batches that have not completed do not show this value. Note that the Total rows for this value are the average times, not the total times.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.1.2 Deleted Batches Reports

Deleted Batches Reports show information about each batch that has been deleted. The data can be organized by batch creation date or by batch deletion date.

Log rules to be enabled for Deleted Batches Report

- ReportBatchCreate
- ReportBatchDelete
- ReportBatchRename

Parameters to be selected for this report:

Table 11-84: Parameters in the Deleted Batches Reports

Parameter	Description
Date range for report period	The date range is inclusive.
Servers	Servers to be included in the report.
Module Name Format	Use official module name or use module executable name.
Report Organization	Select the report organization. The report can be organized by the creation or deletion date of the batch.
Sort Order	Select the sort order of the detail rows. The report can display the detail rows in ascending or descending order.

For each deleted batch, the data to log is:

- Server ID
- Server Name
- Batch name
- Batch Creation Date
- Module Executable Name
- Operator Name
- Batch Deletion Date and Time

The columns for the report are:

Table 11-85: Columns in the Deleted Batches Reports

Column	Description
Servers	The name of the server.
Creation date (or Deletion Date)	The date the batch was created/deleted.
Batch name	The name of the batch.
Deleted by	The name of the operator that deleted the batch.
Module	Module that performed the deletion
Deletion Time	The time the batch was deleted.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.1.3 Dispatcher Auto Classification Rate Report and Associated Files

The Dispatcher Auto Classification Rate report provides the following information and uses the described associated files:

- The bar graph shows the percentage rate of pages that have been successfully processed per template by the Dispatcher Classification module for all the batches defined for the report. Results are displayed in order by either classification rate or template code.
- The table has the following columns:
  - **Template ID**: Unique template identification number (defined by the user).
  - **Template Name**: Template name (defined by the user).
  - **Template Code**: Unique template code (defined by the user).
  - **Template Type**: Type of Dispatcher template.
  - **Number of pages**: Total number of pages classified by the template.
  - **Classification Rate**: Percentage of pages per template classified automatically by the Dispatcher Classification module.

The results can be sorted by:

- Classification Rate
- Template Code

Table 11-86: Automatic Classification Rate Report Associated Files

Associated file type setting	Associated file name	Description
Associated Stored Procedure	`up_RunDispatcherAutoClassificationRateReport`	*SQL* file that specifies the data to be collected.
XML Parameter	`DispatcherAutoClassificationRate.xml`	Specifies the parameters that determine the reports data to extract from the database.
Crystal Reports Project	`DispatcherAutoClassificationRate.rpt`	Specifies the parameters that determine the reports data to be displayed.
Sample Report Image	`DispatcherAutoClassificationRateReport.bmp`	Example sample report graph that shows what the generated report should look like.

11.8.1.4 File Audit Trail Detail Reports

File Audit Trail Detail Reports provide an audit of every page entered into the Intelligent Capture System and the disposition of that page. For example, a File Audit Trail Detail Report may show information about each page that was created in an Intelligent Capture process during the selected time period, who viewed it, which modules acted on it, and whether it completed the process. This report is intended to track each page through the process. It is expected that users would run the report often, perhaps daily, and archive the results for later use.

Task processing and actions on the page are tracked independently. For example, if a page was deleted by a module that was processing a task, the task information and whether it was completed successfully or unsuccessfully is shown on one row and the deletion is shown on another.

Log rules to be enabled for File Audit Trail Detail Report

- ReportBatchCreate
- ReportBatchRename
- ReportNodeCreate
- ReportNodeDelete
- ReportStageFileRead
- ReportStageFileWrite
- ReportTaskFinishCreatePage
- ReportTaskFinishPage
- ReportTaskFinishTask
- ReportTaskFinishDonePage

Parameters to be selected for this report:

Table 11-87: Parameters in the File Audit Trail Detail Reports

Parameter	Description
Date range for report period	The date range is inclusive.
Processes	Processes to be included in the report.
Servers	Servers to be included in the report.
User	The name of the user. This is applicable if the **Show** parameter is **Pages that have been viewed by a specific user**.
Show	Select from the available options to limit the information displayed in the report.
Module Name Format	Use official module name or use module executable name.

For each page level node returned from a module (or whose parent is sent to a module), the data to log is:

- Server ID
- Server Name
- Workflow Name
- Batch name
- Module executable name
- Node ID
- Task start time
- Task end time
- Operator Name (or ID)
- Return Result: Success or Error
- Node Action: Created, Deleted, Replaced or Changed
- Source: if created
- IADone: True or False. True if the node was routed to IADone in the *IPP*

The columns for the report are:

Table 11-88: Columns in the File Audit Trail Detail Reports

Column	Description
Batch Creation Date	Date when batch was created. This does not necessarily equate to the date the first page was scanned.
Process Name	The name of the workflow.
Batch Name	The name of the batch.
Page Node ID	The actual page node is shown on this report because it is the one constant when referring to a page. The order of the pages can change as the page moves through the workflow.
Page Number within the batch	This shows the page number of the page when it was created. Since the order of the pages can change as the page moves through the workflow, it may not be the page number of the page when the batch is done. Note that it is possible for the report to show the same page number for multiple nodes.

Column	Description
Source of the page node	If the page was imported this is the location from which it was imported. If the page was scanned, this is a string returned by the scanning module. Other modules that create nodes will return different values for the source that make sense to those modules.
Module name	Name of the module that accessed the page or the parent of the page.
Operator	If the site is de-identifying operator names for legal purposes, the de-identified names will appear for all attended modules.
Start date	Date & Time the module received the task containing the page.
End date	Date & Time the module returned the task containing the page. For events not associated with a task, this field is blank.
Success	X indicates the task returned successfully.
Error	X indicates the task returned with an error.
Create	X indicates the module created the page.
Delete	X indicates the module deleted the page.
Change	X indicates the module overwrote the original image.
View	X indicates that the module allowed the user to view the image only. If the module is an attended module and the image was a part of the task processed, it is assumed that the operator viewed the image.
To IADone	X indicates that after returning successfully from the module it has completed the workflow. This is controlled by the *IPP* routing the node to the IADone module.

Note: In order for this report to be produced, the page detail data for the time period must be present on the database.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.1.5 Page Level OCR Processing Reports

Page Level *OCR* Processing Reports show information about the performance of each *OCR* module. The information can be viewed in either a detail or a summary report. The report parameters and data to be logged are the same for both reports. For example, an *OCR* Processing Report might show each page processed by the *OCR* module over a selected time period and the processing statistics for the page.

Note: Average for the **% Recognized** is not a weighted average based on character counts, but is calculated as the sum of the **% Recognized** values divided by the number of pages.

Log rules to be enabled for Page Level OCR Processing Detail Report

- ReportBatchCreate
- ReportBatchRename
- ReportTaskFinishOcrPage
- ReportTaskFinishPage
- ReportTaskFinishTask

Log rules to be enabled for Page Level OCR Processing Summary Report

- ReportBatchCreate
- ReportTaskFinishOCRPage
- ReportTaskFinishPage
- ReportTaskFinishTask

Parameters to be selected for this report:

Table 11-89: Parameters in the Page Level OCR Processing Reports

Parameter	Description
Date range for report period	The date range is inclusive.
Processes	Processes to be included in the report.
Servers	Servers to be included in the report.
Modules	Modules to be included in the report. The report can display one or more specific modules or can display all modules.
Report Organization	Select the report organization. The report can be organized by process and then date, or by date first and then the process.
Module Name Format	Select the module name to display. The report can display the official module name or the module executable name.

Parameter	Description
Sort Column	Select the column to be used to sort the detail rows. The detail rows can be sorted by the percentage of characters recognized or the page number.
Sort Order	Select the sort order of the detail rows. The report can display the detail rows in ascending or descending order.
Summary Level – Summary report only	Select the option to indicate how the data must be summarized. The report can display data summarized by the day, week, or month. The Processing Date column on the Summary report changes accordingly.

For each page sent to an *OCR* module, the data to log is:

- Server ID
- Server Name
- Batch name
- Module executable name
- Trigger node id
- Trigger node name
- Page Node ID
- Page Node Name
- Task start time
- Task end time
- Recognition Time for page
- # Recognized Characters
- # Rejected Characters
- Total time in milliseconds
- Page count

The columns for this report are:

Table 11-90: Columns in the Page Level OCR Processing Reports

Column	Description
Date	The date the page was processed.
Module	Official module name or module executable name.

Column	Description
Task	The task is identified by its batch name and the name of trigger node.
Page node	Name of the page recognized (this may be the same as the task).
Total characters	Characters found on the page.
Recognized characters	Calculated as (Characters on page – Characters Rejected).
Rejected characters	Rejected characters in a page.
Time	Recognition time in milliseconds.
% Recognized	Percentage of characters recognized successfully. Calculated as (100 – ((Characters Rejected column * 100)/ Characters on page column)).

Note: Averages shown on the group footings are calculated by adding the individual values in the detail and dividing by the number of pages.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.1.6 Scan Reports

Scan Reports show information about the performance of the scan workstations and operators. For example, a Scan report shows each batch scanned or rescanned over the selected time period. The information is organized by either the operator name (or ID) or the scan workstation name and then by scan date or by scan date and then by either the operator name (or ID) or the scan workstation name. It may also be organized by "Date Only" when the display of the workstation name would reveal the identity of the scan operator.

Log rules to be enabled for Scan Detail Report

- ReportBatchCreate
- ReportBatchRename
- ReportNodeCreate
- ReportTaskFinishCreatePage
- ReportTaskFinishTask

Log rules to be enabled for Scan Summary Report

- ReportBatchCreate
- ReportNodeCreate
- ReportTaskFinishTask

Parameters to be selected for this report:

Table 11-91: Parameters in the Scan Reports

Parameter	Description
Date range for report period	The date range is inclusive.
Workstations	Workstations to be included in the report.
Servers	Servers to be included in the report.
Operators	Operators to be included in the report.
Show	Select the data to display in the report. The report can display the workstation and date information, operator and date information, or only the date information.
Report Organization	Select the report organization. The report can be organized by date first (and then by workstation/operator) or by workstation/ operator first (and then by date). This is not applicable if the **Show** parameter is **Date data only**.
Sort Order	Select the sort order of the detail rows. The report can display the detail rows in ascending or descending order.
Summary Level – (Summary report only)	Select the option to indicate how the data must be summarized. The report can display data summarized by the day, week, or month. The Processing Date column on the Summary report changes accordingly.

For each page scanned by a scan module, the data to log is:

- Server ID
- Server Name
- Batch name
- Module executable name
- Scan Date & Time
- Scan Machine Name
- Scan Operator Name (or unique ID)

- Node ID of page
- Scanning Time in milliseconds
- Scan Driver Name
- Node ID of node flagged to be rescanned (if rescanning)

The columns for this report are:

Table 11-92: Columns in the Scan Reports

Column	Description
Batch Name	Name of the batch.
Scan Machine Name or Operator Name (or ID)	Missing if the **Show** parameter is **Date data only**.
Scan Date	Date page was originally scanned.
Batch count	Number of batches.
Pages scanned	Total number of pages scanned in the batch with that driver.
Pages rescanned	Count of pages that were replaced by a RescanPlus module.
Time (m)	Total time the batch was open, in milliseconds.
% Rescanned	Percentage of pages that required rescanning. Calculated as ((Pages Rescanned/ Pages Scanned) * 100).
Pages per hour	Average number of pages scanned per hour. Calculated as (3600000 / (Total Time in milliseconds / Pages Scanned)).

Note: Values in the group footings are calculated by summing the values in the detail rows and, if percent or averages, dividing by the number of pages. In order for this report to be produced, the page detail data for the time period must be present in the database.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.1.7 Unattended Module Reports

Unattended Module Reports show information about the performance of each unattended Intelligent Capture module. The information can be viewed in either a detail or a summary report. For example, an Unattended Module Report shows each task processed by the module over a selected time period, how many pages were processed and the average time per page. This information may be further broken down by workstation so if the same module is running on multiple workstations, the workstation performance can be compared.

Log rules to be enabled for Unattended Module Detail Report

- ReportBatchCreate
- ReportBatchRename
- ReportTaskFinishTask

Log rules to be enabled for Unattended Module Summary Report

- ReportBatchCreate
- ReportTaskFinishTask

Parameters to be selected for this report:

Table 11-93: Parameters in the Unattended Module Reports

Parameter	Description
Date range for report period	The date range for the report.
Processes	Processes to be included in the report.
Servers	Servers to be included in the report.
Modules	Modules to be included in the report. The report can display one or more specific modules or can display all modules.
Report Organization	Select the report organization. The report can display each process separately or can combine all process information.
Module Name Format	Select the module name to display. The report can display the official module name or the module executable name.
Sort Column	Select the column to be used to sort the detail rows. The detail rows within a group can be sorted by the time or date.
Sort Order	Select the sort order of the detail rows. The report can display the detail rows in ascending or descending order.

Parameter	Description
Summary Level – (Summary report only)	Select the option to indicate how the data must be summarized. The report can display data summarized by the day, week, or month. The Processing Date column on the Summary report changes accordingly

For each task sent to a module, the data that gets logged includes:

- Server ID
- Server Name
- Batch name
- Module executable name
- Trigger node ID
- Trigger node name
- Task start time
- Task end time
- Total time in milliseconds
- Page count

The columns for this report are:

Table 11-94: Parameters in the Unattended Module Reports

Column	Description
Batch node	Displays the module name, host name of the machine running the module, and tasks. Tasks are identified by the batch name and the name of the trigger node.
Processing date	The date on which the task was run. If the task is run multiple times on the same day, the data reflects the totals for all of the tasks.
Page count	Total page count for the task run on the day.
Time (m)	Total processing time for the task. Time is reported in milliseconds.
Average Time per Page	Average processing time for the task per page. This is calculated as Time column / Pages column.

Note: In order for this report to be produced, the task detail data for the time period must be present on the database.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.1.8 Operator Productivity Report

Operator Productivity Report displays operator productivity and uses the Doc Type table.

Parameters to be selected for this report:

Table 11-95: Parameters in the Operator Productivity Report

Parameter	Description
Date range for report period	The date range is inclusive.
Processes	Processes to be included in the report.

Columns for the report are:

Table 11-96: Columns in the Operator Productivity Report

Column	Description
Operator	The Windows account name of the operator running Intelligent Capture Completion.
Keystroke count	Total number of keystrokes entered in any field of this doc type; only includes those stored as part of the field's value and not hotkeys, delete, or backspace.
Keystrokes/hr	The keystrokes per hour. This is calculated as: sum(Key stoke count)/sum(The total processing time in seconds).

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.1.9 Page Extraction Report

This report displays the throughput and accuracy at the page level (using the Template Reports table).

Parameters to be selected for this report:

Table 11-97: Parameters in the Page Extraction Report

Parameter	Description
Date range for report period	The date range is inclusive.
Processes	Processes to be included in the report.

Columns for the report are:

Table 11-98: Columns in the Page Extraction Report

Column	Description
DPP Name	The recognition project used for extraction.
Template Code	The template code used.
Pages Extracted/hr	The pages extracted per hour. This is calculated as: sum(Number of pages processed by the Extraction module)/sum(The total processing time in seconds by the Extraction module).
% Pages with no bad fields	The percentage of pages with no bad fields. This is calculated as: sum(PagesRecognizedOk)/ sum(PagesProcessedByRecognition).

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.1.10 Field Extraction Report

Field Extraction Report displays the accuracy (as determined by fields unchanged by the operator) at the field level (using the Field table)

Parameters to be selected for this report:

Table 11-99: Parameters in the Field Extraction Report

Parameter	Description
Date range for report period	The date range is inclusive.
Processes	Processes to be included in the report.

Columns for the report are:

Table 11-100: Columns in the Field Extraction Report

Column	Description
Doc type	The Doc Type used for field extraction.
Field	The template code used.
% unchanged fields	(sum(Processed) – sum(Changed))/ sum(Processed)

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.2 Predefined Reports Stored Procedures

When the Intelligent Capture Administrator opens a report, it executes a stored procedure to retrieve the data for the report from the Intelligent Capture Database the report. Then it calls Crystal Reports with the data retrieved by the stored procedure. Stored procedures consist of:

- Input parameter: Refines the information retrieved from the Intelligent Capture Database by using the data you type in the user interface for the report in Intelligent Capture Administrator. For example, you can specify the start and end dates for the report which reduces the amount of information retrieved from the database.
- Output dataset: Retrieves data from the Intelligent Capture Database. The dataset is the data organized into rows and columns of data.

The following topics list the input parameters and output datasets used in the predefined stored procedures (located in `C:\Program Files\InputAccel\Databases\DBScripts\ReportsDB\Procedures` by default). When you create a custom report, use these parameters to obtain the information you need. In addition, each topic lists the *XML* file which describes the input parameters and designs the user interface of the **Parameter** area for each predefined report in Intelligent Capture Administrator and the Crystal Reports report.

11.8.2.1 up_RunBatchReconciliationDetailReport

The Batch Reconciliation Detail Report shows the number of pages created, deleted and done over a period of time. This report requires that the following log rules are enabled when processing batches: ReportBatchCreate, ReportBatchRename, ReportNodeCreate, ReportNodeDelete, ReportTaskFinishDonePage.

- Name of the report: Batch Reconciliation Detail Report.
- *XML* parameter file: `BatchReconciliationDetailParams.xml`
- Crystal Reports Project file: `BatchReconciliationDetail.rpt`

The parameters are:

Table 11-101: Input Parameters in the up_RunBatchReconciliationDetailReport Stored Procedure

Input Parameter	Description
FromDate	Beginning date for report or Null.
ToDate	Ending date for report or Null.
Processes	Comma separated list of processes or Null.
Servers	Comma separated list of servers or Null.
OrganizeBy	• 0 = Combine workflows • 1 = Separate workflows
Filter	• 0 = Use All Batches • 1 = Incomplete Batches
SortDetailColumn	• 0 = Batch name • 1 = Time/Page
SortOrder	• 0 = Ascending • 1 = Descending
Locale	Locale name for report. The default is “CurrentLocale”.

Table 11-102: Output Dataset in the up_RunBatchReconciliationDetailReport Stored Procedure

Output Dataset	Description
RPName	Name of process.
RBBatchName	Name of batch.
RBCreateDttm	Create date of batch.
TotalPages	Number of pages created for batch.
DeletedPages	Number of pages deleted.
DonePages	Number of pages routed to **IADone**.
ProcessingSeconds	Number of seconds for processing all tasks or 0 if batch not finished.

Related Topics

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.2.2 up_RunBatchReconciliationSummaryReport

The Batch Reconciliation Summary Report shows the number of pages created, deleted and done over a period of time. This report requires that the following log rules are enabled when processing batches: ReportBatchCreate, ReportNodeCreate, ReportNodeDelete, and ReportTaskFinishDonePage.

- Name of the report: Batch Reconciliation Summary Report.
- *XML* parameter file: `BatchReconciliationSummaryParams.xml`
- Crystal Reports Project file: `BatchReconciliationSummary.rpt`

The parameters are:

Table 11-103: Input Parameters in the up_RunBatchReconciliationSummaryReport Stored Procedure

Input Parameter	Description
FromDate	Beginning date for report or Null.
ToDate	Ending date for report or Null.
Processes	Comma separated list of processes or Null.
Servers	Comma separated list of servers or Null.
OrganizeBy	• 0 = Combine workflows • 1 = Separate workflows

Input Parameter	Description
Filter	• 0 = Use All Batches • 1 = Incomplete Batches
SortOrder	• 0 = Ascending • 1 = Descending
SummaryLevel	• 0 = Daily • 1 = Weekly • 2 = Monthly
Locale	Locale name for report. The default is "CurrentLocale".

Table 11-104: Output Dataset in the up_ RunBatchReconciliationSummaryReport Stored Procedure

Output Dataset	Description
RPName	Process name.
ThisYear	Year batches were created.
ThisMonth	Month or Week batches were created (depending on SummaryLevel).
ThisDay	Day batches were created or 0 if not daily report.
CreatedPages	Page count for all batches created on date.
DeletedPages	Number of pages deleted.
DonePages	Number of pages routed to **IADone**.
TotalBatchProcessingTime	Total seconds to process all batches that were completed.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.2.3 up_RunDeletedBatchesReport

The Deleted Batches Report shows information about each batch that has been deleted. This report requires that the following log rules are enabled when processing batches: ReportBatchCreate, ReportBatchDelete, ReportBatchRename.

- Name of the report: Deleted Batches Report.
- *XML* parameter file: `DeletedBatchesParams.xml`
- Crystal Reports Project file: `DeletedBatchesReport.rpt` Export File

The parameters are:

Table 11-105: Input Parameters in the up_RunDeletedBatchesReport Stored Procedure

Input Parameter	Description
FromDate	Beginning date for report or Null.
ToDate	Ending date for report or Null.
Servers	Comma separated list of servers or Null.
ModuleDisplay	• 0 = Use Official name • 1 = Executable name
Organization	• 0 = CreationDate • 1 = DeletionDate
SortOrder	• 0 = Ascending • 1 = Descending
Locale	Locale name for report. The default is "CurrentLocale".

Table 11-106: Output Dataset in the up_RunDeletedBatchesReport Stored Procedure

Output Dataset	Description
RBBatchName	Name of batch.
RBCreateServer	Server where batch was created.
CreateDate	Create date of batch.
DeleteDate	Date batch was created.
RBDeleteDttm	Date and time batch was deleted.
RBDeleteExe	Executable name of module that deleted the batch.
RBDeleteOperator	User logged into module that deleted the batch.

Output Dataset	Description
MDModuleName	Official name of module that deleted the batch.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.2.4 up_RunFileAuditTrailDetailReport

The File Audit Trail Detail Report shows information about each page created in an Intelligent Capture process during the selected time period, who viewed it, which modules acted on it, and whether it completed the process. This report requires that the following log rules are enabled when processing batches: ReportBatchCreate, ReportBatchRename, ReportNodeCreate, ReportNodeDelete, ReportStageFileRead, ReportStageFileWrite, ReportTaskFinishCreatePage, ReportTaskFinishPage, ReportTaskFinishTask, and ReportTaskFinishDonePage.

- Name of the report: File Audit Trail Detail Report.
- *XML* parameter file: `FileAuditTrailDetailParams.xml`
- Crystal Reports Project file: `FileAuditTrailDetail.rpt`

The parameters are:

Table 11-107: Input Parameters in the up_RunFileAuditTrailDetailReport Stored Procedure

Input Parameter	Description
FromDate	Beginning date for report or Null
ToDate	Ending date for report or Null
Processes	Comma separated list of processes or Null
Servers	Comma separated list of servers or Null
Operator	Name of operator or NULL

Input Parameter	Description
Filter	• 0 = Use No Filter • 1 = Viewed Batches • 2 = Batches Viewed by a specific user • 3 = Batches with errors • 4 = Batches with deleted pages • 5 = Batches with changed pages
ModuleDisplay	• 0 = Use Official name • 1 = Executable name
Locale	Locale name for report. The default is "CurrentLocale".

Table 11-108: Output Dataset in the up_RunFileAuditTrailDetailReport Stored Procedure

Output Dataset	Description
CreateDate	Date page was created.
RPName	Process name for batch.
RBBatchName	Name of batch.
RTStep	Step name within process if action is a task.
NodeId	Node id for the page.
NodeOrdinal	Ordinal for node at the time the action occurred.
RTSource	Source from which the page was created.
RTOperator	Operator who performed the action.
RTStartDttm	Date and time action occurred.
RTEndDttm	Ending time for task if action is task event otherwise 1/1/1900.
RTReturnValue	1 if action is task and unsuccessful, otherwise 0.
Created	1 if action is page creation, otherwise 0.
Deleted	1 if action is page deletion, otherwise 0.
Sent	1 if action is file sent to module, otherwise 0 (if module is attended, this indicates the image was viewed).
Done	1 if this page was sent to **IADone**.
Written	1 if the action wrote the primary stage file otherwise 0.

Output Dataset	Description
RTAttended	1 if the module is an attended module, otherwise 0.
RTModuleName	Executable name or module name of the module depending on parameter.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.2.5 up_RunOperatorDetailReport

The Index Operator Detail Report gives performance information on the index operators and the indexing steps in the process. This report requires that the following rules be enabled when processing batches: ReportBatchCreate, ReportBatchRename, ReportTaskFinishIndexTask, ReportTaskFinishTask.

- Name of the report: Index Operator Detail Report.
- *XML* parameter file: `IndexOperatorDetailParams.xml`
- Crystal Reports Project file: `IndexOperatorDetail.rpt`

The parameters are:

Table 11-109: Input Parameters in the up_RunOperatorDetailReport Stored Procedure

Input Parameter	Description
FromDate	Beginning date for report or Null.
ToDate	Ending date for report or Null.
Processes	Comma separated list of processes or Null.
Servers	Comma separated list of servers or Null.
Modules	Comma separated list of module executable names or Null.
Operators	Comma separated list of operator names or NULL.
Rate	• 0 = Pages/*Hr* • 1 = Docs/*Hr*

Input Parameter	Description
SortField	• 0 = BatchName • 1 = Hourly Rate
SortOrder	• 0 = Ascending • 1 = Descending
Locale	Locale name for report. The default is "CurrentLocale".

Table 11-110: Output Dataset in the up_RunOperatorDetailReport Stored Procedure

Output Dataset	Description
RTOperator	Index operator name or code (if obscuring user names).
RPName	Process name.
RTStep	Step name in process.
RBBatchName	Batch name.
TaskLocalDate	Date the tasks were processed.
TaskCount	Number of tasks processed.
Pages	Number of pages processed in all tasks.
TaskChars	Number of characters typed.
Docs	Number of documents processed (if tasks trigger at 0 level, this is 0).
TotalTime	Task time in milliseconds.
PageSumChars	Number of characters typed.
KeyTime	Keying time (if module returns it) otherwise same as TotalTime.
FieldCount	Count of index fields per task.
Documents	Number of documents processed (if tasks trigger at 0 level, this is 0).
FromDate	Date or "None" from parameters.
ToDate	Date or "None" from parameters.
Servers	Server parameter or "ALL".
Processes	Server parameter or "ALL".
Modules	Server parameter or "ALL".
Operators	Server parameter or "ALL".
Rate	Number of pages/docs per hour processed.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.2.6 up_RunOperatorSummaryReport

The Index Operator Summary Report gives performance information on the index operators and the indexing steps in the process. This report requires that the following log rules are enabled when processing batches: ReportBatchCreate, ReportTaskFinishIndexTask, ReportTaskFinishTask.

- Name of the report: Index Operator Summary Report.
- *XML* parameter file: `IndexOperatorSummaryParams.xml`
- Crystal Reports Project file: `IndexOperatorSummary.rpt`

The parameters are:

Table 11-111: Input Parameters in the up_RunOperatorSummaryReport Stored Procedure

Input Parameter	Description
FromDate	Beginning date for report or Null.
ToDate	Ending date for report or Null.
Processes	Comma separated list of processes or Null.
Servers	Comma separated list of servers or Null.
Modules	Comma separated list of module executable names or Null.
Operators	Comma separated list of operator names or NULL.
Rate	• 0 = Pages/Hr • 1 = Docs/Hr
SortOrder	• 0 = Ascending • 1 = Descending
SummaryLevel	• 0 = Daily • 1 = Weekly • 2 = Monthly

Input Parameter	Description
Locale	Locale name for report. The default is "CurrentLocale".

Table 11-112: Output Dataset in the up_RunOperatorSummaryReport Stored Procedure

Output Dataset	Description
RTOperator	Index operator name or code (if obscuring user names).
RTYear	Year indexing was done.
RTMonthOrWeek	Month or week indexing was done (depending on *SummaryLevel* parameter).
RTDay	Day indexing was done or 0 if not Daily report.
RTProcess	Process name.
RTStep	Step name in process.
TaskCount	Number of tasks processed.
PageCount	Number of pages indexed.
DocCount	Number of documents indexed.
CharCount	Number of characters typed.
TotalTime	Time for indexing tasks in milliseconds.
KeyTime	Keying time in milliseconds.
FieldCount	Total number of fields.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.2.7 up_RunPageLevelOcrDetailReport

The Page Level *OCR* Processing Detail Report gives performance information for each *OCR* module. This report requires that the following log rules are enabled when processing batches: ReportBatchCreate, ReportBatchRename, ReportTaskFinishOcrPage, ReportTaskFinishPage, and ReportTaskFinishTask.

- Name of the report: Page Level OCR Processing Detail Report.
- *XML* parameter file: `PageLevelOcrProcessingDetailParams.xml`
- Crystal Reports Project file: `PageLevelOcrProcessingDetail.rpt`

The parameters are:

Table 11-113: Input Parameters in the up_RunPageLevelOcrDetailReport Stored Procedure

Input Parameter	Description
FromDate	Beginning date for report or Null.
ToDate	Ending date for report or Null.
Processes	Comma separated list of processes or Null.
Servers	Comma separated list of servers or Null.
Modules	Comma separated list of module executable names or Null.
Organization	• 0 = By process • 1 = By date
ModuleDisplay	• 0 = Use Official name • 1 = Executable name
SortDetailColumn	• 0 = Batch name • 1 = Time/Page
SortOrder	• 0 = Ascending • 1 = Descending
Locale	Locale name for report. The default is “CurrentLocale”.

Table 11-114: Output Dataset in the up_RunPageLevelOcrDetailReport Stored Procedure

Output Dataset	Description
RPName	Process name.
RBBatchName	Batch name.
RTServerName	Server name.

Output Dataset	Description
RTModule	Module executable name.
TaskLocalDate	Date task was processed.
RTLevel	Level name of task.
RTLevelNumber	Level number of task.
RTOrdinal	Ordinal number of task node.
RTTaskUUID	Unique ID of task.
RPOrdinal	Ordinal number of page.
RPProcTime	Processing time for the page.
ROPCharCount	Total characters on page.
ROPRejected	Rejected characters on page.
MDModuleName	Module name.
PctRec	Percentage of characters recognized.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.2.8 up_RunPageLevelOcrSummaryReport

The Page Level *OCR* Processing Summary Report gives performance information for each *OCR* module. This report requires that the following log rules are enabled when processing batches: ReportBatchCreate, ReportTaskFinishOcrPage, ReportTaskFinishPage, ReportTaskFinishTask.

- Name of the report: Page Level *OCR* Processing Summary Report.
- *XML* parameter file: `PageLevelOcrProcessingSummaryParams.xml`
- Crystal Reports Project file: `PageLevelOcrProcessingSummary.rpt`

The parameters are:

Table 11-115: Input Parameters in the up_RunPageLevelOcrSummaryReport Stored Procedure

Input Parameter	Description
FromDate	Beginning date for report or Null.

Input Parameter	Description
ToDate	Ending date for report or Null.
WFList	Comma separated list of processes or Null.
ServerList	Comma separated list of servers or Null.
ModList	Comma separated list of module executable names or Null.
Organization	• 0 = By process • 1 = By date
ModuleDisplay	• 0 = Use Official name • 1 = Executable name
SortDetailColumn	• 0 = Batch name • 1 = Time/Page
SortOrder	• 0 = Ascending • 1 = Descending
SummaryLevel	• 0 = Daily • 1 = Weekly • 2 = Monthly
Locale	Locale name for report. The default is "CurrentLocale".

Table 11-116: Output Dataset in the up_RunPageLevelOcrSummaryReport Stored Procedure

Output Dataset	Description
RPName	Process name.
ThisYear	Year tasks were processed.
ThisMonth	Month or week tasks were processed depending on the *SummaryLevel* parameter.
ThisDay	Day tasks were processed or 0 if not Daily report.
Machine	Workstation running module.
Module	Executable name or module name depending on the *ModuleDisplay* parameter.
Pages	Number of pages processed.
AvgTimePerPage	Average recognition time per page.
AvgRecognized	Average percentage of characters recognized.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.2.9 up_RunScanDetailReport

The Scan Detail Report gives performance information for the scan machines and scan operators. This report requires that the following log rules are enabled when processing batches: ReportBatchCreate, ReportBatchRename, ReportNodeCreate, ReportTaskFinishCreatePage, and ReportTaskFinishTask.

- Name of the report: Scan Detail Report.
- *XML* parameter file: `ScanDetailParams.xml`
- Crystal Reports Project file: `ScanDetail.rpt`

The parameters are:

Table 11-117: Input Parameters in the up_RunScanDetailReport Stored Procedure

Input Parameter	Description
FromDate	Beginning date for report or Null.
ToDate	Ending date for report or Null.
Workflows	Comma separated list of processes or Null.
Servers	Comma separated list of servers or Null.
Modules	Comma separated list of module executable names or Null.
OrganizeByWorkflow	• 0 = Combine workflows • 1 = Separate workflows
ModuleDisplay	• 0 = Use Official name • 1 = Executable name
SortDetailColumn	• 0 = Batch name • 1 = Time/Page
SortOrder	• 0 = Ascending • 1 = Descending
Locale	Locale name for report. The default is "CurrentLocale".

Table 11-118: Output Dataset in the up_RunScanDetailReport Stored Procedure

Output Dataset	Description
TaskLocalDate	Date batch was scanned.
PageCount	Total pages scanned (or imported) in batch.
RescanCount	Total pages rescanned.
TotalTime	Task time scanning or rescanning in milliseconds.
RBBatchName	Batch name.
RateValue	Number of pages scanned per hour.
MachineOrOperator	Workstation or operator name depending on the *IncludeData* parameter.
FromDate	Parameter value or "None".
ToDate	Parameter value or "None".
Machines	Parameter value or "ALL".
Servers	Parameter value or "ALL".
Operators	Parameter value or "ALL".

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.2.10 up_RunScanSummaryReport

The Scan Summary Report gives performance information for the scan machines and scan operators. This report requires that the following log rules are enabled when processing batches: ReportBatchCreate, ReportNodeCreate, and ReportTaskFinishTask.

- Name of the report: Scan Summary Report.
- *XML* parameter file: `ScanSummaryParams.xml`
- Crystal Reports Project file: `ScanSummary.rpt`

The parameters are:

Table 11-119: Input Parameters in the up_RunScanSummaryReport Stored Procedure

Input Parameter	Description
FromDate	Beginning date for report or Null.
ToDate	Ending date for report or Null.
Machines	Comma separated list of scan workstations.
Servers	Comma separated list of servers or Null.
Operators	Comma separated list of operators names or codes.
IncludeData	• 0 = Machine and Date • 1 = Operator and Date • 2 = Date Only
OrganizeBy	• 0 = Date first • 1 = Date second
SortOrder	• 0 = Ascending • 1 = Descending
SummaryLevel	• 0 = Daily • 1 = Weekly • 2 = Monthly
Locale	Locale name for report. The default is "CurrentLocale".

Table 11-120: Output Dataset in the up_RunScanSummaryReport Stored Procedure

Output Dataset	Description
MachineOrOperator	Workstation or operator name depending on *IncludeData* parameter.
ThisYear	Year batches were created.
ThisMonth	Month or Week batches were created (depending on *SummaryLevel*).
ThisDay	Day batches were created or 0 if not daily report.
BatchCount	Batches scanned on date.
PageCount	Pages scanned on date.
RescanCount	Pages rescanned on date.
TotalTime	Scan time in milliseconds.
RateValue	Number of pages scanned per hour.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.8.2.11 up_RunUnattendedModuleDetailReport

The Unattended Module Detail Report gives performance information for each unattended Intelligent Capture module. This report requires that the following log rules are enabled when processing batches: ReportBatchCreate, ReportBatchRename, ReportBatchRollback, and ReportTaskFinishTask.

- Name of the report: Unattended Module Detail Report.
- *XML* parameter file: `UnattendedModuleSummaryParams.xml`
- Crystal Reports Project file: `UnattendedModuleSummary.rpt`

The parameters are:

Table 11-121: Input Parameters in the up_RunUnattendedModuleDetailReport Stored Procedure

Input Parameter	Description
FromDate	Beginning date for report or Null.
ToDate	Ending date for report or Null.
Workflows	Comma separated list of processes or Null.
Servers	Comma separated list of servers or Null.
Modules	Comma separated list of module executable names or Null.
OrganizeByWorkflow	• 0 = Combine workflows • 1 = Separate workflows
ModuleDisplay	• 0 = Use Official name • 1 = Executable name
SortDetailColumn	• 0 = Batch name • 1 = Time/Page
SortOrder	• 0 = Ascending • 1 = Descending
Locale	Locale name for report. The default is "CurrentLocale".

Table 11-122: Output Dataset in the up_RunUnattendedModuleDetailReport Stored Procedure

Output Dataset	Description
RPName	Process name.
BatchName	Batch name.
Machine	Workstation that processed task.
WorkflowName	Process name.
TaskDate	Date task was processed.
NodeId	Node id for task node.
Level	Name of trigger level for task.
OrdinalText	Ordinal of task node converted to a string.
OrdinalInt	Ordinal of task node.
Pages	Page count for task.
Totaltime	Task time in milliseconds.
Rate	Page processing time in milliseconds.
ModuleName	Executable name or module name depending on *ModuleDisplay* parameter.
FromDate	Parameter value or “None”.
ToDate	Parameter value or “None”. .
WorkFlows	Parameter value or “ALL”.
Servers	Parameter value or “ALL”.
Modules	Parameter value or “ALL”.
Organization	*OrganizeByWorkflow* parameter value.
SortColumn	*SortDetailColumn* parameter value.
SortOrder	Parameter value.

Related Topics

“Reports” on page 294

“Report Definitions” on page 295

“Report Details” on page 431

“Managing Reports and Logs” on page 205

11.8.2.12 up_RunUnattendedModuleSummaryReport

The Unattended Module Summary Report gives performance information for each unattended Intelligent Capture module. This report requires that the following log rules are enabled when processing batches: ReportBatchCreate, and ReportTaskFinishTask.

- Name of the report: Unattended Module Summary Report.
- *XML* parameter file: `UnattendedModuleSummaryParams.xml`
- Crystal Reports Project file: `UnattendedModuleSummary.rpt`

The parameters are:

Table 11-123: Input Parameters in the up_RunUnattendedModuleSummaryReport Stored Procedure

Input Parameter	Description
FromDate	Beginning date for report or Null.
ToDate	Ending date for report or Null.
Workflows	Comma separated list of processes or Null.
Servers	Comma separated list of servers or Null.
Modules	Comma separated list of module executable names or Null.
OrganizeByWorkflow	• 0 = Combine workflows • 1 = Separate workflows
ModuleDisplay	• 0 = Use Official name • 1 = Executable name
SortDetailColumn	• 0 = Batch name • 1 = Time/Page
SortOrder	• 0 = Ascending • 1 = Descending
Locale	Locale name for report. The default is "CurrentLocale".

Table 11-124: Output Dataset in the up_RunUnattendedModuleSummaryReport Stored Procedure

Output Dataset	Description
RPName	Process name.
Module	Executable name or module name depending on *ModuleDisplay* parameter.

Output Dataset	Description
Machine	Workstation that processed task.
ThisYear	Year batches were created.
ThisMonth	Month or Week batches were created (depending on *SummaryLevel*).
ThisDay	Day batches were created or 0 if not daily report.
Pages	Page count.
TotTime	Total processing time.
AvgTime	Average time per page.

Related Topics

"Reports" on page 294

"Report Definitions" on page 295

"Report Details" on page 431

"Managing Reports and Logs" on page 205

11.9 Intelligent Capture Server Events: Log Code Details

The following table contains the log codes related to Intelligent Capture Server events. Administrators will need to see these log codes when creating custom log rules for the Intelligent Capture Server.

Table 11-125: Intelligent Capture Server Log Codes

Log code	Server event and description	Category	Data syntax	Notes
1	IASEVENT_SERVER.START: InputAccel Server started	Server	Server.Name Server.ID Server.Machine Name Event.DateTime: Date and time of the event for all events in any category.	
2	IASEVENT_SERVERSTOP: InputAccel Server stopped			
3	IASEVENT_SERVERPAUSE: InputAccel Server paused			

Log code	Server event and description	Category	Data syntax	Notes
4	IASEVENT_SERVERCONTINUE: InputAccel Server resumed			
5	IASEVENT_SERVERADDSCALESERVER: InputAccel Server added to ScaleServer group			
6	IASEVENT_SERVERREMOVESCALESERVER: InputAccel Server removed from ScaleServer group			
7	IASEVENT_SERVERREADY: InputAccel Server ready			
8	IASEVENT_SERVERWIPLOADDONE: Work in progress loading complete			
10	IASEVENT_BATCHCREATE: New batch created	Batch	Server.Name Server.ID Server.Machine Name Module.Name Module.ID Connection.ID Connection.*UUID* Connection.MachineName Connection.UserName Connection.SetupMode	
12	IASEVENT_BATCHPRIORITYCHANGE: Batch priority changed			
14	IASEVENT_BATCHSTATUSMESSAGECHANGE: Batch status message has changed			

Log code	Server event and description	Category	Data syntax	Notes
18	IASEVENT_BATCHDESCRIPTIONCHANGE: Batch description has changed		Process.Name Process.UUID Process.ID Batch.Name Batch.ID Batch.UUID Batch.Description Batch.Priority Batch.LastSyncDateTime Batch.CreationDateTime Batch.ModificationDateTime Batch.CompileDateTime Batch.RollbackDateTime Batch.LockedForMoreScanning Event.DateTime	
19	IASEVENT_BATCHRENAME: Batch renamed			

Log code	Server event and description	Category	Data syntax	Notes
11	IASEVENT_BATCHDELETE: Batch deleted	Batch	Server.Name Server.ID Server.Machine Name Process.Name Process.UUID Process.ID Batch.Name Batch.ID Batch.*UUID* Module.Name Module.ID Connection.MachineName Connection.ID Connection.*UUID* Connection.UserName Connection.SetupMode Event.DateTime	
13	IASEVENT_BATCHSTATUSCHANGE: The status of a batch has changed.	Batch	Server.Name Server.ID Server.Machine Name Process.Name Process.*UUID* Process.ID Batch.Name Batch.ID Batch.*UUID*	
16	IASEVENT_BATCHSYNC: Batch sync occurred			
17	IASEVENT_BATCHROLLBACK: Batch rollback occurred			

Log code	Server event and description	Category	Data syntax	Notes
23	IASEVENT_BATCHLOAD: Batch loaded		Batch.Description Batch.Priority Batch.LastSyncDateTime Batch.CreationDateTime Batch.ModificationDateTime Batch.CompileDateTime Batch.RollbackDateTime Batch.LockedForMoreScanning Event.DateTime	
24	IASEVENT_BATCHUNLOAD: Batch unloaded			
50	PROCESSLOAD: *IAP* loaded	Process	Process.Name Process.*UUID* Process.ID Server.Name Server.ID Server.Machine Name Event.DateTime	
51	IASEVENT_PROCESSUNLOAD: *IAP* unloaded			
52	IASEVENT_PROCESSINSTALL: *IAP* installed	Process	Process.Name Process.*UUID* Process.ID Server.Name Server.ID Server.Machine Name Module.Name Module.ID Connection.MachineName	
53	IASEVENT_PROCESSDELETE: *IAP* deleted			
54	IASEVENT_PROCESSPRIORITYCHANGE: *IAP* priority changed			
55	IASEVENT_PROCESSDESCRIPTIONCHANGE: *IAP* description changed			

Log code	Server event and description	Category	Data syntax	Notes
56	IASEVENT_PROCESSRENAME: *IAP* renamed		Connection.ID Connection.UUID Connection.UserName Connection.SetupMode Event.DateTime	
70	IASEVENT_MODULECONNECT: Module connected	Connection	Module.Name Module.ID Connection.MachineName Connection.Departments Connection.ID Connection.*UUID* Connection.UserName Connection.SetupMode Server.Name Server.ID Server.MachineName Event.DateTime	

Log code	Server event and description	Category	Data syntax	Notes
71	IASEVENT_MODULEDISCONNECT: Module disconnected	Connection	Module.Name Module.ID Connection.MachineName Connection.UserName Connection.Departments Connection.ID Connection.*UUID* Server.Name Server.ID Server.MachineName Event.DateTime	

Log code	Server event and description	Category	Data syntax	Notes
80	IASEVENT_STEPSETDEPARTMENT: Department list changed	Step	Step.Number Step.Name Step.Departments Module.Name Module.ID Connection.MachineName Connection.UserName Connection.Departments Connection.ID Connection.*UUID* Server.Name Server.ID Server.MachineName Event.DateTime	

Log code	Server event and description	Category	Data syntax	Notes
100	IASEVENT_NODECREATE : Node created	Node	Node.ID Node.Level Node.LevelName Node.ParentID Node.Ordinal: index of the node within the batch Node.ChildCount.N: where N is the level to count child nodes for 0 through 7 Batch.Name Batch.ID Batch.*UUID* Batch.Description Batch.Priority Batch.LastSyncDateTime Batch.CreationDateTime Batch.ModificationDateTime Batch.CompileDateTime Batch.RollbackDateTime Module.Name Module.ID Connection.MachineName	

Log code	Server event and description	Category	Data syntax	Notes
			Connection.User Name Connection.Departments Connection.ID Connection.*UUID* Server.Name Server.ID Server.Machine Name Event.DateTime	

Log code	Server event and description	Category	Data syntax	Notes
101		Node	Node.ID Node.Level Node.LevelName Node.ParentID Node.ChildCount.N Module.Name Module.ID Connection.MachineName Connection.UserName Connection.Departments Connection.ID Connection.UUID Server.Name Server.ID Server.MachineName Event.DateTime	
102	IASEVENT_NODEMOVEBEGIN: Node move operation started	Node	Node.ID Node.Level Node.LevelName Node.ParentID Node.Ordinal Node.ChildCount.N Module.Name Module.ID	• IA_NET_REMOVESAVEDLOCK This event is logged when the Intelligent Capture Server receives client message IA_NET_REMOVESAVEDLOCK, which is sent
103	IASEVENT_NODEMOVEEND: Node move operation completed			

Log code	Server event and description	Category	Data syntax	Notes
104	IA_NET_REMOVESAVEDLOCK: A lock was removed from a node		Connection.MachineName Connection.UserName Connection.Departments Connection.ID Connection.*UUID* Server.Name Server.ID Server.MachineName Event.DateTime	by Intelligent Capture Administrator when a user removes locks from batches; one message is sent per lock.
121	IASEVENT_TASKSENT: Task sent to a module	Task	Task.UUID Task.PageCount Task.TaskRouting Task.SecondsSinceReady Task.SentDateTime Task.StartDateTime Task.EndDateTime Task.Milliseconds Task.ReturnValue Step.Number Step.Name Step.Departments Connection.MachineName	• Task.TaskRouting Contains the value of a dynamic department on a task level. • Task.SecondsSinceReady The number of seconds that a task remains in the Ready state before it is sent to a module for processing. Only applies to tasks that are placed into the Ready state in the current Intelligent Capture Server runtime session. For example, a
122	IASEVENT_TASKWORKSTART: Task processing started			
123	IASEVENT_TASKFINISH: Task finished			
124	IA_NET_TASKOFFLINE: A task was set offline			
125	IASEVENT_TASKRETRIGGERED: A task was retriggered			

Log code	Server event and description	Category	Data syntax	Notes
126	IASEVENT_TASKREADY: A task was set to ready		Connection.UserName Connection.Departments Connection.ID Connection.*UUID* Server.Name Server.ID Server.MachineName Event.DateTime	task might already be in a Ready state during the current session if an operator had not accepted a task before the server was shut down in the previous session. • IA_NET_TASKSETOFFLINE The event is logged when the Intelligent Capture Server receives client message IA_NET_TASKSETOFFLINE, which is sent by WSInput. • IASEVENT_TASKRETRIGGERED The event is logged when the Intelligent Capture Server receives client message IASEVENT_TASKRETRIGGERED, which is sent by WSInput.

Log code	Server event and description	Category	Data syntax	Notes
130	IASEVENT_NODEFINISHEDTASK_LEVEL0: Level 0 node is finished processing	NodeVerbose	Task.*UUID* Task.PageCount Task.SentDateTime Task.StartDateTime Task.EndDateTime Task.Milliseconds Task.ReturnValue Step.Number Step.Name Step.Departments Connection.MachineName Connection.UserName Connection.Departments Connection.ID Connection.*UUID* Server.Name Server.ID Server.MachineName Event.DateTime	
131	IASEVENT_NODEFINISHEDTASK_LEVEL1: Level 1 node finished			
132	IASEVENT_NODEFINISHEDTASK_LEVEL2: Level 2 node finished			
133	IASEVENT_NODEFINISHEDTASK_LEVEL3: Level 3 node finished			
134	IASEVENT_NODEFINISHEDTASK_LEVEL4: Level 4 node finished			
135	IASEVENT_NODEFINISHEDTASK_LEVEL5: Level 5 node finished			
136	IASEVENT_NODEFINISHEDTASK_LEVEL6: Level 6 node finished			
137	IASEVENT_NODEFINISHEDTASK_LEVEL7: Level 7 node finished			

Log code	Server event and description	Category	Data syntax	Notes
160	IASEVENT_VALUECREATE: Dynamic value created	Data	Value.Key Step.Number Step.Name Step.Departments Node.ID Node.Level Node.LevelName Node.ParentID Node.Ordinal Node.ChildCount.N Batch.Name Batch.ID Batch.*UUID* Batch.Description Batch.Priority Batch.LastSyncDateTime Batch.CreationDateTime Batch.ModificationDateTime Batch.CompileDateTime Batch.RollbackDateTime Module.Name Module.ID Connection.MachineName	

Log code	Server event and description	Category	Data syntax	Notes
			Connection.User Name Connection.Departments Connection.ID Connection.*UUID* Server.Name Server.ID Server.Machine Name Event.DateTime	
161	IASEVENT_VALUEGET: IA Value requested	Data	Value.Key Value.Content Step.Number Step.Name Step.Departments Node.ID Node.Level Node.LevelName Node.ParentID Node.Ordinal Node.ChildCount.N Batch.Name Batch.ID Batch.*UUID* Batch.Description Batch.Priority	• IASEVENT_VALUESET This event is logged when setup values are modified during module setup or regular batch data updates. • IASEVENT_VALUESTEPSET This event is logged as follows: – Any single setup values that are manually edited in Intelligent Capture Administrator are logged. – If log code 162 is also enabled,
162	IASEVENT_VALUESET: IA Value set			
163	IASEVENT_VALUESTEPSET: A step configuration value was set by a module or script code			

Log code	Server event and description	Category	Data syntax	Notes
164	IASEVENT_VALUEMODULESET: A module configuration value was set by a module or script code		Batch.LastSyncDateTime Batch.CreationDateTime Batch.ModificationDateTime Batch.CompileDateTime Batch.RollbackDateTime Module.Name Module.ID Connection.MachineName Connection.UserName Connection.Departments Connection.ID Connection.*UUID* Server.Name Server.ID Server.MachineName Event.DateTime	then this log code does not log setup values modified during module setup because it would be redundant; otherwise, if log code 162 is disabled, then the aforementioned values are also logged. Therefore, if you want only the values that are manually edited in Intelligent Capture Administrator to be logged with this event, then enable log code 162 as well. • IASEVENT_VALUEMODULESET This event is logged when a user changes a global module configuration

Log code	Server event and description	Category	Data syntax	Notes
				or a profile. A common scenario is when a user changes a ScanPlus configuration such as scanner settings or a profile (for example, Standard Export).
170	IASEVENT_STAGEFILEREAD: Stage file read	StageFile	StageFile.Number Node.ID Node.Level Node.LevelName Node.ParentID Node.Ordinal Node.ChildCount.N Batch.Name Batch.ID Batch.UUID Batch.Description Batch.Priority Batch.LastSyncDateTime Batch.CreationDateTime Batch.ModificationDateTime Batch.CompileDateTime	
171	IASEVENT_STAGEFILEWRITE: Stage file written			

Log code	Server event and description	Category	Data syntax	Notes
172	IASEVENT_STAGEFILEDELETE: Stage file deleted		Batch.RollbackDateTime Module.Name Module.ID Connection.MachineName Connection.UserName Connection.Departments Connection.ID Connection.UUID Server.Name Server.ID Server.MachineName Event.DateTime	
180	IASEVENT_CONFIGFILEREAD: Configuration file read	ConfigFile	ConfigFile.FileName Module.Name Module.ID Connection.MachineName Connection.UserName Connection.Departments Connection.ID Connection.UUID Server.Name Server.ID Server.MachineName Event.DateTime	
181	IASEVENT_CONFIGFILEWRITE: Configuration file written			
182	IASEVENT_CONFIGFILEDELETE: Configuration file deleted			

Log code	Server event and description	Category	Data syntax	Notes
190	IASEVENT_SECURITYPERMISSIONCHANGE: Permissions changed	Security	Security.Object  **Note:** For a description of Security Object Values, see "Security Object Values" on page 489. Security.Access  **Note:** For a description of Security Access values, see "Security Access Values" on page 489. Security.Result  **Note:** For a description of Security Result values, see "Security Result Values" on page 491 Module.Name Module.ID Connection.MachineName	
191	IASEVENT_SECURITYCHECKFAILED: Permissions check failed			

Log code	Server event and description	Category	Data syntax	Notes
192	IASEVENT_SECURITYCHECKSUCCEEDED: Permissions check succeeded		Connection.UserName Connection.Departments Connection.ID Connection.UUID Server.Name Server.ID Server.MachineName Event.DateTime	

Security Object Values

The value logged for Security Objects (data syntax Security.Object specified for log codes 190, 191, and 192) can either be in numeric format or string format. The following table lists the security object numeric and string values and the security object that the value refers to.

Security Object Numeric Value	Security Object String Value	Description of the Security Object
1	IASSEC_BATCHORPROC	Batch or Process
2	IASSEC_DEPARTMENT	Department
3	IASSEC_MODULE	Module
4	IASSEC_MODULEVALUE	Module Value
5	IASSEC_SETTING	Server Setting
6	IASSEC_ADMIN	Admin
7	IASSEC_ROLE	Role

Security Access Values

The value logged for Security Access (data syntax Security.Access specified for log codes 190, 191, and 192) can either be in numeric format or string format. The following table lists the security access numeric and string values and a description of what the security access value refers to.

Security Access Numeric Value	Security Access String Value	Description of the Security Access
0	InvalidPermission	Invalid permission.
1	Emc.InputAccel.Server.Create.Batch	Create batches to the server.
2	Emc.InputAccel.Server.Copy.Batch.to.Server	Copy batches to the Intelligent Capture Server.
3	Emc.InputAccel.Server.Install.Process	Install processes on the server.
4	Emc.InputAccel.System.BatchRead	View the batches in the system along with their state and settings.
5	Emc.InputAccel.System.BatchModify	Modify batch data. This includes scanning, indexing, image enhancement, and other operations that modifies batch data.
6	Emc.InputAccel.System.ProcessRead	View the Intelligent Capture processes installed in the system and view their settings.
7	Emc.InputAccel.System.ProcessModify	Add, modify, delete Intelligent Capture processes to the system.
8	Emc.InputAccel.Server.Login	Log in to the Intelligent Capture Server.
9	Emc.InputAccel.Server.Debug	Obtain server debug information.
10	Emc.InputAccel.Server.Read.Module.Data	Read module data from the server.
11	Emc.InputAccel.Server.Write.Module.Data	Write module data to the server.
12	Emc.InputAccel.System.SecurityRead	Read *ACL* security data.
13	Emc.InputAccel.System.SecurityModify	Write *ACL* security data. This permission is required to make any security changes to the roles, process, batch, and department ACLs.

Security Access Numeric Value	Security Access String Value	Description of the Security Access
14	Emc.InputAccel.System.ServerRead	View the servers installed in the Intelligent Capture Database, as well as the ScaleServer groups in the system. This permission is required for any client attempting to connect to a ScaleServer group.
15	Emc.InputAccel.System.ServerModify	Update connection settings for servers, add and modify ScaleServer groups.
16	Emc.InputAccel.Server.LogMessage	Obtain server log messages.
17	Emc.InputAccel.Server.SetLogContext	Set server log context data.
18	Emc.InputAccel.System.ReadProtectedValues	Read protected IA Values.
19	Emc.InputAccel.System.ModifyProtectedValues	Modify protected IA Values.

Security Result Values

The value logged for Security Result (data syntax Security.Result specified for log codes 190, 191, and 192) is in numeric format. The following table lists the security result numeric values and the description of the value.

Security Result Numeric Value	Security Result Description
0	Success
<IA Error_Warning_and_Audit_LogCodes>	Error

A complete list of client module error and log codes is listed in *OpenText Intelligent Capture - Module Reference (ECPCORE-CMD)*.

Chapter 12

Maximizing and Testing Intelligent Capture and Intelligent Capture REST Services System Performance

This section includes information for maximizing and testing the Intelligent Capture and Intelligent Capture REST Services system performance.

12.1 Testing Performance with Performance Counters

Intelligent Capture and Intelligent Capture REST Services has a number of performance counters that can be used to track the performance of the Intelligent Capture and Intelligent Capture REST Services systems and to determine whether the current setup is sufficient to handle your document processing needs.

To test the performance of the Intelligent Capture and Intelligent Capture REST Services systems:

1. On the machines where Intelligent Capture Server, the Intelligent Capture REST Service Web application (on IIS), or the Module Server (a Windows service) are installed, start the Windows Performance Monitor (`perfmon.exe`).
2. Select from the following objects to monitor:
   - **IA:DAL**
   - **IA:Logging**
   - **IA:Security**
   - **IA:Server_InputAccel**
   - **IA:Server_Inputaccel_Modules**
   - **Captiva WebServer**
   - **Captiva ModuleServer**

   Note: The performance counter objects are only available on the machine where the associated Intelligent Capture Server, the Intelligent Capture REST Service Web application, or the Module Server are installed.
3. Add the required performance objects and counters to the System Monitor or to the **Performance Logs and Alerts > Counter Logs**. For information about each performance object and counters available for the object, see "Intelligent Capture and Intelligent Capture REST Services Performance Counters" on page 494.

Notes

- To read performance counter data on Windows Vista as a non-administrator user, you must be a member of the Performance Monitor Users group. To read performance counter data remotely as a non-administrator user, you must be a member of the Performance Monitor Users group on the remote computer and you must modify the registry on the remote computer to grant read access to the Performance Counters.
- On Windows x64 systems, the 64-bit `perfmon.exe` located in the `\Windows\System32` folder will not display 32-bit performance counters. Therefore, you must use the 32-bit `perfmon.exe` located in the `\Windows\SysWOW64` folder. If you select the **Performance** option from the Control Panel, the 64-bit `perfmon.exe` will run, so do not use this option.
- The Performance Logs and Alerts service default user (Network Service) has insufficient permissions to access the Intelligent Capture performance objects. Therefore, you must specify a user with sufficient permissions in the Windows Service Management Console for this service.

Table 12-1: Intelligent Capture and Intelligent Capture REST Services Performance Counters

Performance Counters	
Performance Object: **IA:DAL**	
Counter Name	*Description*

Performance Counters	
% Load Factor	Percentage of elapsed time that the Data Access Layer spends to execute requests. The % Load Factor may exceed 100% if there is more than one *CPU*. For example: • 2 *CPU*s = Maximum load factor 200% • 4 *CPU*s = Maximum load factor 400% • 8 *CPU*s = Maximum load factor 800% The load factor is calculated exactly as it is defined. Therefore, if over a 10 second interval *DAL* executed for 5 seconds (regardless of the number of threads), then the % Load Factor is 50% (5 seconds *DAL* / 10 available seconds * 100). This same calculation holds true with multiple *CPU*s and multi-threading. For example, with 8 *CPU*s, over a 10 second wall clock interval, there are 80 seconds of available processing time because each *CPU* has 10 seconds and there are 8 *CPU*s (10 * 8 = 80). Thus, if the *DAL* is executing on all 8 threads for all 10 seconds of wall clock time, the % Load Factor is 800% (80 seconds of *DAL* execution / 10 seconds of wall clock time.
Avg. Execution Time Millisec	Average execution time in milliseconds for query and non-query.
Current Connection Count	Current count of active connections to the database.
Data Requests/sec	Number of queries and non-queries per second.
Total Connection Count	Total number of connections since the start of the application.
Total Error Count	Total number of errors since the start of the application.
Total Non Query Command Count	Total number of non-query operations since the start of the application.
Total Non Query Execution Time MilliSec	Total execution time in milliseconds for all non-query operations.
Total Query Command Count	Total number of query operations since the start of the application.
Total Query Execution Time Millisec	Total execution time in milliseconds for all query operations.

Performance Counters	
Total Row Count	Total number of rows fetched.
*Performance Object:***IA:Logging**	
Counter Name	*Description*
Average Time Before Sending Log To Sinks/ microseconds	Average time (in microseconds) to process logs before writing them to the sinks. Includes the time to match a log to the rules and prepare it for writing.
Average Time For Unwritten Log/ microseconds	Average time (in microseconds) to process logs that will not be written.
Average Time To Write Log/microseconds	Average time (in microseconds) to write logs.
Logs Received/seconds	Number of logs sent per second from all components to the Logging Library
Logs Written/seconds	Number of logs written per second to their destinations.
Percentage Of Logs Written Successfully	Percentage of logs written successfully to the sinks.
*Performance Object:***IA:Security**	
Counter Name	*Description*
Authorization Requests/sec	Number of authorization checks performed in Intelligent Capture per second.
Number of authorization requests	Number of authorization requests served by the Security Library per step.
Permission set requests/second	Number of seconds it takes a query to retrieve the permission set from the security database for a particular user.
Total number of authorization requests	Number of authorization requests served by Security Library (all the steps on the particular system).
*Performance Object:***IA:Server_InputAccel**	
Counter Name	*Description*
Authorization Requests/sec	Number of authorization checks performed in Intelligent Capture Server per second.
Permission Updates/sec	Number of permissions updated in Intelligent Capture per second.
Batch Loads/sec	Number of batches being loaded into memory per second.
Batches Loaded	Number of batches loaded in memory at a given time. This number is less than or equal to the `BatchMaxLoaded` value set in the Intelligent Capture Database.

Performance Counters	
Connections	Number of clients connected to the server.
Disk Bytes Read/sec	Number of bytes read from the disk by the server in response to file requests by clients.
Disk Bytes Written/sec	Number of bytes written to the disk by the server in response to files sent from clients.
VBA Calls/sec	Number of *VBA* calls made per second. This includes the `Finish` and `Prepare` events defined in the active batches.
Network Bytes Read/sec	Number of bytes read from the network by the server.
Network Bytes Written/sec	Number of bytes written to the network by the server.
Packets Received/sec	Number of packets received by the server from clients per second.
Packets Sent/sec	Number of packets sent to clients by the server per second.
Pending I/O	Number of packets waiting to be sent by the server. This number is proportional to the number of connected clients.
Processing Message Count	Number of messages actively being processed.
Total Batch Count	The total number of batches that can be loaded by the server.
Total Message Bytes	Total backlog of the messages in bytes. Keep-alive (ping) messages between clients and server are not included in this count.
Total Message Count	Total number of message objects. This includes message objects in any queue.
VBA Message Thread Queue Length	Number of messages remaining in the *VBA* thread queue to be processed by Intelligent Capture.
WIP Event Queue Length	The number of events remaining in the WIP event queue to be sent to the database by the server.
WIP Event Queue Blocked Count	The total number of times the WIP event queue has been blocked because the maximum length has been reached.
WIP Event Queue Blocked Time	The total time in milliseconds that the WIP event queue has been blocked.

Performance Counters	
Stat Event Queue Length	The number of events remaining in the Report Statistics event queues to be sent to the database. This is the total sum of queue length for all ten Report Statistics queues.
Stat Event Queue Blocked Count	The total number of times that the Report Statistics event queues has been blocked because the maximum length has been reached. This is the total sum of blocked count for all ten Report Statistics queues.
Stat Event Queue Blocked Time	The total time in milliseconds that the Report Statistics event queue has been blocked. This is the total sum of blocked time for all ten Report Statistics queues.
Misc Event Queue Length	The number of events remaining in the Misc event queue to be sent to the database.
Misc Event Queue Blocked Count	The total number of times the Misc event queue has blocked because the maximum length has been reached.
Throttle DB requests count	The number of DB requests being throttled.
Misc Event Queue Blocked Time	The total time in milliseconds that the Misc event queue has been blocked.
Heavy DB requests count	The number of heavy database requests being serviced.
*Performance Object:***IA:Server_Inputaccel_Modules**	
Counter Name	*Description*
Task Queue Length For Module	Task Queue Length For Module.
Task Queue Drain Time Per Module	Number of seconds needed to process all tasks for this module by all currently connected instances.
Module Instance Count	Number of module instances running.
Performance Object: Intelligent Capture Module Server	
Counter Name	*Description*
total calls	Total number of calls to this server.
total callsavgexecms	Average call execution time (in milliseconds) for all calls on this server.
total callserrors	Number of errors for all calls on this server.

Performance Counters	
clm-<*Module Name*>	Number of calls made to the <*Module Name*> module, where <*Module Name*> is any of the following module names specified in the system: • `clientnoop` • `cpextrac` • `cpimgpro` • `imgconv` • `fpocr` • `cpexport`
clm-<*Module Name*>avgexecms	Average execution time (in milliseconds) of the <*Module Name*> module.
clm-<*Module Name*>errors	Number of errors encountered for the <*Module Name*> module.
clm-<*Module Name*>perhour	Number of calls to the <*Module Name*> module per hour.
<*Module Name*>-qlen	Represents the queue length of requests pending for the <*Module Name*> module.
file read	Number of files read.
file readavgexecms	Average execution time (in milliseconds) for reading files.
file readerrors	Number of read errors.
file readperhour	Number of files read per hour.
file write	Number of files written.
file writeavgexecms	Average execution time (in milliseconds) for writing a file.
file writeerrors	Number of write errors.
file writeperhour	Number of files written per hour.
file access conflicts	Number of access conflicts.
file readwrite	Number of files read and written.
file readwriteavgexecms	Average execution time (in milliseconds) for reading and writing files.
file readwriteerrors	Number of read and write errors.
file readwriteperhour	Number of files read and written per hour.
file rw conflicts	Number of read/write conflicts.
clients created	Number of client modules created.
clients createdavgexecms	Average execution time (in milliseconds) for creating the clients.

Performance Counters	
clients createderrors	Number of client creation errors.
clients createdperhour	Number of clients created per hour.
clients recycled	Number of clients recycled.
clients recycledavgexecms	Average execution time (in milliseconds) for recycling clients.
clients recyclederrors	Number of client recycling errors.
clients recycledperhour	Number of clients recycled per hour.
minute timer	Number of times the minute timer executed.
minute timeravgexecms	Average execution time (in milliseconds) of minute timer processing.
minute timererrors	Number of minute timer errors.
minute timerperhour	Number of minute timer calls per hour.
second timer	Number of times the second timer executed.
second timeravgexecms	Average execution time (in milliseconds) of second timer processing.
second timererrors	Number of second timer errors.
second timerperhour	Number of second timer calls per hour.
servers purged	Number of servers purged.
servers purgedavgexecms	Average execution time (in milliseconds) for server purging.
servers purgederrors	Number of errors for server purging.
servers purgedperhour	Number of servers purged per hour.
Performance Object: Intelligent Capture WebService Server	
Counter Name	*Description*
user sessions	The number of active sessions on this server.
sessions purged	The number of sessions purged.
sessions purgedavgexecms	The average execution time (in milliseconds) that it took to purge the session.
sessions purgederrors	The number of purge errors encountered.
sessions purgedperhour	The number of purged sessions per hour.
total calls	The total number of calls reported by this server.
total callsavgexecms	The total calls average execution time in milliseconds.
total callserrors	The total call errors.

Performance Counters	
total callsperhour	The total calls per hour.
batches submitted	The number of batches submitted.
batches submittedavgexecms	The average execution time (in milliseconds) for batches.
batches submittederrors	The number of batch submission errors.
batches submittedperhour	The number of batches submitted per hour.
tasks served	Number of tasks served.
tasks servedavgexecms	Average execution time (in milliseconds) for tasks served.
tasks servederrors	Number of errors for task served.
tasks servedperhour	Number of tasks served per hour.
tasks finished	Number of tasks finished.
tasks finishedavgexecms	Average execution time (in millseconds) for tasks finished.
tasks finishederrors	Number of errors for tasks finished.
tasks finishedperhour	Number of tasks finished per hour.
iaconnect	Number of Intelligent Capture Server connections.
iaconnectavgexecms	Average execution time (in milliseconds) of Intelligent Capture Server connections.
iaconnecterrors	Number of errors for Intelligent Capture Server connections.
iaconnectperhour	Number of Intelligent Capture Server connection per hour.
ia free connections	Number of Intelligent Capture Server free connections.
ia images uploaded	Number of images uploaded to Intelligent Capture Server.
ia image data kb	Amount of data (in kilobytes) of Intelligent Capture Server images.
files exported	The number of files exported.
files exportedavgexecms	The average execution time (in milliseconds) for exported files.
files exportederrors	The number of errors for exported files.
files exportedperhour	The number of files exported per hour.
documents exported	The number of documents exported.

Performance Counters	
documents exportedavgexecms	The average execution time (in milliseconds) for documents exported.
documents exportederrors	The number of errors for exported documents.
documents exportedperhour	The number of documents exported per hour.
cl-<*Module Name*>	<*Module Name*> is any of the following module names specified in the system: • `clientnoop` • `cpextrac` • `cpimgpro` • `imgconv` • `fpocr` • `cpexport` **Note:** This counter does not publish a value.
cl-<*Module Name*>_alloc	The number of times the <*Module Name*> module was allocated in the resource pool.
cl-<*Module Name*>_allocavgexecms	The average execution time (in milliseconds) for the <*Module Name*> module allocation.
cl-<*Module Name*>_allocerrors	The number of allocation errors for the <*Module Name*> module.
cl-<*Module Name*>_allocperhour	The number of <*Module Name*> modules allocated per hour.

Performance Counters	
svc<*Service Name*>()	The number of calls to the <*Service Name*> service, where <*Service Name*> is any of the following module names specified in the system: • `classify` • `classifyextractpage` • `extractdocument` • `extractpage` • `classifyextractdocument` • `fullpageocr` • `processimage` • `processimagepipeline` • `readbarcodes` • `uimdata` • `designer` • `convertimages` • `export` • `iatask`
svc<*Service Name*>()avgexecms	The average execution time (in milliseconds) for the <*Service Name*> service.
svc<*Service Name*>()errors	The number of errors that occurred for the <*Service Name*> service.
svc<*Service Name*>()perhour	The number of calls to the <*Service Name*> service per hour.
file read	Number of files read.
file readavgexecms	Average execution time (in milliseconds) for reading files.
file readerrors	Number of read errors.
file readperhour	Number of files read per hour.
file write	Number of files written.
file writeavgexecms	Average execution time (in milliseconds) for writing a file.
file writeerrors	Number of write errors.
file writeperhour	Number of files written per hour.
file access conflicts	Number of access conflicts.
file readwrite	Number of files read and written.
file readwriteavgexecms	Average execution time (in milliseconds) for reading and writing files.

Performance Counters	
file readwriteerrors	Number of read and write errors.
file readwriteperhour	Number of files read and written per hour.
file rw conflicts	Number of read/write conflicts.
file data bytes	Amount (in bytes) of file data.
file data bytesavgexecms	Average execution time (in milliseconds) for writing file data bytes.
file data byteserrors	Number of errors encountered when reading or writing file data.
file data bytesperhour	Amount of file data (in bytes) per hour.
minute timer	Number of times the minute timer executed.
minute timeravgexecms	Average execution time (in milliseconds) of minute timer processing.
minute timererrors	Number of minute timer errors.
minute timerperhour	Number of minute timer calls per hour.
second timer	Number of times the second timer executed.
second timeravgexecms	Average execution time (in milliseconds) of second timer processing.
second timererrors	Number of second timer errors.
second timerperhour	Number of second timer calls per hour.
servers purged	Number of servers purged.
servers purgedavgexecms	Average execution time (in milliseconds) for server purging.
servers purgederrors	Number of errors for server purging.
servers purgedperhour	Number of servers purged per hour.

12.2 Improving Intelligent Capture Server Performance

To improve the performance of the Intelligent Capture Server, we recommend:

- **Do not run dynamic disk defragmentation software on the Intelligent Capture Server**

  This type of utility can increase the risk of data corruption and decrease performance of the Intelligent Capture Server by slowing disk access and using *CPU* time.

- **Do not execute possible long-running and high-load CaptureFlow script or VBA operations**

CaptureFlow script and VBA execution is single-threaded within an Intelligent Capture Server instance and runs inside the Intelligent Capture Server process. We strongly recommend that you avoid executing possible long-running and high-load CaptureFlow script or VBA operations. The following are examples of operations that are not supported: ODBC calls, access to external databases such as Documentum, SQL Server, etc.; calls to an external system using web services; local and network file access, other network operations; calls to any third-party libraries or external processes; long-running computations, complex data analysis, and other CPU and memory intensive operations. Instead, as an alternative, add code used for long running operations to a dedicated code module, for example the .NET code module.

- **Do not run antivirus software on the `IAS` folder**

  Running antivirus software on the `IAS` folder and its subfolders will drastically degrade Intelligent Capture Server performance due to the number of files being written to the directory structure. In addition, some antivirus programs intercept network traffic and can interfere with Intelligent Capture Server operation. In all cases, you should exclude the Intelligent Capture Server installation folder (`C:\Program Files\InputAccel\Server` by default) and all of its subfolders from antivirus scanning.

- **Do not run additional Intelligent Capture modules on the server**

  Due to the way Windows switches tasks, running additional Intelligent Capture modules on the same machine as the Intelligent Capture Server can result in a significant performance drop, even if the additional modules do not use much *CPU* time.

- **Do not use screen savers that use a lot of CPU time**

  Suggestion: use a logon or blank screen for your screen saver.

- **Run Intelligent Capture on a discrete sub-network**

  Create a separate sub-network for the Intelligent Capture System and connect it to the main network through a switching hub or a router. Segmenting Intelligent Capture from the rest of the network prevents the rest of the network from causing Intelligent Capture performance problems.

- **Minimize read and write operations in the IPP**

  Each time that a file must be read or written, the system must open and close the file, which is a relatively slow operation. These operations must be kept to a minimum.

- ***Minimize looping through nodes in the IPP***

  Looping through the nodes in a batch can be time-consuming because the body of the loop is executed many times. Avoid some loops by moving commands to a different `Prepare` or `Finish` event handler or by adding trigger variables. (If loops are created in the *IPP*, then note that looping through all the Level 0 nodes in a Level 7 batch is worse than running and looping at Level 0.)

- **Optimize the number of images in batches**

The optimal number of images per batch will vary depending on many factors, including the size of images and the complexity of operations performed. Note, however, that a minimum of 10 pages per batch is recommended.

- **Delete batches when they are finished processing**

  After Intelligent Capture has finished processing and exported a batch to the database, delete the batch from the Intelligent Capture Server. This reduces the amount of disk space required on the server machine.

- **Modify server parameters**

  There are several Intelligent Capture Server parameters which may improve performance when properly tuned. These parameters can be updated in Intelligent Capture Administrator. For instructions to modify server parameters, see Viewing Intelligent Capture Server properties. Suggested values for some of the Intelligent Capture parameters:

  – `BatchMaxAddressSpaceK`

    For optimal performance, it is recommended that this parameter be set to 0.5 GB less than the machine's physical memory. For example, if a machine has 16 GB of physical memory, then this parameter would be 16252928 (15.5 GB).

  – `BatchSyncMaxTime`: 2000 (2 seconds)

  – `EventQueueDepth`: 50,000 or higher if you have a reporting license and a slow database. The `Event Queue Length` performance counter can be used to determine the number of messages in the server queue.

- **Ensure proper number of servers**

  The average *CPU* utilization for multi-*CPU* Intelligent Capture Servers should approach, on average, about 70 percent.

12.3 Improving Database Performance

The Intelligent Capture Database must periodically be defragmented, reindexed, and purged to optimize performance.

Defragmenting and Rebuilding Indexes in the Intelligent Capture Database

Depending on the volume and type of processing, periodically defragmenting and rebuilding indexes in the Intelligent Capture Database may help prevent application performance degradation. The Intelligent Capture Database installer installs these two stored procedures into the SQL Server to perform these functions on a small set of pre-selected tables. Use these stored procedures in conjunction with *SQL Server* scheduled job functionality to defragment and rebuild indexes on a regular basis:

- `up_ReorganizeIndexes`: Defragments all of the indexes in the pre-selected set of Intelligent Capture Database tables. This stored procedure can be run at any time since it does not affect concurrent application query activity.

- `up_RebuildIndexes`: Rebuilds all of the indexes in the pre-selected set of Intelligent Capture Database tables. This stored procedure must be run when application activity is at a minimum since application queries will not have access to the tables during the rebuilding process.

Notes

- These stored procedures can be run manually or as scheduled jobs; however, these stored procedures are not set up to run automatically as scheduled jobs. You can create your own scheduled jobs to run these stored procedures. See the SQL Server documentation for steps to create scheduled jobs.
- Preferably, defragment indexes once a day and rebuild indexes once a week. The most appropriate schedule for these activities depends on your specific implementation, workload and operations schedules, and can only be determined by the customer.

Purging the Intelligent Capture Database

The Intelligent Capture Database may grow large with all of the report data and it is necessary to periodically purge or clear this data from the system. Purges can be configured and scheduled from Intelligent Capture Administrator.

Running Reports

Avoid running reports that use complex queries against large tables, which can put significant time and load on the databases.

Storing the SQL Server Transaction Log on a Separate Hard Drive

The SQL Server writes all transactions to the transaction log. The size of the transaction log can impact the performance of the Intelligent Capture Database negatively. Consider storing the transaction log on a separate drive controlled by a different disk controller for improved performance.

12.4 Prefetching Tasks

Prefetching tasks enables the module to have one or more additional tasks waiting to be processed, so the module does not have to wait for the Intelligent Capture Server and the network to transfer data each time it needs another task to process. The number of prefetched tasks is controlled by the *`PrefetchDefault`*INI value. The default setting is two. A few modules override this setting and make note of it in their help files.

When a module is connected to multiple servers, ScaleServer technology limits the number of tasks a module receives per server connection to *`PrefetchDefault`* divided by the number of connected servers, rounded-up to the next whole number. If rounding occurs, extra prefetched tasks may be queued up for the module. These extra prefetched tasks will be returned to the server after the timeout value in the *INI* setting *`ReleasingTasksTimer`* is reached.

Chapter 13

Recovering from System Errors, Protecting Data, and Maintaining High Availability

The Intelligent Capture Server supports both Active/Passive and Active/Active clustering for failover protection. Individual Intelligent Capture Servers or entire ScaleServer groups can be clustered to provide both high availability and failover. In addition, we strongly advise using clustering to provide high availability and failover protection for the database server platform. If the Intelligent Capture Database becomes unavailable, the entire Intelligent Capture System stops. Consider using clustering for your Intelligent Capture web servers and other key Windows services. For instructions on setting up Intelligent Capture in an MSCS cluster, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*. Other Intelligent Capture components are also compatible with clustering because their host software can be clustered. Topics in this section discuss how Intelligent Capture handles and recovers from failures not handled by high availability planning, and provide suggestions for protecting data from damage in the event of a system failure.

13.1 Automatic System Recovery

Intelligent Capture has several automatic recovery features that protect your data in the event of a system failure. System failures may be caused by software failures, a memory leak, hardware failures, power failures, network failures, or any unpredictable event that interrupts production. The effects of system failures on production can be minimized by using high availability and failover practices, as described in the *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*. Automatic recovery occurs when high availability and failover practices are not used, or when the system failure is of a nature that the failover systems cannot help, for example, a network failure between the Intelligent Capture Servers and the Intelligent Capture Database.

13.1.1 Intelligent Capture Database Unavailable

If the Intelligent Capture Database becomes unavailable for any reason, such as a power failure, system failure, or network failure, Intelligent Capture Server recovery logic is automatically initiated. In most cases, the Intelligent Capture Server will automatically recover and reconnect to the Intelligent Capture Database. No data is lost, but processing is suspended until the database becomes available.

If an error is not “critical”, the Intelligent Capture Server will continue to try and reconnect to the database every 60 seconds, unless the default is changed by an administrator. If the connection succeeds, normal processing resumes. If the connection fails, the server will wait another 60 seconds and try again to connect. However, if the Intelligent Capture Server detects a critical error when attempting to access the database, then it will not try and connect again. Instead, the server is

immediately paused and the service must be started again from the Windows **Services** panel or by typing `continue` in the console window. Although modules continue to run when the Intelligent Capture Server is paused, they do not receive any tasks until the server becomes available.

An error is considered critical if it results from a statistic log rule. These rules are used for reporting and consequently are considered more important than audit or other logging messages. When the Intelligent Capture Server receives a critical error, it performs an additional evaluation to determine if the server should enter its recovery logic. This evaluation is based on the StopOnLoggingError setting in the Tbl_ServerConfig.

13.1.2 Intelligent Capture Server Unavailable

If an Intelligent Capture Server becomes unavailable for any reason, such as a power failure, system failure, network failure, or intentional shutdown, the following Intelligent Capture Server recovery logic is automatically initiated:

- Client modules that are already connected to the Intelligent Capture Server stop receiving tasks from that server. If the module is connected to a single Intelligent Capture Server, the module will enter a "Waiting for a response from the server" state until the server again becomes available. If the module is connected to a ScaleServer group, it will continue to receive tasks from other Intelligent Capture Servers in that group. Tasks in process owned by a server that disconnects will be held and resubmitted to the Intelligent Capture Server when it reconnects.
- Client modules that are not connected to the Intelligent Capture Server cannot connect. If the unavailable server is a member of a ScaleServer group, and if the operator who is starting the module is aware of an alternative server name, then the module can be started by connecting to one of the available Intelligent Capture Servers.
- When the unavailable Intelligent Capture Server restarts, the batches that were in its memory when it became unavailable are rolled back to their last known good state. The work-in-progress information in the Intelligent Capture Database is always purged and rebuilt when an Intelligent Capture Server starts, even if the server shut down normally.
- The `Tbl_ReportTasks` table in the Intelligent Capture Database contains a column named `RTRolledBack`. If any tasks have been rolled back, this column will be flagged, enabling the Reports subsystem to be aware of rolled-back tasks.
- When an Intelligent Capture Server becomes unavailable, it may require the administrator to restart the server. To avoid production delays, install the Intelligent Capture Server as a service and set it to restart automatically.

13.1.3 Client Module Unavailable

A client module can become unavailable either through an orderly shutdown or an unexpected failure.

- When a module, including a module that is running as a service, receives a `Stop` command, it finishes processing the current task (but does not process any prefetched tasks that have not been started). The client module then stops processing and disconnects from the Intelligent Capture Server.
- When a module becomes unavailable due to an unexpected failure (system stops responding, network failure, local power failure), then from the point-of-view of the Intelligent Capture Server, the following events take place:
  - For tasks that were actively being processed by the module:
    1. The Intelligent Capture Server finishes each task with the error `IA_ERR_RETRYSOME`.
    2. The error is passed to the batch `Error` routine for the module step. If no error routine has been provided in the `IPP`, then the default error routine is invoked, which retriggers the task in question. The task is then queued for processing by the next available instance of the module.
    3. If the task is finished with an error again, the previous step repeats until the trigger variable named <*RetriesLeft*> decrements to 0. (The default is to retry the failed task 3 times.)
    4. When <*Retries Left*> = 0, the error flag of the task is set. At this point, the Intelligent Capture Server stops retriggering the task. Manual intervention is required to continue processing tasks from this batch.

    Note: If you have tasks that take a long time to complete (for example, more than five seconds), you may need to extend the *`ServiceWaitTime`* setting so that when a service is attempting to shut down gracefully, Windows does not force a shutdown because it appears that the service has stopped responding. For instructions, see "Configuring the Service Wait Time for Long-running Tasks" on page 526.
  - For tasks that were prefetched but not actively being processed by the module:
    1. The Intelligent Capture Server finishes each prefetched task with the error `IA_ERR_CANCEL`.
    2. The error is passed to the batch `Error` routine for the module step. If no error routine has been provided in the *IPP*, then the default error routine is invoked, which retriggers the task in question. The task is then queued for processing by the next available instance of the module.

Note: The `Error` event can be used to retrigger or reroute tasks as appropriate for the work flow.

13.2 Backing Up an Intelligent Capture System

This section contains information about how to back up and restore the database and the servers.

13.2.1 Backing Up and Restoring the Intelligent Capture Database

During Intelligent Capture setup and production operations, the Intelligent Capture Database is populated with both persistent and transient data. The Intelligent Capture Database should be backed up periodically. If a system failure, or accidental deletion of data, requires that you restore the database from a backup, then there are special steps you must follow to ensure a successful Intelligent Capture restart.

Some database tables hold transient data and is automatically repopulated every time Intelligent Capture Server starts. However, configuration and reporting tables hold persistent data that the Intelligent Capture Server can not automatically repair if they are corrupted or lost. Therefore it is critically important to back up the database regularly.

13.2.1.1 Backing Up the Intelligent Capture Database

Microsoft SQL Server 2005 has built-in backup tools that enable you to configure backups and back up individual databases. Configure the SQL Server to back up the Intelligent Capture Database (named `IADB` by default). It is not necessary to stop Intelligent Capture production to back up your system. For detailed instructions, see the SQL Server 2005 documentation.

13.2.1.2 Restoring the Intelligent Capture Database

After a disabling event, you may need to restore your Intelligent Capture Database, either to its original host system or to another system. When restoring, follow these steps:

To restore the Intelligent Capture Database

1. Stop the **InputAccel Server** service for all Intelligent Capture Servers.

Caution

All Intelligent Capture Servers must be stopped, not just paused. This is required because during the restore, the Work-In-Progress tables will be restored, and their data will be out of sync with the actual work in progress. After you restore the database, each Intelligent Capture Server purges its data from the Work-In-Progress tables when you restart it. This automatic purge will not happen if an Intelligent Capture Server is paused and resumed. Use the Windows Service Control Manager to stop and restart the Intelligent Capture Server.

2. Use the **Restore Database** feature in Microsoft SQL Server Management Studio to restore the Intelligent Capture Database.

3. If the database is restored to a different host computer, use Microsoft SQL Server Management Studio to create a user and password. The user you create must be mapped to the **db_owner** role for both the Intelligent Capture Database and the msdb system database. This is the user and password your Intelligent Capture Servers will use to connect to the restored database. It does not need to be the same as the user and password that were previously used.

4. If the Intelligent Capture Database is restored to a different host computer, run `DalConfig.exe` on each of your Intelligent Capture Servers. `DalConfig.exe` is located in the `binnt` folder of the Intelligent Capture Server installation folder. By default, the location is `C:\Program Files\InputAccel\Server\Server\binnt`. For the procedure on running this utility, see "Resolving SQL Server Database Connectivity Issues and Maintaining Database Access Credentials" on page 517.

5. Start each of your Intelligent Capture Servers and use Intelligent Capture Administrator to verify that each Intelligent Capture Server is working. To do this, check the **Connected** column in the **List of all registered servers** table in the **Servers** window, as explained in the section "Viewing the List of Intelligent Capture Servers" on page 115.

13.2.2 Backing Up Intelligent Capture Servers

The Intelligent Capture Server is not intended to be used as an archival system; it is designed to quickly capture, process, and export information. Although you can perform backups of the data stored by Intelligent Capture Server, a great deal of information may move in and out of the system between scheduled backups. Nevertheless, if you have a workflow in which you retain batch data for a longer period of time, then you may want to consider backing up this data periodically.

If you choose to back up the files on your Intelligent Capture Servers, you must pause the Intelligent Capture Server that you are backing up. If you are using multiple Intelligent Capture Servers in a ScaleServer group, then backing up and other maintenance operations are easy, because one Intelligent Capture Server at a time can be shut down without impacting the flow of new tasks to client modules.

Caution

Before pausing an Intelligent Capture Server, make sure that batch creation modules (ScanPlus, Standard Import, Web Services Input) are not actively creating tasks on a batch residing on the Intelligent Capture Server you are preparing to back up. Use the Windows Service Control Manager to pause and resume the Intelligent Capture Server.

To back up an Intelligent Capture Server, configure your backup software to back up the `IAS` folder and all of its subfolders. By default, this folder is located at `C:\IAS`.

Note: Configure your backup software to skip the file `IAS\ialock.txt`. This file is locked whenever the Intelligent Capture Server is running or paused, but contains no data; therefore, it is safe to skip.

IAS Folder Structure

The `IAS` folder contains several files and subfolders. The following table explains the layout of the folder structure.

Table 13-1: IAS Folder Structure

Folder	Contents	Remarks
`\IAS`	Debug logs, `values.idx` (no longer used), `batchidx.txt`, `iaslock.txt`.	Settings that were stored in`values.idx` in previous releases are now stored in the Intelligent Capture Database.
`\IAS\activation`	Stores *CAF* file activation data.	When a *CAF* file is used to activate a server, *CAF* file data is written into this directory.
`\IAS\batches`	Batch files. The 10-digit batch ID is used to create three nested folders. The top-level folder is named with digits 1-4. This folder contains a subfolder named with the digits 5-7. This subfolder contains a subfolder named with digits 8-10. For example, a batch ID of 0123456789 produces a path to the batch of `\IAS\batches\0123\456\789`. The folder lowest in the tree (`789` in our example) are the actual batch files, including the batch file (`0123456789.iab` in our example), an empty file named `guid.txt` to aid in recovery, and all batch stage files.	Batch stage files are the output files from each batch step. They are named using the hexadecimal node ID with a numeric extension indicating the stage from which they were created. For example, a node from the first step in a batch (usually the ScanPlus module's <*OutputImage*>) might be named `1c2.1`. Batches that have been deactivated are renamed with an `IAU` extension.

Folder	Contents	Remarks
`\IAS\process`	Includes a list of process files (*IAP* files) and the `Versions` folder which stores process versions. The `Versions` folder contains process folder/folders named exactly as the processes which have been uploaded to the server. In its turn, each *<<Process name>-dir>* folder contains version process folder/folders named in accordance with the automatically generated CaptureFlow version ID. Each *<<CaptureFlow version ID>-dir>* folder includes the following process files: • *IAP* file which name appears in this folder as the process version ID: *<CaptureFlow version ID>*`.iap` • `Emc.InputAccel.CodeBehind.AG`*<CaptureFlow name>*`.dll` file • *<CaptureFlow name>*`.xpp` file	If a process has been deleted, the appropriate *IAP* file is removed from `process` folder. However, the corresponded process folder in the `Versions` folder is not removed and remains unchanged.
`\IAS\temp`	Stores temporary files used by the server.	
`\IAS\modules`	Module-specific information. This includes page templates, support files, and settings used by some third-party modules.	

In addition to the files contained within the `\IAS` root folder, there are other files that should be backed up occasionally on both the Intelligent Capture Server and the client computers. The names and locations of these files are provided in the *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

13.3 Backup and Recovery Considerations for Intelligent Capture REST Services

If you have not implemented high availability for Intelligent Capture REST Services, then, at a minimum, make sure that the Intelligent Capture REST Services shared data folder is periodically or continuously backed up.

Note: The `Sessions` subfolder should not be backed up. This subfolder contains temporary session data (for example, images that were uploaded by the Intelligent Capture Web Client or other Intelligent Capture REST Service clients). Consequently, the temporary session data might not match the client's expectations after recovering from a failure and errors might occur.

If a hardware failure occurs on the system on which the shared data folder is located, then you can attempt to restore the system as follows:

Note: The shared data folder (except for the `Sessions` subfolder) should be restored to the most recent point in time before the hardware failure occurred.

1. Shut down the Intelligent Capture CWC and REST IIS server instances and Module Servers.
2. If the primary disks were corrupted, then restore the shared data folder from the latest backup.
3. If required, update the Intelligent Capture CWC and REST IIS server instances and Module Servers configurations to point to the shared data folder's new location.
4. Restart the Intelligent Capture CWC and REST IIS server instances and Module Servers.

Chapter 14

Troubleshooting

This section provides information that helps administrators troubleshoot issues in their Intelligent Capture System. For information on troubleshooting installation issues, see *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

14.1 Resolving SQL Server Database Connectivity Issues and Maintaining Database Access Credentials

Database connectivity issues can occur in the following situations:

- The configuration of the SQL Server or its host computer changes.
- The Intelligent Capture Database is renamed.
- The database user account is removed.
- The Intelligent Capture Database is backed up and then restored on a computer with a different name.

In these cases, run the Data Access Layer Configuration utility (`DalConfig.exe`) on each Intelligent Capture Server machine to establish correct connection parameters. You can also run this utility to change database credentials as required by your organization.

The Data Access Layer Configuration utility enables you to configure and test database connections. The utility is located in the `binnt` directory where the Intelligent Capture Server is installed (by default, `C:\Program Files\InputAccel\Server\Server\binnt\DalConfig64.exe`).

To use the Data Access Layer Configuration utility:

1. Run `DalConfig64.exe` from the `binnt` directory where the Intelligent Capture Server is installed. The **Data Access Layer Configuration** window displays.
2. In the **Database Type** list, select **MSSQL Server**.
3. In the **Data Source ID** list, specify **Intelligent Capture Database** to fix connection problems involving the Intelligent Capture Database.
4. In the **Data Source (Server)** field, type the name of the SQL Server to which you want to connect.
5. In the **Catalog** field, type the name of the database on the SQL Server. The default name for the Intelligent Capture Database is "IADB"; however, it can be renamed. To verify the correct name, use Microsoft SQL Server Management Console to locate the database and view its name.

6. In the **User** and **Password** fields, type the name of the user and password that the Intelligent Capture Server uses to connect to the Intelligent Capture Database. This account must have `db_owner` access to both the Intelligent Capture Database and the msdb system database.

7. Click **Test Connection** to test the connection to the database. If the connection succeeds, a message window displays indicating a successful connection. If the connection fails, an error message window displays a trace to help diagnose the error.

8. Click **Save** to save your settings.

9. Click **Done** to close the window.

10. Repeat these steps for each Intelligent Capture Server that connects to the Intelligent Capture Database.

14.2 Resolving Internal File-based Database Connectivity Issues

The internal file-based database may have connectivity issues when the files required for the internal file-based database are moved from the default `C:\IAS` folder. The required files are: `IADBConfig.data`, `IADBWip.data`, and `IADBLog.data`.

In this situation, run the Data Access Layer Configuration utility (`DalConfig64.exe`) on each Intelligent Capture Server machine to provide the correct location of these files.

The utility is located in the `binnt` directory where the Intelligent Capture Server is installed (by default, `C:\Program Files\InputAccel\Server\Server\binnt\DalConfig64.exe`).

To use the Data Access Layer Configuration utility:

1. Run `DalConfig64.exe` from the `binnt` directory where the Intelligent Capture Server is installed. The **Data Access Layer Configuration** window displays.

2. In the **Database Type** list, select **Internal Database**.

3. Browse for the location of the `IADBConfig.data` file in the **Config path** field, `IADBWip.data` file in the **WIP path** field, and the `IADBLog.data`in the **Log path** field.

4. Click **Test Connection** to test the connection to the files.

5. Click **Save** to save your settings.

6. Click **Done** to close the window.

7. Repeat these steps for each Intelligent Capture Server.

14.3 Resolving Server Connection and Performance Issues

When having problems connecting to the Intelligent Capture Servers, consider the following:

- **Startup issues**: If the database is installed, then the Intelligent Capture Database server must start before the Intelligent Capture Server can start. The Intelligent Capture Server service waits for up to 10 minutes for the Intelligent Capture Database to become available, and then gives up and fails to start. To determine the problem, check the Application Event Log on the Intelligent Capture Server machine for the following entry: `IADBConnectionFailed, Event #2210`. If this entry is present, troubleshoot the Intelligent Capture Database server to determine why it is not starting.
- **Client permissions issues**: For information about resolving client permissions issues, see "Resolving Client Permissions Issues" on page 522.
- **Host name resolution issues**: When defining or connecting to a ScaleServer group, specify one of the Intelligent Capture Servers in the group by using the name of its host computer. Do not use the IP address or "localhost" as a connection string.
- **Client user account issues**: A client module cannot connect to an Intelligent Capture Server when the module is running as a service using a local machine account, such as Network Service, unless one of the following is true:
  - The Intelligent Capture Server machine is configured to allow anonymous access.
  - The client module is running on the same machine as the Intelligent Capture Server.
  - The Intelligent Capture system is configured to use Kerberos and an *SPN* is set for the Intelligent Capture Server, as explained in the *OpenText Intelligent Capture - Installation Guide (ECPCORE-IGD)*.

The Intelligent Capture Server may encounter temporary slower performance if there are connectivity issues between the server and the Intelligent Capture Database. Often when connectivity problems occur, tables in the database that store information about batches and processes are re-populated. Depending on the number and size of batches, and the server hardware being used, the slower performance can last for a noticeable amount of time. When the re-population is complete, the server performance will return to normal. For ideas to improve server performance, see "Improving Intelligent Capture Server Performance" on page 504.

14.4 Resolving Server Permissions Issues

The account used to run the Intelligent Capture Server may not have the necessary rights and permissions. Add the user account specified for the Intelligent Capture Server service to the local *LUA* group that is created when the Intelligent Capture Server is installed: **InputAccel_Server_admin_group**. If the *LUA* group has been deleted, follow these instructions to recreate it:

1. Stop all instances of the Intelligent Capture Server service on the machine on which the group is to be created.
2. Open a command prompt window on the Intelligent Capture Server machine.
3. Type the following command line:

   ```
   ias64.exe -repair -r <datadir> -s <servicename> [-a1 <account1>]
   ```

   where:

   - *<datadir>* is the name of the Intelligent Capture Server data directory (default: `C:\IAS`).
   - *<servicename>* is the instance name of the service that runs the Intelligent Capture Server (default: `InputAccel`).
   - *a1* is the account to add to the *LUA* group. If not specified, an empty **InputAccel_Server_admin_group** group is added.

     Notes

     – Zero to one account may be added using the command line. Additional accounts may be added by using the Microsoft Management Console. To add domain accounts, specify the *a1* argument using the syntax: *<domain>**<account>*. To add local accounts, do not specify a domain.

     – Security permissions of the `IAS` data directory are updated when this command is run.

   Example: Examples

   Intelligent Capture

   - Create the *LUA* group using the default Intelligent Capture Server data directory and service instance name, adding one local user account to the group:

     ```
     ias64.exe -repair -r C:\IAS -s InputAccel -a1 dasna_o
     ```

   - Create the *LUA* group using the default Intelligent Capture Server data directory and service instance name, adding one domain user account to the group:

     ```
     ias64.exe -repair -r C:\IAS -s InputAccel -a1 federal\potus
     ```

4. Confirm *LUA* account creation by viewing **Local Users and Groups** in the Microsoft Management Console.
5. Repeat this command for each instance of the Intelligent Capture Server installed on the machine.

6. Start all instances of the Intelligent Capture Server service.

14.5 Resolving Server Startup Issues

Intelligent Capture Server needs to read certain server configuration parameters to startup. These parameters are maintained in the database. If these parameters are corrupted, then the server refuses to start. In such a situation, the parameters must be created in the registry. During the next server startup, the server reads the values from the registry and then writes the values to the database.

Follow these instructions to recreate server configuration parameters in the registry.

1. Stop all instances of the Intelligent Capture Server service on the machine where you want to fix the configuration parameters.
2. Open a command prompt window on the Intelligent Capture Server machine and change the directory to the `Server\binnt` folder of the installed Intelligent Capture. By default, this location is `C:\Program Files\InputAccel\Server\Server\binnt`. Then, type the following command line:

   Command line to write server parameters to the registry (when the server is not used in a clustered environment):

   ```
   ias64.exe -repair -s<servicename> -setRootDir <rootdir> -setTcpIpPort <tcpipport>
   ```

   Command line to write server parameters to the registry (when the server is used in a clustered environment):

   ```
   ias64.exe -repair -s<servicename> -setRootDir <rootdir> -setTcpIpPort <tcpipport> -
   setTcpIpAddress <tcpipaddress> -setTcpIpV6Address <tcpipv6address>
   ```

   where:

   - <*servicename*> is the instance name of the Intelligent Capture Server service (default: `InputAccel`). Mandatory parameter for the `-repair` command.
   - <*rootdir*> is the name of the Intelligent Capture Server folder (default: `C:\IAS`). Mandatory server configuration parameter.
   - <*tcpipport*> is the TCP/IP port number of the Intelligent Capture Server. Mandatory server configuration parameter.
   - <*tcpipaddress*> is the TCP/IP address for the IPv4 protocol. Mandatory server configuration parameter only if running the server in a Microsoft Failover Clustered environment.
   - <*tcpipv6address*> is the TCP/IP address for the IPv6 protocol. Mandatory server configuration parameter only if running the server in a Microsoft Failover Clustered environment.
3. Repeat this command for each instance of the Intelligent Capture Server installed on the machine.
4. Start all instances of the Intelligent Capture Server service.

14.6 Resolving Client Permissions Issues

Users must be assigned to user roles that have been granted appropriate permissions. Permissions are assigned in the Intelligent Capture Administrator. If a logged-in user does not have the necessary permissions, then the client module does not function as expected.

For example, every Intelligent Capture operator must be a member of a role that has been granted **Server.Login** permission. If the user does not have this permission, then the module login fails. As another example, users who install processes on Intelligent Capture Servers must belong to a role that has been granted **Server.Install.Process** permission.

Other permissions grant the system-wide ability to read batches or processes, modify batches or processes, and perform other specific system functions. Some modules have their own, specific permissions that must be granted to users who use them.

Related Topics

"Defining Roles, Role Members, and Role Permissions" on page 132

"Adding Users and Groups to Roles" on page 142

"Configuring Roles" on page 131

"Add Roles and Role Settings" on page 266

"Viewing Roles" on page 131

"Intelligent Capture Permissions List" on page 381

14.7 Resolving Documentum Advanced Export Object Retrieval Delays during Setup

By default, Documentum Advanced Export caches a maximum of 500 *ACL*s and 500 User Objects, which is adequate for common usage scenarios. However, if your repository contains a higher number of *ACL*s and User Objects, you can experience long delays (up to several hours) while the module retrieves additional objects during setup.

To correct object retrieval delays during setup:

1. On the machine where you are running the module in setup mode, close any running instances of the module (or stop the module services if applicable).

2. Use a text editor to edit the file `DocumentumAdvancedExport.dll.config` located in the `Programs Files\InputAccel\Client\Binnt` folder of your installation folder. This file is an *XML* file that configures several aspects of the module. The default file provided contains an `<appSettings>` element that looks like this:

```
<configuration>
    <appSettings>
        <add key="DisableWarningMessages" value="False" />
        <add key="PopulateMaxAcls" value="-1" />
        <add key="PopulateMaxUsers" value="-1" />
    </appSettings>
    .
    .
    .
</configuration>
```

3. The value of `-1` for `PopulateMaxAcls` and `PopulateMaxUsers` means cache the default number of objects (500). Replace these values with a positive integer greater than 500 that reflects the actual number of *ACL*s and User Objects in your repository. If you are unaware of the actual number to specify, you must experiment with progressively higher numbers until you achieve satisfactory performance in setup mode.

4. After determining the correct numbers for these values, make the same changes on all client machines where you run Documentum Advanced Export in setup mode.

14.8 Running the Intelligent Capture Server in Console Mode

Normally, the Intelligent Capture Server runs as a service. As such, you cannot view its operation in real time, only view log file entries to determine whether a problem has occurred. Sometimes it can be helpful to run the Intelligent Capture Server as an application, in which case it displays information and responds to typed commands as it runs. This mode allows an administrator to view messages in the console as they occur, rather than looking for information in the log files afterwards. Running the Intelligent Capture Server as an application can also be a useful tool during module or *IPP* development. However, in most cases you run the Intelligent Capture Server in console mode only under the advice and guidance of a support representative.

To run the Intelligent Capture Server in console mode:

1. Use the Microsoft Service Control Manager to stop the Intelligent Capture Server service.

2. Open a command prompt window and navigate to the location of the Intelligent Capture Server executable (`IAS64.EXE`) By default, this location is `C:\Program Files\InputAccel\Server\Server\binnt`.

3. At the command prompt, type `IAS64` and press **ENTER**.

The console displays a series of messages as the Intelligent Capture Server starts up. After a few moments, the message, "Intelligent Capture Server ready" displays, followed by other messages.

4. Press **ENTER** to display an `IAS>` command prompt.
5. Type the preferred command. Type `help` to see a list of commands.
6. When finished with the console session, type `quit` to stop the Intelligent Capture Server, then close the command prompt window.

Note: `IAS64.EXE` must always run under an Administrator account. In Vista operating systems with User Account Control (*UAC*) enabled, `IAS64.EXE` must be run with the administrator permissions. To elevate permissions, create a shortcut for `IAS64.EXE` and configure it to **Run as Administrator**.

The following table explains the available console mode commands:

Table 14-1: Intelligent Capture Server Console Mode Command Summary

Command	Remarks
`help`	Displays a summary of valid console mode commands.
`version`	Displays Intelligent Capture Server version information.
`pause`	Pauses the Intelligent Capture Server if it is running.
`continue`	Resumes the Intelligent Capture Server if it is paused.
`quit`	Stops the Intelligent Capture Server. If any modules are connected, this command displays a message and gives you an opportunity to cancel.

Command	Remarks
`loglevelc [<level>]`	Controls logging to the console. When specified with no parameter, displays the current logging level. To stop logging to the console, type `loglevelc 0`. This level is not a valid log level, but it restores the default log level. Sets the console logging level to the value specific in <*level*>. The level parameter is specified by adding the following level numbers to achieve the preferred logging information: 1: misc debug 2: net debug 4: console 8: info 16: warning 32: error 64: fatal
`loglevelf <level>`	Controls logging to `debug.out`. When specified with no parameter, displays the current file logging level. Sets the file logging level to the value specific in <*level*>. The <*level*> parameter is specified by adding the following level numbers to achieve the preferred logging information: 1: misc debug 2: net debug 4: console 8: info 16: warning 32: error 64: fatal

Command	Remarks
`loglevele <level>`	Controls logging to the Windows Event Log. When specified with no parameter, displays the current logging level. Sets the Windows Event Log logging level to the value specific in <*level*>. The <*level*> parameter is specified by adding the following level numbers to achieve the preferred logging information: 1: error 2: warning 4: info 8: audit success 16: audit failure 128: success
`logflush`	Clears the log.

14.9 Configuring the Service Wait Time for Long-running Tasks

For Intelligent Capture modules that run as services, the service wait time can be modified. The service wait time is the amount of time that Windows Service Control Manager waits for a module to finish a task before it pauses or stops the service.

There are several reasons to pause or stop a client service, including:

- To stop a module from executing that is causing a high load on the processor of the client computer.
- To process specific batches that have a higher priority, instead of processing batches in the order they become available.
- To stop processing all batches so that an administrator can update the *IPP*.
- To perform system maintenance on the client computer.

If you pause or stop a client service, the module finishes processing its current task before responding to the request. If the service wait time expires before the module finishes processing the task, then the module continues to run and ignores the request to pause or stop.

The default service wait time for Intelligent Capture modules is 10 minutes. To modify the service wait time, use the `ServiceWaitTimeOut:<s>` argument in the module startup command line, where <*s*> is the number of seconds to wait.

14.10 Configuring Web Services Incoming Message Request Length

By default, the Web Services subsystem uses the default incoming message request length of 4 *MB* as implemented by the underlying Microsoft ASP.NET settings. If this limited size does not meet the needs of your web services implementation, you can increase the size by using the following procedure.

To increase the default incoming message request length:

1. Open the file `WebServices.Hosting.exe.config` located in the Web Services Hosting installation folder (`C:\Program Files\InputAccel\Client\binnt`, by default).
2. Insert the following elements immediately before the last closing element (`</configuration>`):

   ```
   <system.web>
       <httpRuntime maxRequestLength="<length in kilobytes>" />
   </system.web>
   ```

   where <*length in kilobytes*> is the required integer message length; for example `10000`. (The default is "4096".)
3. Save the file.
4. Use the Windows Service Control Manager to restart the Web Services Hosting service.

Additional information on this parameter and other ASP.NET parameters can be found on the Microsoft MSDN website (`http://msdn.microsoft.com`). Search for "httpRuntime Element (ASP.NET Settings Schema)".

14.11 Troubleshooting scanning and image issues

The PixView module can assist you in troubleshooting problems when scanning pages or when processing images. This module is not directly used to administer the system or to process data.

For more information, see *OpenText Intelligent Capture - Pixview Guide (ECPCORE-TSC)*.

14.12 Troubleshooting module execution

The DLL Viewer module can assist you in troubleshooting module and process execution. This module displays a list of all 32-bit processes currently running on the machine and all of the libraries loaded by the selected process.

For more information, see *OpenText Intelligent Capture - DLL Viewer Guide (ECPCORE-TDL)*.

Chapter 15

Reports Tables

The Intelligent Capture Database contains tables that can be used to collect data for reports. These tables can also be used to write custom reports. This table provides a summary of the reports tables. For instructions on creating custom reports, see "Creating a Custom Report" on page 242.

Table 15-1: Reports Tables in the Intelligent Capture Database

Table Name	Description
"Tbl_ReportBatchDailySummary" on page 531	Contains summary information about the batch level information logged to the database based on the date that the batch was created.
"Tbl_ReportBatches" on page 532	Contains batch information.
"Tbl_ReportBatchMonthlySummary" on page 533	Contains summary information about the batch level information logged to the database based on the month that the batch was created.
"Tbl_ReportBatchWeeklySummary" on page 534	Contains summary information about the batch level information logged to the database based on the week that the batch was created.
"Tbl_ReportBatchYearlySummary" on page 535	Contains summary information about the batch level information logged to the database based on the year that the batch was created.
"Tbl_ReportCreatePages" on page 536	Contains additional information about new pages created by tasks.
"Tbl_ReportDailySummary" on page 537	Contains summary information about the events logged to the database based on the date the task was processed.
"Tbl_ReportDeletePages" on page 539	Contains information about deleted batches.
"Tbl_ReportFilesSent" on page 539	Contains information about stage files sent to a client module from the server.
"Tbl_ReportFilesWritten" on page 540	Identifies when the original image file for a page has been overwritten.
"Tbl_ReportIndexTasks" on page 541	Contains additional information about indexing tasks.

Table Name	Description
"Tbl_ReportMonthlySummary" on page 542	Contains summary information about the events logged to the database based on the month that the task was processed.
"Tbl_ReportOcrPages" on page 543	Contains additional information about pages in an *OCR* task.
"Tbl_ReportPages" on page 544	Contains information about task processing at the page level.
"Tbl_ReportScanDailySummary" on page 544	Contains summary information about the scan information logged to the database based on the day that tasks from the scanning modules are processed.
"Tbl_ReportScanMonthlySummary" on page 545	Contains summary information about the scan information logged to the database based on the month that tasks from scanning modules are processed.
"Tbl_ReportScanWeeklySummary" on page 546	Contains summary information about the scan information logged to the database based on the week that tasks from the scanning modules are processed.
"Tbl_ReportScanYearlySummary" on page 547	Contains summary information about the scan info logged to the database based on the year that tasks from scanning modules are processed.
"Tbl_ReportTasks" on page 547	Contains information about task processing.
"Tbl_ReportTemporaryFileAudit" on page 549	Contains information to be summarized in the File Audit Trail Detail Report.
"Tbl_ReportTemporaryOperatorSummary" on page 550	Contains information to be summarized in the Index Operator Summary Report.
"Tbl_ReportTemporaryPageLevelOcrSummary" on page 551	Contains information to be summarized for the Page Level Ocr Summary Report.
"Tbl_ReportTemporaryPurge" on page 552	Collects the task data to be summarized during a Purge Report Detail operation.
"Tbl_ReportTemporaryScanSummary" on page 553	Collects the data to be summarized for the Scan Summary Report.
"Tbl_ReportTemporaryUnattendedModuleSummary" on page 554	Contains information to be summarized for the Unattended Module Summary Report
"Tbl_ReportWeeklySummary" on page 554	Contains summary information about the events logged to the database based on the week the task was processed.
"Tbl_ReportYearlySummary" on page 556	Contains summary information about the events logged to the database based on the year the task was processed.

Table Name	Description
"Tbl_StatTemplate" on page 558	Stores information about the pages processed by the Extraction and Identification modules.
"Tbl_StatField" on page 559	Stores information about the fields changed in the Completion and Identification modules.
"Tbl_StatDocumentType" on page 561	Stores information about the documents processed by the Completion, Extraction, and Identification modules.
"Tbl_ReportDispatcherData Table" on page 563	Stores the main reports data (such as template, field, and operator) data.
"Tbl_ReportDispatcherParams Table" on page 566	Enables access the unique parameter key for a specific recognition project.
"Tbl_ReportDispatcherTask Table" on page 567	Stores information about the batch being processed through Advanced Recognition modules.

15.1 Tbl_ReportBatchDailySummary

This table contains summary information about the batch level information logged to the database based on the creation date of the batch. This table is updated when the user purges detailed data from the tables. One row is written for each unique day, process, and sever name each time a purge is performed. The data is then aggregated when the reports are written. Because the data might appear in different days depending upon whether the reporting is done using universal time or local time, column `BDSDateIsLocal` is used to indicate whether time is universal or local.

Table 15-2: Tbl_ReportBatchDailySummary Table

Column Name	Description	Column Type
BDSYear	Year being summarized.	int
BDSMonth	Month being summarized.	int
BDSDay	Date being summarized.	int
BDSProcess	Name of the process being summarized.	nvarchar, 256
BDSServer	Server name being summarized.	nvarchar, 400
BDSDateIsLocal	Indicates whether the time is universal or local.	bit
BDSBatchCount	Total count of batches processed on the specific date.	int
BDSPgCreated	Total count of pages created for the process and server on the specific date.	int

Column Name	Description	Column Type
BDSPgDeleted	Total count of pages deleted for the process and server on the specific date.	int
BDSPgDone	Total count of pages that completed processing for the process and server on the specific date.	int
BDSTotalBatchProcessingTime	The total batch processing time for all the batches on the specific date. The batch processing time is the total time in seconds from the time the batch was created until all pages are marked done.	int

15.2 Tbl_ReportBatches

This table contains information about batches. A row is written to the table when the Intelligent Capture Server logs a `BatchCreate` event and is updated when the server logs a `BatchSync` event, `BatchRollback` event, or `BatchDelete` event.

Table 15-3: Tbl_ReportBatches Table

Column Name	Description	Column Type
RBUUID (PK)	Unique batch ID.	nvarchar, 100
RBBatchName	Current name of the batch. If the name of the batch changes, this field is updated.	nvarchar, 256
RBProcess	Name of the process on which the batch is based.	nvarchar, 256
RBProcessUUID	Unique process ID.	nvarchar, 100
RBCreateDttm	Date and time the batch was created in universal time.	datetime
RBCreateTimeDiff	Difference between universal time and the time on the server when the batch was created.	int
RBCreateServer	Name of the server on which the batch was created.	nvarchar, 100
RBCreateExe	Executable name of the module that created the batch.	nvarchar, 100
RBCreateOperator	ID of the user that created the batch.	nvarchar, 100
RBDeleteDttm	Date and time the batch was deleted in universal time.	datetime
RBDeleteTimeDiff	Difference between universal time and the time on the server when the batch was deleted.	int

Column Name	Description	Column Type
RBDeleteExe	Executable name of the module that deleted the batch.	nvarchar, 100
RBDeleteOperator	ID of the user that deleted the batch.	nvarchar, 100
RBDeleteServer	Name of the server where the batch was deleted.	nvarchar, 100
RBCurrentServer	Name of the server that currently owns the batch. Only this server can record that the batch is deleted.	nvarchar, 100
RBLastSyncDttm	Date and time of the last sync for the batch.	datetime
RBTotalProcessingTime	Total time in seconds that it took the batch to complete processing.	nvarchar, 8
RBCreateDBDttm	Date and time the batch was created in the database time zone.	datetime
RBDeleteDBDttm	Date and time the batch was deleted in the database time zone.	datetime

15.3 Tbl_ReportBatchMonthlySummary

This table contains summary information about the batch level information logged to the database based on the month that the batch was created. This table is updated when the user purges detailed data from the tables. One row is written for each unique month, process, and sever name each time a purge is performed. The data is then aggregated when the reports are written. Because the data might appear in different months depending upon whether the reporting is done using universal time or local time, column `BMSDateIsLocal` is used to indicate if time is universal or local.

Table 15-4: Tbl_ReportBatchMonthlySummary Table

Column Name	Description	Column Type
BMSYear	Year being summarized.	int
BMSMonth	Month being summarized.	int
BMSProcess	Name of the process being summarized.	nvarchar, 256
BMSServer	Server name being summarized.	nvarchar, 400
BMSDateIsLocal	Indicates whether the time is universal or local.	bit
BMSBatchCount	Total count of batches processed during the month.	int
BMSPgCreated	Total count of pages created for the process and server during the month.	int

Column Name	Description	Column Type
BMSPgDeleted	Total count of pages deleted for the process and server during the month.	int
BMSPgDone	Total count of pages that completed processing for the process and server during the month.	int
BMSTotalBatchProcessingTime	The total batch processing time for all the batches during the month. The batch processing time is the total time in seconds from the time the batch was created until all pages are marked done.	int

15.4 Tbl_ReportBatchWeeklySummary

This table contains summary information about the batch level information logged to the database based on the week that the batch was created. This table is updated when the user purges detailed data from the tables. One row is written for each unique week, process and sever name each time a purge is performed. The data is then aggregated when the reports are written. Because the data might appear in different weeks depending upon whether the reporting is done using universal time or local time, column `BWSDateIsLocal` is used to indicate if time is universal or local.

Table 15-5: Tbl_ReportBatchWeeklySummary Table

Column Name	Description	Column Type
BWSYear	Year being summarized.	int
BWSWeek	Week being summarized.	int
BWSProcess	Name of the process being summarized.	nvarchar, 256
BWSServer	Server name being summarized.	nvarchar, 400
BWSDateIsLocal	Indicates whether the time is universal or local.	bit
BWSBatchCount	Total count of batches processed during the week.	int
BWSPgCreated	Total count of pages created for the process and server during the week.	int
BWSPgDeleted	Total count of pages deleted for the process and server during the week.	int
BWSPgDone	Total count of pages that completed processing for the process and server during the week.	int

Column Name	Description	Column Type
BWSTotalBatchProcessingTime	The total batch processing time for all the batches during the week. The batch processing time is the total time in seconds from the time the batch was created until all pages are marked done.	int

15.5 Tbl_ReportBatchYearlySummary

This table contains summary information about the batch level information logged to the database based on the year that the batch was created. This table is updated when the user purges detailed data from the tables. One row is written for each unique year, process flow & sever name each time a purge is performed. The data is then aggregated when the reports are written. Because the data might appear in different years depending upon whether the reporting is done using universal time or local time, column `BYSDateIsLocal` is used to indicate if time is universal or local.

Table 15-6: Tbl_ReportBatchYearlySummary Table

Column Name	Description	Column Type
BYSYear	Year being summarized.	nvarchar, 256
BYSProcess	Name of the process being summarized.	nvarchar, 400
BYSServer	Server name being summarized.	bit
BYSDateIsLocal	Indicates whether the time is universal or local.	int
BYSBatchCount	Total count of batches processed during the year.	int
BYSPgCreated	Total count of pages created for the process and server during the year.	int
BYSPgDeleted	Total count of pages deleted for the process and server during the year.	int
BYSPgDone	Total count of pages that completed processing for the process and server during the year.	int
BYSTotalBatchProcessingTime	The total batch processing time for all the batches during the year. The batch processing time is the total time in seconds from the time the batch was created until all pages are marked done.	int

15.6 Tbl_ReportCreatePages

This table contains additional information about new pages created by tasks. One or more rows are written to the table when the Intelligent Capture Server logs a `TaskDone` event. The Tbl_ReportCreatePages table joins with the Tbl_ReportBatches table using the `RCPBatchUUID` field.

Table 15-7: Tbl_ReportCreatePages Table

Column Name	Description	Column Type	Relates to
RCPBatchUUID (PK) (FK)	Unique ID for the batch.	nvarchar, 100	Tbl_ReportBatches.RBUUID
RCPNodeId (PK)	Node ID of the page.	int	
RCPSource	Source information for the new page. New modules that create pages save some source information for newly created pages.	nvarchar, 200	
RCPNodeOrdinal	Node ordinal.	int	
RCPStageFile	Number of the stage file for the original image.	int	
RCPRescanNode	If this page replaced another page by rescanning, this contains a 1. Otherwise this field is null.	int	
RCPScanNode	If this page was created by a scanning module, this contains 1. Otherwise this field is null.	int	
RCPScanMilliseconds	If this page was created by a scanning module, this contains the time for scanning in milliseconds.	int	
RCPCreateDttm	Date and time in universal time that the node was created.	datetime	
RCPCreateTimeDiff	Difference between universal time and the local time on the server when the node was created.	datetime	
RCPModule	Executable name of the module that created the node.	nvarchar, 100	
RCPOperator	Name of the operator logged into the module that created the node.	nvarchar, 100	
RCPMachine	Name of the computer running the module that created the node.	nvarchar, 400	
RCPCreateServer	Name of the server on which the node was created.	nvarchar, 100	

Column Name	Description	Column Type	Relates to
RCPDoneDttm	Date and time that the node finished processing in universal time.	datetime	
RCPNodeDone	A bit that indicates that the node finished processing.	bit	
RCPAttended	A bit that indicates whether the module that created the page was an attended module.	bit	
RCPCreateDBDttm	Date and time that the node was created in the database time zone.	datetime	

15.7 Tbl_ReportDailySummary

This table contains summary information about the events logged to the database based on the date the task was processed. This table is updated when the user purges detailed data from the tables. One row is written for each task with a unique day, process, module, user, and computer each time a purge is performed. The data is then aggregated when the reports are written. Because the data might appear in different days depending upon whether the reporting is done using universal time or local time, column `DSDateIsLocal` is used to indicate whether time is universal or local.

Table 15-8: Tbl_ReportDailySummary Table

Column Name	Description	Column Type
DSYear	The year being summarized.	int
DSMonth	The month being summarized.	int
DSDay	The date being summarized.	int
DSDateIsLocal	Indicates whether the time is universal or local.	bit
DSProcess	Name of the process for which the tasks are summarized.	nvarchar, 256
DSServer	Name of the server being summarized.	nvarchar, 400
DSModule	Executable name of the module being summarized.	nvarchar, 100
DSStep	Name of the step in the process being summarized.	nvarchar, 512
DSMachine	Name of the computer processing the functionality being summarized.	nvarchar, 400
DSUser	Name of the user performing the functionality being summarized.	nvarchar, 100

Column Name	Description	Column Type
DSBatchCount	Total count of batches processed on the specific date.	int
DSTaskCount	Total count of tasks processed by the process, module step, computer, and user on the specific date.	int
DSDocCount	Total count of documents processed by the process, module step, computer, and user on the specific date.	int
DSPageCount	Total count of pages processed by the process, module step, computer, and user on the specific date.	int
DSTotalTime	Total time (in milliseconds) spent by the process, module step, computer, and user to process tasks on the specific date.	int
DSPageTime	Total time (in milliseconds) spent by the process, module step, computer, and user to process the page on the specific date.	int
DSOcrChars	(*OCR* modules only) Total count of the characters analyzed by the process, module step, computer, and user on the specific date.	int
DSOcrRecChars	(OCR modules only) Total count of the characters recognized by the process, module step, computer, and user on the specific date.	int
DSOcrRejChars	(OCR modules only) Total count of the characters rejected by the process, module step, computer, and user on the specific date.	int
DSIdxCharCnt	(Index modules only) Total count of the characters typed by the user for the process, module step, and computer on the specific date.	int
DSIdxFieldCnt	(Index modules only) Total count of the fields processed by the user for the process, module step, and computer on the specific date.	int
DSKeyTime	(Index modules only) Total time (in milliseconds) spent by the user keying data for the process, module step, and computer on the specific date.	int

15.8 Tbl_ReportDeletePages

This table contains information about deleted pages. One row is written to the table when the Intelligent Capture Server logs a `NodeDeleted` event for a page. Nodes can be deleted outside of a task.

Table 15-9: Tbl_ReportDeletePages Table

Column Name	Description	Column Type	Relates to
RDPBatchUUID (PK) (FK)	Unique ID for the batch containing the deleted page.	nvarchar, 100	Tbl_ReportBatches.RBUUID
RDPNodeId (PK)	Node ID of the deleted node.	int	
RDPModule	Executable name of the module that deleted the node.	nvarchar, 100	
RDPOrdinal	Ordinal of the page within the task.	int	
RDPDeleteServer	Intelligent Capture Server on which the node was deleted.	nvarchar, 100	
RDPOperator	Name of the user logged into the module that deleted the node.	nvarchar, 100	
RDPMachine	Computer on which the module that deleted the node was executing.	nvarchar, 400	
RDPDeleteDttm	Date and time in universal time that the page was deleted.	datetime	
RDPDeleteTimeDiff	Difference between universal time and the time on the server when the page was deleted.	int	
RDPDeleteDBDttm	Date and time the node was deleted in the database time zone.	datetime	

15.9 Tbl_ReportFilesSent

This table contains information about stage files sent to a module from the server.

Table 15-10: Tbl_ReportFilesSent Table

Column Name	Description	Column Type	Relates to
RFSBatchUUID (FK)	Unique ID for the batch.	nvarchar, 100	Tbl_ReportBatches.RBUUID
RFSModule	Executable name of the module that was sent the file.	nvarchar, 100	

Column Name	Description	Column Type	Relates to
RFSOperator	Name of the user logged into the module that was sent the file.	nvarchar, 100	
RFSMachine	Name of the computer which was running the module that was sent the file.	nvarchar, 400	
RFSServerName	Name of the server that sent the file.	nvarchar, 100	
RFSNodeId	Node ID of the stage file.	int	
RFSNodeOrdinal	Ordinal of the node within the batch.	int	
RFSFileNo	Number of the stage file that was sent.	int	
RFSSentDttm	Date and time in universal time that the file was sent.	datetime	
RFSSentDateDiff	Difference between universal time and the time on the server when the file was sent.	int	
RFSSentDBDttm	Date and time the file was sent in the database time zone.	datetime	

15.10 Tbl_ReportFilesWritten

This table is used to identify when the original image file for a page has been overwritten, and therefore, does not contain entries for every stage file that is written.

Table 15-11: Tbl_ReportFilesWritten Table

Column Name	Description	Column Type	Relates to
RFWBatchUUID (FK)	Unique ID for the batch.	nvarchar, 100	Tbl_ReportBatches.RBUUID
RFWNodeId	Node ID of the stage file.	int	
RFWNodeOrdinal	Ordinal for the node within the batch.	int	
RFWModule	Executable name of the module that wrote the file.	nvarchar, 100	

Column Name	Description	Column Type	Relates to
RFWOperator	Name of the user logged into the module that wrote the file.	nvarchar, 100	
RFWMachine	Name of the computer running the module that wrote the file.	nvarchar, 400	
RFWServerName	Name of server on which the file was written.	nvarchar, 100	
RFWFileNo	Number of the stage file that was written.	int	
RFWWrittenDttm	Date and time in universal time that the file was written.	datetime	
RFWWrittenDateDiff	Difference between universal time and the time on the server when the file was written.	int	
RFWWrittenDBDttm	Date and time the file was written in the database time zone.	datetime	

15.11 Tbl_ReportIndexTasks

This table contains additional information about indexing tasks. One row is written to the table when the Intelligent Capture Server logs a `TaskDone` event. The Tbl_ReportIndexTasks table joins with the Tbl_ReportTasks table using the `RITTaskUUId` field.

Table 15-12: Tbl_ReportIndexTasks Table

Column Name	Description	Column Type
RITTaskUUId (PK)	Unique ID for the indexing task.	nvarchar, 100
RITDocCount	Number of documents processed by the task.	int
RITCharCount	Total number of characters entered for the task if the module returns this information in an IAValue.	int
RITKeyTime	Keying time for the task if the module returns this information in an IAValue.	int
RITFieldCount	Number of fields processed by the task if the module returns this information in an IAValue.	int

15.12 Tbl_ReportMonthlySummary

This table contains summary information about the events logged to the database based on the month that the task was processed. This table is updated when the user purges detailed data from the tables. One row is written for each task with a unique month, process, module, user, and computer name each time a purge is performed. The data is then aggregated when the reports are written. Because the data might appear in different months depending upon whether the reporting is done using universal time or local time, column `MSDateIsLocal` is used to indicate whether time is universal or local.

Table 15-13: Tbl_ReportMonthlySummary Table

Column Name	Description	Column Type
MSYear	The year being summarized.	int
MSMonth	The month being summarized.	int
MSDateIsLocal	Indicates whether the time is universal or local.	bit
MSProcess	Name of the process for which the tasks are summarized.	nvarchar, 256
MSServer	Name of the server being summarized.	nvarchar, 400
MSModule	Executable name of the module being summarized.	nvarchar, 100
MSStep	Name of the step in the process being summarized.	nvarchar, 512
MSMachine	Name of the computer processing the functionality being summarized.	nvarchar, 400
MSUser	Name of the user performing the functionality being summarized.	nvarchar, 100
MSBatchCount	Total count of batches processed during the month.	int
MSTaskCount	Total count of tasks processed by the process, module step, computer, and user during the month.	int
MSDocCount	Total count of documents processed by the process, module step, computer, and user during the month.	int
MSPageCount	Total count of pages processed by the process, module step, computer, and user during the month.	int
MSTotalTime	Total time (in milliseconds) spent by the process, module step, computer, and user to process tasks during the month.	int

Column Name	Description	Column Type
MSPageTime	Total time (in milliseconds) spent by the process, module step, computer, and user to process pages during the month.	int
MSOcrChars	(*OCR* modules only) Total count of the characters analyzed by the process, module step, computer, and user during the month.	int
MSOcrRecChars	(OCR modules only) Total count of the characters recognized by the process, module step, computer, and user during the month. *Column Type*: int.	int
MSOcrRejChars	(OCR modules only) Total count of the characters rejected by the process, module step, computer, and user during the month.	int
MSIdxCharCnt	(Index modules only) Total count of the characters typed by the user for the process, module step, and computer during the month.	int
MSIdxFieldCnt	(Index modules only) Total count of the fields processed by the user for the process, module step, and computer during the month.	int
MSIdxKeyTime	(Index modules only) Total time (in milliseconds) spent by the user keying data for the process, module step, and computer during the month.	int

15.13 Tbl_ReportOcrPages

This table contains additional information about pages in an *OCR* task. One or more rows are written to the table when the Intelligent Capture Server logs a `TaskDone` event. The Tbl_ReportOcrPages table joins with the Tbl_ReportPages table using the `ROPTaskUUId` and `ROPNodeId` fields.

Table 15-14: Tbl_ReportOcrPages Table

Column Name	Description	Column Type
ROPTaskUUID (PK)	Unique ID for the *OCR* task.	nvarchar, 100
ROPNodeId (PK)	Node ID for the page processed by the *OCR* task.	int
ROPCharCount	Number of characters recognized on the page.	int
ROPRejected	Number of characters on the page that were rejected.	int

15.14 Tbl_ReportPages

This table contains information about task processing at the page level. One or more rows are written to the table when the Intelligent Capture Server logs a `TaskFinish` event. The Tbl_ReportPages table joins with the Tbl_ReportTasks table using the `RPTaskUUId` field.

Table 15-15: Tbl_ReportPages table

Column Name	Description	Column Type	Relates to
RPTaskUUId (PK) (FK)	Unique ID for the task that processed the page.	nvarchar, 100	Tbl_ReportTasks.RTTaskUUID
RPNodeID (PK)	Node ID of the page.	int	
RPOrdinal	Ordinal of the page within the task.	int	
RPResult	Result of the page processing, if returned by the module in an IAValue. 0=Success 1=Failure.	int	
RPProcTime	Processing time for the page in milliseconds if returned by the module in an IAValue.	int	

15.15 Tbl_ReportScanDailySummary

This table contains summary information about the scan information logged to the database based on the date that tasks from scanning modules are processed. This table is updated when the user purges detailed data from the tables. One row is written for each unique day, sever name, operator, and computer each time a purge is performed. The data is then aggregated when the reports are written. Because the data might appear in different days depending upon whether the reporting is done using universal time or local time, column `SDSDateIsLocal` is used to indicate whether time is universal or local.

Table 15-16: Tbl_ReportScanDailySummary Table

Column Name	Description	Column Type
SDSYear	Year being summarized.	int
SDSMonth	Month being summarized.	int
SDSDay	Date being summarized.	int
SDSServer	Server name being summarized.	nvarchar, 400
SDSOperator	Name of the operator that scanned the pages.	nvarchar, 100
SDSMachine	Name of the computer on which the pages were scanned.	nvarchar, 400
SDSDateIsLocal	Indicates whether the time is universal or local.	bit

Column Name	Description	Column Type
SDSBatchCount	Total count of batches processed on the specific date.	int
SDSRescan	Total count of the pages on the server that were rescanned by the operator on the computer on the specific date.	int
SDSScan	Total count of pages on the server that were scanned by the operator on the computer on the specific date.	int
SDSTotalScanTime	Total time in milliseconds spent by the operator to scan pages on the computer on the specific date.	int

15.16 Tbl_ReportScanMonthlySummary

This table contains summary information about the scan information logged to the database based on the month when tasks from scanning modules are processed. This table is updated when the user purges detailed data from the tables. One row is written for each unique month, sever name, operator, and computer each time a purge is performed. The data is then aggregated when the reports are written. Because the data might appear in different days depending upon whether the reporting is done using universal time or local time, column `SDSDateIsLocal` is used to indicate whether time is universal or local.

Table 15-17: Tbl_ReportScanMonthlySummary Table

Column Name	Description	Column Type
SMSYear	Year being summarized.	int
SMSMonth	Month being summarized.	int
SMSServer	Server name being summarized.	nvarchar, 400
SMSOperator	Name of the operator that scanned the pages.	nvarchar, 100
SMSMachine	Name of the computer on which the pages were scanned.	nvarchar, 400
SMSDateIsLocal	Indicates whether the time is universal or local.	bit
SMSBatchCount	Total count of batches processed during the month.	int
SMSRescan	Total count of the pages on the server that were rescanned by the operator on the computer during the month.	int
SMSScan	Total count of pages on the server that were scanned by the operator on the computer during the month.	int

Column Name	Description	Column Type
SMSTotalScanTime	Total time in milliseconds spent by the operator to scan pages on the computer during the month.	int

15.17 Tbl_ReportScanWeeklySummary

This table contains summary information about the scan information logged to the database based on the week that tasks from scanning modules are processed. This table is updated when the user purges detailed data from the tables. One row is written for each unique week, sever name, operator, and computer each time a purge is performed. The data is then aggregated when the reports are written. Because the data might appear in different days depending upon whether the reporting is done using universal time or local time, column `SDSDateIsLocal` is used to indicate whether time is universal or local.

Table 15-18: Tbl_ReportScanWeeklySummary Table

Column Name	Description	Column Type
SWSYear	Year being summarized.	int
SWSWeek	Week being summarized.	int
SWSServer	Server name being summarized.	nvarchar, 400
SWSOperator	Name of the operator that scanned the pages.	nvarchar, 100
SWSMachine	Name of the computer on which the pages were scanned.	nvarchar, 400
SWSDateIsLocal	Indicates whether the time is universal or local.	bit
SWSBatchCount	Total count of batches processed during the week.	int
SWSRescan	Total count of the pages on the server that were rescanned by the operator on the computer during the week.	int
SWSScan	Total count of pages on the server that were scanned by the operator on the computer during the week.	int
SWSTotalScanTime	Total time in milliseconds spent by the operator to scan pages on the computer during the week.	int

15.18 Tbl_ReportScanYearlySummary

This table contains summary information about the scan information logged to the database based on the year that tasks from scanning modules are processed. This table is updated when the user purges detailed data from the tables. One row is written for each unique year, sever name, operator, and computer each time a purge is performed. The data is then aggregated when the reports are written. Because the data might appear in different days depending upon whether the reporting is done using universal time or local time, column `SDSDateIsLocal` is used to indicate whether time is universal or local.

Table 15-19: Tbl_ReportScanYearlySummary Table

Column Name	Description	Column Type
SYSYear	Year being summarized.	int
SYSServer	Server name being summarized.	nvarchar, 400
SYSOperator	Name of the operator that scanned the pages.	nvarchar, 100
SYSMachine	Name of the computer on which the pages were scanned.	nvarchar, 400
SYSDateIsLocal	Indicates whether the time is universal or local.	bit
SYSBatchCount	Total count of batches processed during the year.	int
SYSRescan	Total count of the pages on the server that were rescanned by the operator on the computer during the year.	int
SYSScan	Total count of pages on the server that were scanned by the operator on the computer during the year.	int
SYSTotalScanTime	Total time in milliseconds spent by the operator to scan pages on the computer during the year.	int

15.19 Tbl_ReportTasks

This table contains information about task processing. A row is written to the table when the Intelligent Capture Server logs a `TaskFinish` event.

Table 15-20: Tbl_ReportTasks Table

Column Name	Description	Column Type	Relates to
RTTaskUUID (PK)	Unique task ID.	nvarchar, 100	Tbl_ReportTasks.RTTaskUUID

Column Name	Description	Column Type	Relates to
RTBatchUUID (FK)	Unique ID for the batch associated with the task.	nvarchar, 100	Tbl_ReportBatches.RBUUID
RTServerName	Name of the Intelligent Capture Server that contains the batch at the time the task was run. Note that this may be different from the server where the batch was created.	nvarchar, 100	
RTStartDttm	The date and time the task was sent to the module for execution in universal time.	datetime	
RTEndDttm	The date and time the task was returned by the module after execution in universal time.	datetime	
RTDateDiff	The difference between universal time and the local time on the server when the task was run.	int	
RTNodeID	The node ID of the node that was the trigger for the task.	int	
RTLevel	Level of the node that was the trigger for the task.	nvarchar, 100	
RTLevelNumber	Level number of the node that was the trigger for the task.	int	
RTOrdinal	Ordinal of the node that was the trigger for the task at its level within the batch (example: document 3).	int	
RTStep	Name of the step that executed the task.	nvarchar, 512	
RTModule	The executable name of the module that executed the task.	nvarchar, 100	
RTMachine	Name of the computer on which the task was executed.	nvarchar, 400	
RTOperator	Name of the user logged into the module that executed the task.	nvarchar, 100	
RTTaskTimeServer	The time in milliseconds from the time the server sent the task until it received the task result.	int	
RTTaskTimeValue	Task time in milliseconds returned by the task in an IAValue, if any.	int	
RTPageCount	Number of pages processed for the task.	int	
RTReturnValue	Task result. 0=Success 1=Failure.	bit	

Column Name	Description	Column Type	Relates to
RTResult	Error number returned from the task, if any. Not all modules return the error number.	int	
RTRolledBack	Indicates if the task was rolled back after it completed.	int	
RTStartDBDttm	Date and time the task was sent to the client module in the database time zone.	datetime	
RTEndDBDttm	Date and time the task was returned from the client module in the database time zone.	datetime	

15.20 Tbl_ReportTemporaryFileAudit

This table is used for collecting data to be summarized in the File Audit Trail Detail Report. The data for the report must be collected using multiple queries and is combined for the report. The data is kept in the table only while being prepared for the report. After the data has been prepared, it is deleted from the table. Because multiple users can be running the report at the same time, the rows for each request are identified by a unique column that identifies the data for a particular request.

Table 15-21: Tbl_ReportTemporaryFileAudit Table

Column name	Description	Column Type
RTUniqueID	Unique ID for a specific request.	nvarchar, 80
RTCreateLocalDate	Date and time that the batch was created in local time.	datetime
RTProcess	Name of the process for the task.	nvarchar, 400
RTBatchName	Name of the batch for the task.	nvarchar, 400
RTStep	Name of the step for the task	nvarchar, 400
RTNodeId	Node ID of the node processed by the task.	int
RTNodeOrdinal	Ordinal number (page number) of the node when it was processed by the task.	int
RTSource	Source string for the page when it was created.	nvarchar, 200
RTOperator	Operator who executed the task.	nvarchar, 100
RTStartDttm	Date and time the task was started in local time (time zone of the database).	datetime
RTEndDttm	Date and time the task was completed in local time (time zone of the database).	datetime
RTReturnValue	0 if the task was successful; 1 if the task was not successful.	int

Column name	Description	Column Type
RTCreated	>0 if the task created the page; 0 if it did not.	int
RTDeleted	>0 if the task deleted the page; 0 if it did not.	int
RTSent	>0 if the image file was sent to the task; 0 if no image was sent (this is important for task processed by an attended module).	int
RTNodeDone	1 if the page was processed by IADone; 0 if it was not.	int
RTWritten	>0 if the task overwrote the original image file; 0 if it did not.	int
RTAttended	>0 if the module processing the task is an attended module; 0 if it is not.	int
RTModuleName	Module Name of the module who processed the task. This may be either the Module Short Name or the Module Name depending on the parameters passed to the report.	nvarchar, 200
RTCreateLocalDttm	Date and time that the batch was created in the time zone of the database.	datetime

15.21 Tbl_ReportTemporaryOperatorSummary

This table is used for collecting data to be summarized in the Index Operator Summary Report. The data for the report must be summarized from the detail data and also from the summarized data, then the two summaries are combined for the report. The data is kept in the table only while being prepared for the report. After the data has been prepared, it is deleted from the table. Because multiple users can be running the report at the same time, the rows for each request are identified by a unique column that identifies the data for a particular request.

Table 15-22: Tbl_ReportTemporaryOperatorSummary Table

Column name	Description	Column Type
RTUniqueID	Unique ID for a particular request.	nvarchar, 80
RTOperator	User name of the operator being summarized.	nvarchar, 400
RTYear	Year being summarized.	int
RTMonthOrWeek	Month or week being summarized.	int
RTDay	Day being summarized.	int
RTProcess	Name of the process being summarized.	nvarchar, 256
RTStep	Name of the step being summarized.	nvarchar, 512
RTTaskCount	Number of tasks for the step, operator and date.	int

Column name	Description	Column Type
RTPageCount	Number of pages for the step, operator and date.	int
RTDocCount	Number of documents processed for the Step, Operator and date.	int
RTCharCount	Number of characters typed for the step, operator and date.	int
RTTotalTime	Number of milliseconds to process the tasks for the step, operator and date.	int
RTKeyTime	Number of milliseconds used for keying index data for the step, operator and date.	int
RTFieldCount	Number of fields for the step, operator and date.	int

15.22 Tbl_ReportTemporaryPageLevelOcrSummary

This table is used for collecting the data to be summarized for the Page Level Ocr Summary Report. The data for the report must be summarized from the detail data and also from the summarized data, then the two summaries are combined for the report. The data is kept in the table only while being prepared for the report. After the data has been prepared, it is deleted from the table. Because multiple users can be running the report at the same time, the rows for each request are identified by a unique column that identifies the data for a particular request.

Table 15-23: Tbl_ReportTemporaryPageLevelOcrSummary Table

Column name	Description	Column Type
RTUniqueID	Unique ID for a specific request.	nvarchar, 80
RTYear	Year being summarized.	int
RTMonthOrWeek	Month or week being summarized.	int
RTDay	Day being summarized.	int
RTProcess	Name of the process being summarized.	nvarchar, 250
RTMachine	Name of the workstation being summarized.	nvarchar, 400
RTModule	Name of the module being summarized.	nvarchar, 200
RTPageCount	Number of pages for the process, workstation, module, and date.	int
RTTotalTime	Number of milliseconds to process the tasks for the process, workstation, module, and date.	int
RTOcrChars	Number of total characters for the process, workstation, module, and date.	int

Column name	Description	Column Type
RTRecognized	Number of characters recognized for the process, workstation, module, and date.	int

15.23 Tbl_ReportTemporaryPurge

This table is used for collecting the task data to be summarized during a Purge Report Detail operation. The data is kept in the table only during the purge itself. After it has been summarized, the data is deleted.

Table 15-24: Tbl_ReportTemporaryPurge Table

Column Name	Description	Column Type
RTPPurgeTime	Key that identifies all of the rows in this purge.	datetime
RTPTaskUUID	Unique task ID.	nvarchar, 100
RTPTaskDttm	Date and time the task was processed.	datetime
RTPTimeDiff	Difference between the local time and universal time on the task computer.	int
RTPProcess	Name of the process for the task.	nvarchar, 256
RTPServer	Server where the task was processed.	nvarchar, 400
RTPModule	Module that processed the task.	nvarchar, 100
RTPStep	Step name in the process for the task.	nvarchar, 512
RTPMachine	Computer on which the task was processed.	nvarchar, 400
RTPUser	User logged into the module that processed the task.	nvarchar, 100
RTPBatchUUID	Unique batch ID.	nvarchar, 256
RTPDocCount	Count of documents returned by IndexPlus for the task if the module for the task was IndexPlus.	int
RTPPageCount	Count of pages processed by the task.	int
RTPTotalTime	Processing time for the task.	int
RTPPageTime	Processing time for each page.	int
RTPOcrChars	(*OCR* modules only) Number of characters processed for the task.	int
RTPOcrRecChars	(*OCR* modules only) Number of characters recognized for the task.	int
RTPOcrRejChars	(*OCR* modules only) Number of characters rejected for the task.	int
RTPIdxCharCnt	(Index modules only) Number of characters typed by the user for the task.	int

Column Name	Description	Column Type
RTPIdxFieldCnt	Number of fields for the task if the task was for the IndexPlus module.	int
RTPIdxKeyTime	Time spent keying in data, if the task was for the IndexPlus module.	int
RTPTaskDBDttm	Date and time the task was processed in the database time zone.	datetime

15.24 Tbl_ReportTemporaryScanSummary

This table is used for collecting the data to be summarized for the Scan Summary Report. The data for the report is summarized from the detail data and also from the summarized data, then the two summaries are combined for the report. The data is kept in the table only while being prepared for the report. After the data has been prepared, it is deleted from the table. Because multiple users can be running the report at the same time, the rows for each request are identified by a unique column that identifies the data for a particular request.

Table 15-25: Tbl_ReportTemporaryScanSummary Table

Column Name	Description	Column Type
RTUniqueID	Unique ID for a particular request.	nvarchar, 80
RTMachineOrOperator	Name of the computer or operator being summarized.	nvarchar, 400
RTYear	Year being summarized.	int
RTMonthOrWeek	Month or week being summarized.	int
RTDay	Day being summarized.	int
RTBatchCount	Number of batches for the Computer/Operator and date.	int
RTPageCount	Number of pages scanned for the Computer/ Operator and date.	int
RTRescanCount	Number of pages rescanned for the Computer/ Operator and date.	int
RTTotalTime	Total time in milliseconds for the Computer/ Operator and date.	int

15.25 Tbl_ReportTemporaryUnattendedModuleSummary

This table is used for collecting the data to be summarized for the Unattended Module Summary Report. The data for the report must be summarized from the detail data and also from the summarized data, then the two summaries are combined for the report. The data is kept in the table only while being prepared for the report. After the data has been prepared, it is deleted from the table. Because multiple users can be running the report at the same time, the rows for each request are identified by a unique column that identifies the data for a particular request.

Table 15-26: Tbl_ReportTemporaryUnattendedModuleSummary Table

Column name	Description	Column Type
RTUniqueID	Unique ID for a specific request.	nvarchar, 80
RTYear	Year being summarized.	int
RTMonthOrWeek	Month or week being summarized.	int
RTDay	Day being summarized.	int
RTProcess	Name of the process being summarized.	nvarchar, 256
RTMachine	Name of the workstation being summarized.	nvarchar, 400
RTModule	Name of the module being summarized.	nvarchar, 200
RTPageCount	Number of pages for the process, workstation, module, and date.	int
RTTotalTime	Number of milliseconds to process the tasks for the process, workstation, module, and date.	int

15.26 Tbl_ReportWeeklySummary

This table contains summary information about the events logged to the database on the week that the task was processed. This table is updated when the user purges detailed data from the tables. One row is written for each task with a unique week, process, module, user, and computer each time a purge is performed. The data is then aggregated when the reports are written. Because the data might appear in different weeks depending upon whether the reporting is done using universal time or local time, column `WSDateIsLocal` is used to indicate whether time is universal or local.

The day that marks the beginning of the week is a database setting that can be set globally for the database. This table will base the week begin dates using this global setting.

Table 15-27: Tbl_ReportWeeklySummary Table

Column Name	Description	Column Type
WSYear	The year being summarized.	int
WSWeek	The week being summarized.	int
WSDateIsLocal	Indicates whether the time is universal or local.	bit
WSProcess	Name of the process being summarized.	nvarchar, 256
WSServer	Name of the server being summarized.	nvarchar, 400
WSModule	Name of the executable for the module being summarized.	nvarchar, 100
WSStep	Name of the step in the process being summarized.	nvarchar, 512
WSMachine	Name of the computer being summarized.	nvarchar, 400
WSUser	Name of the user being summarized.	nvarchar, 100
WSBatchCount	Total count of batches processed during the specific week.	int
WSTaskCount	Total count of tasks processed by the process, module step, computer, and user during the specific week.	int
WSDocCount	Total count of documents processed by the process, module step, computer, and user during the specific week.	int
WSPageCount	Total count of pages processed by the process, module step, computer, and user during the specific week.	int
WSTotalTime	Total time (in milliseconds) spent by the process, module step, computer, and user to process tasks during the specific week.	int
WSPageTime	Total time (in milliseconds) spent by the process, module step, computer, and user to process pages during the specific week.	int
WSOcrChars	(*OCR* modules only) Total count of the characters analyzed by the process, module step, computer, and user during the specific week.	int
WSOcrRecChars	(*OCR* modules only) Total count of the characters recognized by the process, module step, computer, and user during the specific week.	int

Column Name	Description	Column Type
WSOcrRejChars	(*OCR* modules only) Total count of the characters rejected by the process, module step, computer, and user during the specific week.	int
WSIdxCharCnt	(Index modules only) Total count of the characters typed by the user for the process, module step, and computer during the specific week.	int
WSIdxFieldCnt	(Index modules only) Total count of the fields processed by the user for the process, module step, and computer during the specific week.	int
WSKeyTime	(Index modules only) Total time (in milliseconds) spent by the user keying data for the process, module step, and computer during the specific week.	int

15.27 Tbl_ReportYearlySummary

This table contains summary information about the events logged to the database based on the year that the task was processed. This table is updated when the user purges detailed data from the tables. One row is written for each task with a unique year, process, module, user & machine each time a purge is performed. The data is then aggregated when the reports are written. Because the data might appear in different years depending upon whether the reporting is done using universal time or local time, column `YSDateIsLocal` is used to indicate whether time is universal or local.

Table 15-28: Tbl_ReportYearlySummary Table

Column Name	Description	Column Type
YSYear	The year being summarized.	int
YSDateIsLocal	Indicates whether the time is universal or local.	bit
YSProcess	Name of the process being summarized.	nvarchar, 256
YSServer	Name of the server being summarized.	nvarchar, 400
YSModule	Name of the executable for the module being summarized.	nvarchar, 100
YSStep	Name of the step in the process being summarized.	nvarchar, 512
YSMachine	Name of the computer being summarized.	nvarchar, 400
YSUser	Name of the user being summarized.	nvarchar, 100
YSBatchCount	Total count of batches processed during the year.	int

Column Name	Description	Column Type
YSTaskCount	Total count of tasks processed by the process, module step, computer, and user during the year.	int
YSDocCount	Total count of documents processed by the process, module step, computer, and user during the year.	int
YSPageCount	Total count of pages processed by the process, module step, computer, and user during the year.	int
YSTotalTime	Total time (in milliseconds) spent by the process, module step, computer, and user to process tasks during the year.	int
YSPageTime	Total processing time (in milliseconds) for each page processed by the process, module step, machine and user.	int
YSOcrChars	(*OCR* modules only) Total count of the characters analyzed by the process, module step, computer, and user during the year.	int
YSOcrRecChars	(*OCR* modules only) Total count of the characters recognized by the process, module step, computer, and user during the year.	int
YSOcrRejChars	(*OCR* modules only) Total count of the characters rejected by the process, module step, computer, and user during the year.	int
YSIdxCharCnt	(Index modules only) Total count of the characters typed by the user for the process, module step, and computer during the year.	int
YSIdxFieldCnt	(Index modules only) Total count of the fields processed by the user for the process, module step, and computer during the year.	int
YSKeyTime	(Index modules only) Total time (in milliseconds) spent by the user keying data for the process, module step, and computer during the year.	int

15.28 Tbl_StatTemplate

This table stores information about pages processed by the Extraction and Identification modules. If an Extraction template is not identified for the page or if Extraction for a page fails due to run-time exceptions, then template statistics are saved for that page.

This data provides users with classification and extraction results for a specified recognition template. Information is divided by the CaptureFlow to separate the reporting by line-of-business in cases where templates are shared.

Notes

- The running module creates new records as required, but no more than one record per hour. The cumulative statistics for a given date and hour is calculated by aggregating all rows for the specified duration. For example, the number of pages processed by the Extraction module on 1/23/2012 between 10:00 and 11:00 is the total of all records where the Date is set to "1/23/2012 10:00".
- The columns with **Descriptions** that start with *For Classification only* are unused in this version and are reserved for future use.

Table 15-29: Tbl_StatTemplate Table

Column Name	Description	Column Type
Date	Date and hour that the page was extracted.	DateTime
ServerId	A system-defined value identifying the server that generated this record.	string
ProcessName	Name of the CaptureFlow.	string
DocType	Name of the Document Type.	string
DppName	The recognition project name as specified during Extraction module setup.	string
TemplateId	The template ID. int	int
TemplateType	For Classification only.	
TemplateCode	The code defined for the template in Recognition Designer.	string
PagesProcessedByClassification	For Classification only.	
PagesClassifiedOk	For Classification only.	
ClassificationTimeSeconds	For Classification only.	

Column Name	Description	Column Type
PagesProcessedByRecognition	For Extraction only: Total number of pages processed. A page is considered processed if it is routed to an Extraction step and is associated with a template regardless of whether any content was extracted from it.	int
PagesRecognizedOk	For Extraction only: Number of pages in which no field has a "?" returned by OCR.	int
FieldsProcessedByRecognition	For Extraction only: Total number of fields processed. A field is processed if Extraction returns a value for it, even if that value is an empty string.	int
FieldsRecognizedOk	For Extraction only: Total number of fields without a "?" returned from the OCR engine.	int
RecognitionTimeSeconds	For Extraction only: Total time in seconds the pages were processed for extraction. For a given page, this is the time the page was spent being extracted.	double
ReportTag1 ReportTag2 ReportTag3	These columns are used to separate reporting data according to business needs. For example, ReportTag1 may be used to capture data for each line of business where capture services are shared across an organization.	string

15.29 Tbl_StatField

This table stores information about the fields processed in the Completion and Identification modules. A field is considered to have been processed if the operator saves the document, regardless of whether he completes the work or continues it later; it is not counted if the work is canceled and changes are abandoned. Users can use this data to determine which fields take the longest time to process or have high data correction rates. Capturing character counts enables accuracy measurement by calculating the percent of characters that were changed.

Note: The running module creates new records as required, but no more than one record per hour. The cumulative statistics for a given date and hour is calculated by aggregating all rows for the specified duration. For example, the number of pages processed by the Extraction module on 1/23/2012 between 10:00 and 11:00 is the total of all records where the Date is set to "1/23/2012 10:00".

Table 15-30: Tbl_StatField Table

Column Name	Description	Column Type
Date	Date and hour that the document containing the field was saved.	DateTime

Column Name	Description	Column Type
ProcessName	Name of the CaptureFlow.	string
DocType	Name of the Document Type.	string
Operator	The Windows user name of the operator in the format `Domain\user`.	string
Field	The name of the document type field.	string
CharsProcessed	Total number of characters across all fields in all processed field instances. The character count is determined when the document is completed. For example, if the value of a field was “Rob” when the document loaded and “Robert” when it was completed, the character count for that field is 6 and not 3.	int
KeyedChars	Total number of keystrokes entered when the field has focus; only includes characters stored as part of the field’s value and not the default shortcut keys, the **DELETE** key, or the **BACKSPACE** key.	int
Processed	The number of field instances processed. A field is considered processed if its document was routed to a Completion step and was saved, regardless of whether that document was completed or continued later. It is not counted if the work was canceled. For non-table fields, the number of field instances processed is the same as the number of documents processed. Each row in a table contains one instance of a field. Therefore, for table fields, the number of field instances processed is the same as the total number of rows in all documents processed.	int
Changed	The number of fields changed (either by an operator or a script) during processing.	int
ProcessingTimeSeconds	Total time the field has focus (in seconds). If the field never has focus, this value is set to zero.	double
ReportTag1 ReportTag2 ReportTag3	Used to further divide the reporting data according to business needs. For example, ReportTag1 might be used to capture separate data for each line of business in cases where capture services are shared across an organization.	string

15.30 Tbl_StatDocumentType

This table stores information about the documents processed by the Completion, Extraction, and Identification modules. A document is considered processed in Extraction if a template was identified for one or more of its pages. A document is considered processed in the Completion module if the operator saves the document, regardless of whether the operator completes the work or continues it later; it is not counted if the work is canceled and changes are abandoned. Users may use this data to determine which document types take the longest time to process or have high re-classification rates. Information is divided by CaptureFlow to enable reporting by line-of-business in cases where templates are shared. Capturing character counts enables accuracy measurement by calculating the percent of characters that were changed.

Note: The running module creates new records as required, but no more than one record per hour. The cumulative statistics for a given date and hour is calculated by aggregating all rows for the specified duration. For example, the number of pages processed by the Extraction module on 1/23/2012 between 10:00 and 11:00 is the total of all records where the Date is set to "1/23/2012 10:00".

Table 15-31: Tbl_StatDocumentType Table

Column Name	Description	Column Type
Date	Date and hour that the document was saved.	DateTime
ClientID	A system-defined value identifying the server that generated this record.	string
ProcessName	Name of the CaptureFlow.	string
DocType	Name of the Document Type.	string
Operator	For Completion only: The Windows user name of the operator in the format `Domain\user`.	string
DocsProcessed	Total number of documents processed by the module. A document is considered processed by Extraction if one or more of its pages were associated with a template, regardless of whether that template returned any content. A document is considered processed by Completion if it was saved, regardless of whether that document was completed or continued later. It is not counted if the work was canceled.	int
PagesProcessed	Total page count across all processed documents.	int

Column Name	Description	Column Type
CharsProcessed	Total number of characters across all fields in all processed documents. The character count is determined when the document is completed. For example, if the value for one of the fields was "Rob" when the document loaded and "Robert" when it was completed, that field counts as 6 characters and not 3.	int
Changed	For Completion only: The number of documents that were changed for this document type. For example, if the type for a document received by Completion was Invoice and the operator changed the type to PurchaseOrder, the changed count will be incremented for the Invoice statistic. This column can be used to determine the rate of incorrectly classified documents.	int
FieldsProcessed	The number of field instances processed for documents of this type. Within each document, a non-table field counts as 1 and a table field counts as one per table row. For example, assume the document had the non-table fields **Date**, **Name**, and **ID** and the table fields **Description** and **Amount**. If the table had 4 rows, the total number of fields would be 11, 3 for the non-table fields plus 4 rows with 2 fields each.	int
FieldsChanged	The number of field instances changed for documents of this type (either by an operator or script) during processing.	int
KeyedChars	For Completion only: Total number of keystrokes entered in any field of this document type; only includes characters stored as part of the field's value and not default shortcut keys, the **DELETE** key, or the **BACKSPACE** key.	int
ProcessingTimeSeconds	The total processing time in seconds. The processing time in Extraction is the total time required to extract all pages in the document. The processing time in the Completion module is the total time that the data entry form is displayed to the operator. If the work contains multiple documents, the processing time is measured separately for each. If one document in that work is never viewed by the operator, that document has zero processing time.	double
ReportTag1 ReportTag2 ReportTag3	Used to further divide the reporting data according to business needs. For example, ReportTag1 might be used to capture separate data for each line of business in cases where capture services are shared across an organization.	string

15.31 Tbl_ReportDispatcherData Table

This table is used to store the main reports data (such as template, field, and operator). This table is designed in a generic manner so it can store any kind of report data.

Table 15-32: Tbl_ReportDispatcherData Column Matrix

Column Name	Type (Size)	Description
`ParamsID` (PK) (FK)	Int (4)	The unique ID of the **Recognition Project (DPP)** being analyzed. See "Tbl_ReportDispatcherParams Table" on page 566.
`DataName`	NVarChar (50)	Name of the reports data.
`DataType`	Int (4)	Type of data such as Template, Field, or Operator. For more information, see "Tbl_ReportDispatcherData Data Type Matrix" on page 564 .
`DataId`	Int (4)	Data ID (either Template ID or Field ID).
`DataCode`	NVarChar (50)	Template code (see "Tbl_ReportDispatcherData Data Type and Data Value Matrix" on page 564).
`DataCategory`	NVarChar (50)	Template category (Standard, *HPA*, Generic, and Text matching). See "Tbl_ReportDispatcherData Data Type and Data Value Matrix" on page 564.
`Cnt1`	Int (4)	Numeric counter (see "Tbl_ReportDispatcherData Data Type and Data Value Matrix" on page 564).
`Cnt2`	Int (4)	Numeric counter (see "Tbl_ReportDispatcherData Data Type and Data Value Matrix" on page 564).
`Cnt3`	Int (4)	Numeric counter (see "Tbl_ReportDispatcherData Data Type and Data Value Matrix" on page 564).

Column Name	Type (Size)	Description
Cnt4	Int (4)	Numeric counter (see "Tbl_ReportDispatcherData Data Type and Data Value Matrix" on page 564).
Cnt5	Int (4)	Numeric counter (see "Tbl_ReportDispatcherData Data Type and Data Value Matrix" on page 564).
Time1	BigInt (8)	Cumulated time (see "Tbl_ReportDispatcherData Data Type and Data Value Matrix" on page 564).
Time2	id	Cumulated time (see "Tbl_ReportDispatcherData Data Type and Data Value Matrix" on page 564).
Time3	id	Cumulated time (see "Tbl_ReportDispatcherData Data Type and Data Value Matrix" on page 564).
Time4	id	Cumulated time (see "Tbl_ReportDispatcherData Data Type and Data Value Matrix" on page 564).
DateUpdated	NVarChar (25)	Date and time of the last update reflected in the following format: yyyy/mm/dd hh:mm:ss:zzz

Table 15-33: Tbl_ReportDispatcherData Data Type Matrix

Data Type	Description
100	Template data type.
102	Index field data type. This is the index field of an index family.
103	Operator data type.

Table 15-34: Tbl_ReportDispatcherData Data Type and Data Value Matrix

Column Name	Template	Field	User
DateName	Template Name	Field Name	User Name
DataType	100	102	103
DataId	Template ID	Field ID	n/a

Column Name	Template	Field	User
DataCode	Template Code	Linked to Template ID	Last workstation name used by the operator
DataCategory	Template Category (Standard, *HPA*, Generic, and Text matching)	Name of the Index Family	n/a
Cnt1	Total number of documents classified automatically for this Template ID.	Number of index fields processed for this Field ID.	Number of documents classified manually by this user.
Cnt2	Total number of documents classified manually for this Template ID.	Number of index fields recognized and validated automatically for this Field ID.	Number of documents validated manually by this user.
Cnt3	Total number of documents validated automatically for this Template ID.	Number of documents validated manually for this Field ID.	Number of folders validated manually by this user.
Cnt4	Total number of documents validated manually for this Template ID.	Number of folders validated manually for this Field ID.	Number of characters typed by this user.
Cnt5	n/a	Number of characters typed for this Field ID..	n/a
Time1	Total classification time for this template ID, in microseconds.	Recognition time for this Field ID, in milliseconds.	Identification time for this user, in milliseconds.
Time2	Total Identification time for this Template ID, in milliseconds.	Validation time for this Field ID, in milliseconds.	Total time to validate documents for this user (in milliseconds).
Time3	Recognition time for this Template ID, in microseconds.	n/a	Total time to validate fields for this user (in milliseconds).
Time4	Validation time for this Template ID, in milliseconds.	n/a	n/a

Related Topics

"Tbl_ReportDispatcherParams Table" on page 566

"Tbl_ReportDispatcherTask Table" on page 567

15.32 Tbl_ReportDispatcherParams Table

Use this table to access the unique parameter key for a specific recognition project.

Table 15-35: Tbl_ReportDispatcherParams Column Matrix

Column Name	Type	Description
`ParamsID` (PK) (FK)	Int (4)	This is the primary key for the table. Contains unique ID parameters that result from a combination of the columns: `NomFichier`, `ServerName`, `InstanceId` and `ProcessId`.
`ProcessId`	nvarchar (50)	The associated column in Intelligent Capture that defines this `ProcessId` is `RBProcessUUID`, in the `Tbl_ReportBatches` table. This column can be used to make a join on an *SQL* query when defining a report definition.
`InstanceId`	int	The `InstanceId` column enables producing reports data for one given instance of a given process.
`ServerName`	nvarchar (50)	This column contains the server name. The associated column in Intelligent Capture that defines this `ServerName` is `RBCurrentServer` in the Tbl_ReportBatches.
`NomFichier`	NVarChar (255)	Full path to the project being analyzed.
`EstActif`	Int (4)	Indicates whether the project is activated or deactivated. This value is not used within an Intelligent Capture environment.
`DateDebut`	NVarChar (25)	Scheduled starting time. This value is not used within an Intelligent Capture environment.

Column Name	Type	Description
DateFin	NVarChar (25)	Scheduled ending time. This value is not used within an Intelligent Capture environment.

Related Topics

"Tbl_ReportDispatcherData Table" on page 563

"Tbl_ReportDispatcherTask Table" on page 567

15.33 Tbl_ReportDispatcherTask Table

This table is used to store information about the batch being processed through Advanced Recognition modules. This table enables you to track the number of batches, folders and documents that are processed daily. Each record in this table represents the data processed by a module for a specific day.

Table 15-36: Tbl_ReportDispatcherTask Column Matrix

Column Name	Type	Description
ParamsID (PK) (FK)	Int (4)	The unique key for the DPP project used for this module and date. See "Tbl_ReportDispatcherParams Table" on page 566.
DateUpdated	NVarChar (25)	The date and time of the last update. Format is: yyyy/mm/dd hh:mm:ss:zzz
ModuleId	Int (4)	The ID of the module being processed. See "Tbl_ReportDispatcherTask Module ID Matrix" on page 568.
TaskCnt	Int (4)	The number of tasks processed for this **ModuleId** and date.
DocCnt	Int (4)	The number of documents processed for this **ModuleId** and date.
PageCnt	Int (4)	The number of pages processed for this **ModuleId** and date.

Table 15-37: Tbl_ReportDispatcherTask Module ID Matrix

ModuleId	Description
110	Classification module
120	Identification module

Related Topics

"Tbl_ReportDispatcherData Table" on page 563

"Tbl_ReportDispatcherParams Table" on page 566

Chapter 16

Appendix—Intelligent Capture Client Modules

"Intelligent Capture Modules" on page 569 lists Intelligent Capture client modules and their capabilities.

Caution

Some modules may run as multiple application instances or multiple service instances, but it may not be safe to do so because you might experience data loss. See this table for the list of modules that you can safely run as multiple application or service instances.

Table 16-1: Intelligent Capture Modules

Module	Version introduced	Executable[a]	*MDF* File Name	DBCS[b]	ScaleServer[c]	Attended[d]	Unattended[e]	Application[f]	Multi-application instances[g]	Service[h]	Multi-service[i]	Scripting[j]
.NET Code Module	New in 6.x	`CodeClient.exe`	`code.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[k]
ApplicationXtender Export	Available prior to 6.0	`exax.exe`	`exax.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Archive Export	Available prior to 6.0	`exsapal.exe`	`exsapal.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Intelligent Capture Administrator	New in 7.0 - 7.7, 16.5, 16.6, 20.2	`CaptivaAdministrator.exe`	Not applicable	Not applicable	No	Yes	No	Yes	Yes	No	No	No

Module	Version introduced	Executable[a]	*MDF* File Name	DBCS[b]	ScaleServer[c]	Attended[d]	Unattended[e]	Application[f]	Multi-application instances[g]	Service[h]	Multi-service[i]	Scripting[j]
Classification	Available prior to 6.0	`Emc.InputAccel.DPCLSSF.dll`	`dpclssf.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[l]
Collector	Available prior to 6.0	`Emc.InputAccel.DPCollec.dll`	`dpcollec.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[m]
Completion (previously known as Intelligent Capture)	New in 7.0 - 7.7, 16.5, 16.6, 20.2	`cpdsktop.exe`	`cpdsktop.mdf`	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes[n]
Copy	Available prior to 6.0	`iacopy.exe`	`iacopy.mdf`	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
Documentum Advanced Export	New in 6.x	`DocumentumAdvancedExport.dll`	`iaexdm.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[o]
Email Import	Available prior to 6.0	`EmailImport.exe`	`emailimp.mdf`	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No

Module	Version introduced	Executable[a]	*MDF* File Name	DBCS[b]	ScaleServer[c]	Attended[d]	Unattended[e]	Application[f]	Multi-application instances[g]	Service[h]	Multi-service[i]	Scripting[j]
Extraction	New in 7.0 - 7.7, 16.5, 16.6, 20.2	`cpextrac.exe`	`cpextrac.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[p]
FileNet Content Manager Export	Available prior to 6.0	`exfncm.exe`	`exfncm.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
FileNet Panagon IS/CS Export	Available prior to 6.0	`iaxfnet2.exe`	`iaxfnet2.mdf`	Yes	No	Yes	Yes	Yes	Yes[q]	No	No	No
Global 360 Export (formerly known as eiStream WMS Export)	Available prior to 6.0	`iaexwnt.exe`	`iaexwnt.mdf`	No	No	Yes	Yes	Yes	Yes	No	No	No

Module	Version introduced	Executable[a]	*MDF* File Name	DBCS[b]	ScaleServer[c]	Attended[d]	Unattended[e]	Application[f]	Multi-application instances[g]	Service[h]	Multi-service[i]	Scripting[j]
Export for IBM Content Manager	Available prior to 6.0	`exicm.exe`	`exicm.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Export for SAP Archive and AP Connect	Available prior to 6.0	`excssap.exe`	`excssap.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Identification	New in 7.0 - 7.7, 16.5, 16.6, 20.2	`cpidentf.exe`	`cpidentf.mdf`	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes[r]
Image Converter	New in 7.0 - 7.7, 16.5, 16.6, 20.2	`imgconv.exe`	`imgconv.mdf`	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Image Processor	New in 7.0 - 7.7, 16.5, 16.6, 20.2	`cpimgpro.exe`	`cpimgpro.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[s]
Microsoft SharePoint Export	Available prior to 6.0	`exshrpt2.exe`	`exshrpt2.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No

Module	Version introduced	Executable[a]	*MDF* File Name	DBCS[b]	ScaleServer[c]	Attended[d]	Unattended[e]	Application[f]	Multi-application instances[g]	Service[h]	Multi-service[i]	Scripting[j]
Multi	Available prior to 6.0	`iamulti.exe`	`iamulti.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Multi-Directory Watch	Available prior to 6.0	`MultiDirectoryWatch.exe`	`iamdw.mdf`	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
NuanceOCR	New in 6.x	`NuanceOCR.dll`	`ssocr.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[t]
ODBC Export	Available prior to 6.0	`iaxodbc2.exe`	`iaxodbc2.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Export for Open Text Content Server	Available prior to 6.0	`exll2.exe`	`exll2.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
RescanPlus	New in 6.x	`Emc.InputAccel.ReScan.dll`	`rescanplus.mdf`	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes[u]
Scan Plus	New in 6.x	`Emc.InputAccel.Scan.dll`	`scanplus.mdf`	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes[v]

Module	Version introduced	Executable[a]	*MDF* File Name	DBCS[b]	ScaleServer[c]	Attended[d]	Unattended[e]	Application[f]	Multi-application instances[g]	Service[h]	Multi-service[i]	Scripting[j]
Standard Export	New in 7.0 - 7.7, 16.5, 16.6, 20.2	`cpexport.exe`	`cpexport.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Standard Import	New in 7.0 - 7.7, 16.5, 16.6, 20.2	`cpimport.exe`	`cpimport.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[w]
Standard OCR	New in 7.0 - 7.7, 16.5, 16.6, 20.2	`CPOCR.exe`	`CPOCR.mdf`	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Timer	Available prior to 6.0	`iatimer.exe`	`iatimer.mdf`	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No
WS Input	New in 6.x	`WebServicesInput.dll`	`wsinput.mdf`	Yes	Yes	No	No	No	No	Yes	Yes	Yes[x]
WS Output	New in 6.x	`WebServicesOutput.dll`	`wsoutput.mdf`	Yes	Yes	No	No	No	No	Yes	Yes	Yes[y]

[a] Executable name of the module.

[b] Can process tasks that include double-byte character values, such as Korean and Chinese.

[c] Can connect to multiple Intelligent Capture Servers that are configured as a ScaleServer group.

[d] Can be operated in attended production mode, displaying an interactive user interface.

[e] Can be operated in unattended production mode using command line parameters; no user interaction is required.

[f] Can be run as an application.

[g] Multiple application instances can safely be run on a single machine.

[h] Can be configured to run as Windows services.

[i] Multiple instances can safely be run as Windows services on a single machine.

[j] Can use scripting.

[k] .NET Code Module provides a separate programming interface that is independent of the client-side scripting interface used by other modules. The *OpenText Intelligent Capture - Utilities Modules Guide (ECPCORE-CMU)* provides configuration and reference information.

[l] Use Recognition Scripting

[m] Use Recognition Scripting

[n] Use Document Scripting

[o] Use client-side scripting

[p] Use Document Scripting

[q] FileNet IS/CS Export allows running multiple application instances, but multiple connections may be restricted by the repository.

[r] Use Document Scripting

[s] Use Document Scripting

[t] Use client-side scripting

[u] Use client-side scripting

[v] Use client-side scripting

[w] Use Document Scripting

[x] Use client-side scripting

[y] Use client-side scripting

Glossary

AC

Administration Console

ACL

Access Control List

API

Application Programming Interface

ASP.NET

Active Server Pages for .NET applications.

Avg.

Average

CAF

Captiva Activation File

CFR

Code of Federal Regulations

CPU

Central processing unit

CSV

Comma Separated Variable

DAL

Data Access Layer

DLL

Dynamic Link Library

FDA

Food and Drug Administration

FIPS

Federal Information Processing Standard

FQDN

Fully Qualified Domain Name

GB

Gigabyte

GIF

Graphic Interchange Format

HIPPA

Health Insurance Portability and Accountability Act

HPA

High Precision Anchor

Hr

Hour

HTTP

Hypertext Transfer Protocol

HTTPS

Hypertext Transfer Protocol Secure

IAP

InputAccel process file extension

IMAP4

Internet Message Access Protocol version 4

INI

Microsoft Windows initialization filename.

IP

Internet Protocol

IPP

Integrated ProcessFlow Project

IPSec

Internet Protocol Security

ISAPI

Internet Server Application Programming Interface

IT

Information Technology

KB

kilobyte

LOG

Log file extension

LUA

least privileged user account

MB

megabyte

MDF

Module Definition File

msecs

milliseconds

NAS

Network Attached Storage

NAT

Network Address Translation

NT

Microsoft Windows New Technology

NTFS

Microsoft Windows NT File System

NTLM

NT LAN Manager authentication protocol

OCR

Optical Character Recognition

OMR

Optical Mark Recognition

OS

Operating System

PDF

Portable Document Format

PM

Post Meridian

POP3

Post Office Protocol version 3

RPT

Report file extension

RW

Read Write

SAN

Storage Area Network

SMTP

Simple Mail Transfer Protocol

SOA

Service Oriented Architecture

SOAP

Service-Oriented Access Protocol

SPN

Service Principal Name

SQL Server

Microsoft implementation of a database server that uses Structured Query Language

SQL

Structured Query Language

SSL

Secure Sockets Layer

TCP/IP

Transmission Control Protocol/Internet Protocol

TCP

Transmission Control Protocol

UAC

User Account Control

UI

User Interface

URI

Uniform Resource Identifier

URL

Uniform Resource Locator

UUID

Universally Unique Identifier

VB

Microsoft Visual Basic

VBA

Microsoft Visual Basic for Applications

WSDL

Web Services Description Language

XML

Extensible Markup Language