opentext™

OpenText™ Intelligent Capture

Installation Guide

This guide explains how to install, configure, upgrade, remove, and troubleshoot Intelligent Capture and Intelligent Capture Real Time Services.

ECPCORE220200-IGD-EN-01

OpenText™ Intelligent Capture
Installation Guide

ECPCORE220200-IGD-EN-01
Rev.: 2022-Mar-17

This documentation has been created for OpenText™ Intelligent Capture CE 22.2.
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

Table of Contents

Chapter 1

Overview

Intelligent Capture captures and processes documents from a variety of sources including scanners, fax servers, email servers, file systems, web services, and via RESTful web services. Document information can be stored as images, text, or both. Intelligent Capture is optimized for capturing documents, not storing them for long-term access. Typically, documents remain in the system for a few hours to a few days, until they are exported to a content repository or other back-end system.

1.1 Intelligent Capture

Intelligent Capture is a scalable solution that optionally uses multiple servers to manage resources. Therefore, it can process large amounts of data from throughout your enterprise. It also handles multiple languages and system locale settings.

Why use Intelligent Capture?

The benefits of Intelligent Capture include:

- Reducing operating costs caused by factors such as document preparation and data entry.
- Reducing recovery costs caused by mishandled physical documents.
- Improving information quality for critical business processes.
- Accelerating business processes by providing immediate access to all information and supporting documentation.
- Enforcing strong compliance control by storing documents and metadata electronically.
- Minimizing processing errors, improving data accuracy, and boosting productivity.

1.2 Intelligent Capture Real Time Services

Intelligent Capture Real Time Services is a product offering based on Intelligent Capture REST Services, which are a set of RESTful web service interfaces that custom client applications can use to call the services of the Intelligent Capture Server or the Module Server. An example of an Intelligent Capture REST Services client is Intelligent Capture Web Client.

You use the Intelligent Capture REST Services in your application to perform a batch request in a CaptureFlow or an Ad Hoc Service request for Module Server services as follows:

- In a *batch request*, your application sends documents and data to the Intelligent Capture REST Service Web application, which creates an Intelligent Capture batch, adds the documents and data to the batch, and then sends the batch to the Intelligent Capture Server, which executes the specified CaptureFlow. You can also write a custom Intelligent Capture REST Service Web application authentication plug-in that authenticates and maps the Intelligent Capture REST Service Web application's callers to the appropriate Intelligent Capture user roles.
- In an *Ad Hoc Service request*, your application makes a request to the Intelligent Capture REST Service Web application for Module Server services, such as classifying and extracting pages or reading barcodes.

Intelligent Capture Real Time Services can be deployed standalone or in combination with an Intelligent Capture system as follows:

Standalone Intelligent Capture Real Time Services

- Document Services and Image Services licenses (on a single Intelligent Capture REST Services system)
- (Optional) Text-searchable PDF license
- Real-Time Advanced Recognition license (also available separately)
- Two Intelligent Capture Server licenses (including an annual page count of 1 page per year) for configuration and user authentication only in a high-availability environment
- Intelligent Capture REST Services feature code
- ScaleServer feature code
- Extraction module and Recognition Designer feature code

Intelligent Capture Real Time Services in combination with Intelligent Capture

- Document Services and Image Services licenses (on a single Intelligent Capture REST Services system)
- (Optional) Text-searchable PDF license
- Real-Time Advanced Recognition license (also available separately)

Chapter 2

Installation Planning for Intelligent Capture

A successful Intelligent Capture installation depends on having a good installation plan. Carefully planning the installation requires attention to many aspects, including: hardware, software, locale, networking, security, system availability, backup, recovery, and more.

Table 2-1: Planning considerations

Item	Planning activity
Locale considerations	Carefully consider the locale and code page requirements of all components. This is especially important in a distributed capture system.
Performance	An enterprise document capture system should be able to keep up not only with the data coming into the system, but also the data being processed through the system.
Scalability	Decide whether to install the entire system at once or start with a small system and then expand. Intelligent Capture supports both server and client scalability.
Security	Carefully consider the security implementation. The plan should cover the security providers relative to local and remote administrators, local and remote operators, and the SQL Server that hosts the Intelligent Capture Database (if installed).
Network configuration	Determine how Intelligent Capture fits into your network topology. Intelligent Capture can be deployed to a single domain, multiple domains, or to a single, standalone machine.
High availability and failover	Perform an appropriate level of planning to keep your document capture system online and productive at all times. This might be as simple as an additional Intelligent Capture Server configured as part of a ScaleServer group to provide load balancing, or as complex as configuring a Microsoft Failover Clustering cluster sharing a Storage Area Network (*SAN*) to provide an automated response to hardware failures.

Item	Planning activity
Disaster recovery	Prepare a disaster plan with attention to restoring your document capture operation and keeping the organization productive after various types of disasters. This may be as simple as routine backups with offsite storage or as complex as multiple Microsoft Failover Clustering clusters in both local and remote locations with replicated Storage Area Networks to provide an automated response to hardware failures. This provides ongoing and uninterrupted production at all times.
Licensing and activation	Many different licensing plans are offered to meet the needs of different types of customers. Obtain license codes for each Intelligent Capture Server and use a software activation file.

Note: For planning considerations specific to Intelligent Capture REST Services and Intelligent Capture Web Client, see "Installation Planning for Intelligent Capture Real Time Services" on page 43.

2.1 Locale Considerations

Intelligent Capture supports multiple languages within a deployment, thereby enabling global document processing. Multiple language support enables batches and tasks to process data in multiple languages and use multiple locale settings. To understand the multiple language feature, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

Locale considerations that are important before you install:

- User-specified information entered in the setup program must only include values from the code page of the machine running the installer. Non-code page values will result in data corruption.
- On machines running client modules and the Intelligent Capture Server, the language specified by the locale setting must be supported by the code page selected on that machine.

2.2 Performance and Throughput

Maximizing performance and throughput are key objectives when designing an Intelligent Capture system. Many factors affect performance and throughput, but at the top of the list are the server processors, their disk systems, and the network to which they connect. Good infrastructure planning results in taking full advantage of Intelligent Capture modularity.

Intelligent Capture modularity enables you to adjust the configuration to meet production needs after observing the system in production mode for a period of time. To meet your production goals, add more modules, more machines, more Intelligent Capture Servers, and more operators as needed.

2.2.1 Database Server Considerations

The SQL Server hosted Intelligent Capture Database is an optional component.

Environments requiring an Intelligent Capture Database

The database is required only if your environment has any of the following requirements:

- Reporting functionality is required
- ScaleServer capability is required
- WS Input (Web Services) and WS Output (Web Services) must be supported
- Microsoft Failover Clustering support is required
- Side-by-side Intelligent Capture Servers are required
- You are upgrading from an Intelligent Capture 7.x environment that included the Intelligent Capture Database

Note: In a ScaleServer environment, only one database is allowed.

Machine requirements for the Intelligent Capture Database

- The machine that hosts the Intelligent Capture Database must service queries, process every transaction related to reporting and logging, and store these results until they are purged, either by a manual or scheduled job.
- In high volume environments, install the Intelligent Capture Database server on a fast multi-*CPU* machine with fast, RAID hard drives, and with as much *RAM* as the operating system supports.
- When database storage requirements become large, due to process volumes and enabled logging and reporting rules, high throughput becomes critical to maintaining production volumes. Choose the latest high-speed technology from among available disk storage systems. The network connection between the Intelligent Capture Server and the Intelligent Capture Database must have high bandwidth (about 1 *GB* per second) and low latency. For the

Intelligent Capture Database data directory, configure multiple identical disk drives in a *RAID* configuration to achieve the required reliability and failure protection. Use trusted and reliable disk drives with high performance and high capacity ratings.

- Although any RAID level is supported, optimization for maximum performance and the use of fault tolerance is highly recommended. For example, RAID 0 does not have fault tolerance and is therefore not recommended. Also, although RAID 5 and 6 have fault tolerance, their performance is lower than RAID 10. Therefore, RAID 10 is the recommended RAID level.

  Note: RAID 5 is not recommended for high volume deployments.

- Disk drives should have on-board disk caching of at least 32 MB, write-back caching (write to RAM), read-ahead optimization, and battery backup for the on-board cache.

  Note: Disk controllers that are integrated into motherboards typically do not provide the features, performance, or reliability that an enterprise platform demands.

Server requirements for the Intelligent Capture Database

- For all but low volume deployments, Intelligent Capture requires a dedicated computer for the SQL Server that hosts the Intelligent Capture Database. This computer must meet the recommended hardware requirements specified in the *Intelligent Capture Release Notes* (available in My Support (https://support.opentext.com/)). High volume deployments may require larger than the recommended hardware.
- Make sure that the SQL Server that hosts the Intelligent Capture Database has sufficient connections available to accommodate your Intelligent Capture system. Each Intelligent Capture Server and web service instance consumes one connection.
- Multiple Intelligent Capture deployments that are completely separate and should be kept separate, require separate Intelligent Capture Databases.

ScaleServer group deployments

A ScaleServer group must have a single Intelligent Capture Database. All Intelligent Capture Servers within the ScaleServer group must access the same Intelligent Capture Database. Within an Intelligent Capture deployment, independent Intelligent Capture Servers not configured as a ScaleServer group may access the same Intelligent Capture Database or separate Intelligent Capture Databases based on business requirements.

Database performance considerations

- The machine hosting the Intelligent Capture Database should have the highest-speed network connection with low latency available to ensure maximum throughput.
- Reports that issue complex queries put a much greater load on the database. To increase database performance, increase the performance of the server that hosts the Intelligent Capture Database. You cannot increase performance by adding more instances of the Intelligent Capture Database.
- A test Intelligent Capture Database and a production Intelligent Capture Database can be installed on the same SQL Server. However, it is recommended that at a minimum, the test and production databases be installed on different SQL Servers and for most efficient performance, the two databases be installed on different machines. This ensures that the production databases maintains optimum performance despite the possibility of excessive *CPU* utilization of the test database.
- If SQL Server has the necessary performance, then multiple Intelligent Capture Databases (each with a different name) can be installed on a single instance of SQL Server. However, each Intelligent Capture Server requires only one Intelligent Capture Database. If you have multiple, independent Intelligent Capture Servers, then they can share the same Intelligent Capture Database, or they can have independent Intelligent Capture Databases.

SQL Server Express

- By default, SQL Server Express does not accept connections over the *TCP/IP* protocol. Enable *TCP/IP* connections before installing the Intelligent Capture Database. In SQL Server Configuration Manager, SQL Server Express must be configured to allow TCP/IP protocol access over port 1433. Enable *TCP/IP* protocol for each *IP* address used by the system, making sure that the **TCP Dynamic Ports** field is blank, to disable dynamic ports, and then restart the SQL Server Express service. Connection errors can occur if SQL Server Express is not configured to allow for TCP/IP access.
- SQL Server Express editions must only be used in low page volume deployments with minimal reporting and logging due to the following limitations:
  - SQL Server Express does not support configuration for failover or high availability.
  - SQL Server Express supports the use of one *GB* of *RAM*, and uses one *CPU*. With multiple CPUs, SQL Server Express uses only one from those available.
  - By default, SQL Server Express creates a named instance. Named instances require specifying the instance name in all database connection strings. To avoid this issue, create an unnamed instance during SQL Server Express installation.

– Microsoft SQL Server Management Studio Express is not automatically installed with all versions of SQL Server Express, but it is available as a separate installation from Microsoft.

Logging considerations

The amount of data written to the Intelligent Capture Database is related to the logging and reporting configuration. Enabling Audit Logging and Reporting writes significant amounts of data to the Intelligent Capture Database.

2.2.2 Intelligent Capture Server Considerations

The Intelligent Capture Server is memory and disk intensive. The server stores multiple copies of each processed image, often one or more for each step in a process. Also, the image data being processed requires significant processing and space on the server. For this reason, you must consider some important factors related to the Intelligent Capture Server.

- For all but low volume deployments, Intelligent Capture requires a dedicated computer for the Intelligent Capture Server. This computer must meet the recommended hardware requirements specified in the *Release Notes* (available in My Support (https://support.opentext.com)). High volume deployments may require larger than the recommended hardware.
- Use the same performance considerations as for the Intelligent Capture Database (described in "Database Server Considerations" on page 13) for selecting a network connection and a disk system for the Intelligent Capture Server data directory (`C:\IAS` by default). Also, do not locate the Intelligent Capture Server data directory and the Microsoft Windows paging file on the same physical disk drive.

Caution

Do not run antivirus software on the Intelligent Capture Server data directory and its subfolders. Doing so will drastically degrade Intelligent Capture Server performance due to the large number of files being written to the directory structure. In addition, some antivirus software intercept network traffic and can interfere with Intelligent Capture Server operation. In all cases, exclude the following directories and their subdirectories from antivirus scanning:

– Intelligent Capture Server data directory (by default, `C:\IAS`)

– Intelligent Capture Server installation folder (by default, `C:\Program Files\InputAccel\Server`)

– `C:\ProgramData\EMC\InputAccel`

– Windows Temp folder (`%TEMP%`)

– `C:\Users\<username>\AppData\Local\Temp` (where *<username>* represents the name of a user)

- Antivirus software is not designed to check in real-time the kind of volume and file size needed for a Intelligent Capture Server to maintain full production throughput. This high volume of work tends to manifest antivirus software issues (usually hanging) that can in turn cause a production Intelligent Capture system to crash. The files in the directories for Intelligent Capture use are transitory; that is, they exist only as long as the batch is in Intelligent Capture Server.

  Note: You might consider an audit by security professionals who are familiar with Intelligent Capture and the whole chain of custody from the hardware scanner up to final data output in the repository. They might be able to advise on the optimal points in the chain of custody at which to apply virus-scanning technology such that system performance is not impacted or the production system is not put at risk for a production-down situation. For example, a network file share that is used as a drop zone for images coming from other (non-Intelligent Capture) systems could be one such optimal point in the chain of custody. Another alternative is to schedule a full virus scan of the Intelligent Capture Server data folder to occur during off-production hours when the Intelligent Capture Server service can be paused or stopped.

- To improve performance, install multiple Intelligent Capture Server instances as described in "Installing Multiple Instances of Intelligent Capture Servers" on page 79. Each Intelligent Capture Server instance should have 4 GB RAM and should have its data directory on a separate disk drive.
- The Intelligent Capture Server fully supports locating its main directory structure 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.
- Be aware that even though the Intelligent Capture Server will run under a VMware ESX Server, doing so will degrade the Intelligent Capture Server performance by approximately 20% or more.

2.2.3 Web Services Subsystem Considerations

To use the Web Services subsystem, consider setting up one or more dedicated Web Services Hosting servers. A single server may be adequate; however, many enterprises have a need to handle both internal and external web service requests and responses, and so you may want to have one instance of Web Services Hosting openly accessible from the local network and another instance accessible from the Internet through a firewall.

A single instance of Web Services Coordinator handles requests from all instances of Web Services Hosting. Web Services Coordinator communicates directly with the Intelligent Capture Database, and should therefore be installed on a secure server

with a high-speed network connection to the Intelligent Capture Database host machine. Depending on the required performance of the Web Services subsystem, Web Services Coordinator may share the same machine as the internal-facing Web Services Hosting instance or may require a separate, dedicated machine.

Note: Although you can install multiple instances of Web Services Hosting, this component does little processing. Typically, the only reason to install multiple instances is to separate internal from external request/response traffic. In any case, an Intelligent Capture system may have only one Web Services Coordinator instance.

Before attempting to use Web Services Input be sure that the Web Services Hosting and Web Services Coordinator services are started.

2.2.4 Client Machine Considerations

Intelligent Capture provides operator-attended client modules and unattended client modules. The Client setup program supports installation of any combination of Intelligent Capture modules on a single machine.

It is recommended that the network connection between the Intelligent Capture Server and the client modules have high bandwidth (1 *GB* per second) and low latency for optimal performance.

Typically, only the modules that will be run on a machine must be installed on that machine.

Unattended modules are configured and run continuously in a *wait for task* mode, processing tasks whenever they are received from the Intelligent Capture Servers. Unattended modules are server-grade applications that should be installed on *IT*-managed servers and, if supported, run as Microsoft Windows services. (For a list of modules that run in unattended mode and that run as services, see "Intelligent Capture Modules" on page 189.) For unattended modules that run as services, no operator intervention is required. When running modules as services, run them under a user account or a machine account.

Export modules typically use minimal amounts of processing power and only process tasks intermittently. Several modules using minimal processing power can be hosted by a single computer without creating a bottleneck. On the other hand, page recognition and image enhancement modules (for example) can use all available processing power over extended periods and still may not keep up with the number of tasks being generated for them. Modules of this type typically should have dedicated computer with dual cores and, in some cases, multiple instances of a module may be needed, each running on a separate computer.

To determine the actual number of module instances required, use client balancing to observe the system in typical production operation, find the bottlenecks, and add module instances until the throughput is satisfactory. Client balancing is accomplished by bringing one module instance on line at a time until the average number of new tasks being generated for the module is less than the number of tasks being processed by all module instances.

Client balancing

When performing client balancing, it may not be necessary to install multiple module instances on separate physical machines. For example, if using high-performance, multiprocessor machine systems, you may be able to install multiple instances of a page recognition or image processing module on one machine. Or install a combination of processor-intensive modules and non-processor-intensive modules on one machine. To see a list of modules that can run as services as well as modules for which multiple instances can be configured to run as services on a single machine, see "Intelligent Capture Modules" on page 189. To learn how to configure modules that have already been installed to run as services, see "Manually Registering a Client Module to Run as a Service" on page 121.

Scalability

For modules that support multiple service instances (as listed in "Appendix—Intelligent Capture Client Modules" on page 189), consider installing multiple instances on a single multi-core machine to achieve client balancing and scalability as needed. For modules that do not support multiple service instances, consider running multiple instances on separate virtual machines on the same physical, multi-core machine. In all cases, you must ensure that the machine has sufficient processing capacity to run multiple instances.

2.2.5 Running Modules as Services

When configuring modules to run as services, you must configure the following:

1. Windows account under which the module runs
2. Ability for this account to log into the Intelligent Capture Server
3. Intelligent Capture permissions

Note: For a list of client modules that can be run in unattended mode and as services, see "Intelligent Capture Modules" on page 189.

Choosing a "run-as" account

You can choose to run modules as services under a user account or under the Network Service account.

- **User account**: Modules connect to the Intelligent Capture Server in the same way as if they were running as applications—by authenticating with a specific domain user name and password. This is the recommended way to configure modules as services, because it simplifies configuration as well as ongoing account maintenance.

  Note: The user account under which modules run must be granted the "Log on as a service" user right. This right is granted automatically when the module is installed to run as a service under a user account and is updated automatically if the user account is changed through the Windows

Service Control Manager. This right is managed in the **User Rights Assignment** branch of the machine's **Local Security Settings**.

- **Network Service account**: Intelligent Capture supports the use of the Network Service account in cases where customers cannot use a user account to run modules as services. Multiple ways are available to configure a module running under Network Service to authenticate with the Intelligent Capture Server machine. We recommend that you enable and configure Kerberos authentication, as explained in "Configuring Intelligent Capture to use Kerberos authentication" on page 21.

  Notes

  – All modules that are installed during a single execution of the client setup program to run as services are configured to use the same type of account (user or Network Service).

  – All modules that are installed during a single execution of the client setup program to run as services under a user account are configured to use the same user name, password, and domain name. (These settings can be changed later by using the Services application of the Microsoft Management Console).

  – User accounts must be domain accounts except when all Intelligent Capture components are installed on a single machine. When all components are installed on a single machine, there are no issues with using the Network Service account because the machine already has the ability to log into itself.

  – When using the Network Service account to run client modules as services, make sure to run the Intelligent Capture Server under the LocalSystem account.

  – Make sure that the client machine running the client module as a service is added to the **Module Operator** role in Intelligent Capture Administrator.

Enabling the "run-as" account to log into the Intelligent Capture Server

Regardless of whether a module runs under a user account or Network Service, that account must have the ability to log into the Intelligent Capture Server machine. This ability is automatically configured when using a domain user account—members of the `Domain\Users` group are added to the Intelligent Capture Server machine's local `Users` group by default.

However, machine accounts such as Network Service do not, by default, have the ability to log into the Intelligent Capture Server (unless the module is running on the same machine as the Intelligent Capture Server). This ability must be granted by adding the client machine name (in the form of *<domain>*\ *<machinename>*$) to a local group (for example the local `Users` group) of the Intelligent Capture Server machine.

Configuring Intelligent Capture Permissions

Use Intelligent Capture Administrator to assign appropriate permissions to the group to which the user account belongs.

- If the module is running as a service under a user account, configuring permissions consists of assigning one or more groups to one or more permission roles, possibly adding new roles or modifying existing roles to provide the necessary permissions.
- If the module is running as a service under the Network Service account, configuring permissions consists of assigning the Network Service account to one or more permission roles, possibly adding new roles or modifying existing roles to provide the necessary permissions. The only difference is that when adding the account to a role in the **Select User or Group** window of Intelligent Capture Administrator, you must add the machine account for the modules running under Network Service in the form of *<domain>**<machinename>*$.

Tip: Consider adding all such machine accounts to a domain group and then adding that group to the role. This will simplify ongoing permissions maintenance of Intelligent Capture modules running as services under Network Service.

For more information on adding users and groups to permission roles, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

Configuring Intelligent Capture to use Kerberos authentication

To configure authentication using Kerberos in your Intelligent Capture system, Kerberos protocol must be enabled on both client and server machines, and the correct service principal name (*SPN*) must be set for the Intelligent Capture Server.

Notes

- Each Intelligent Capture Server must have its own, unique *SPN*.
- The default `SecurityPackage` authentication setting for the Intelligent Capture Server and all Intelligent Capture clients is “Negotiate”. Kerberos authentication will work with this default setting.

To configure Intelligent Capture to use Kerberos authentication:

1. On the client machine, set the `SecurityPackage` key in the `settings.ini` file to “Negotiate” or “Kerberos”.

Note: If the `SecurityPackage` is set to “Negotiate”, the client machine attempts to connect to the Intelligent Capture Server using “Kerberos” authentication and then if that fails, defaults to using “NTLM” authentication. If the `SecurityPackage` is set to “Kerberos”, then the client machine only attempts to connect to the Intelligent Capture Server using “Kerberos” authentication that is explained in step 3 in this section.

If “Kerberos” authentication fails, then the client machine does not connect to the Intelligent Capture Server and the connection fails.

2. On the Intelligent Capture Server machine, set `SecurityPackage` to “Negotiate” or “Kerberos”.

Note: If any client machine is set to “Negotiate”, then the Intelligent Capture Server must be set to “Negotiate”.

3. Set a service principal name (*SPN*) for the Intelligent Capture Server by using the Microsoft Windows `setspn.exe` utility program to set the Intelligent Capture Server *SPN* as follows:

```
setspn -A <ServiceClass>/<Host>:<Port> [<MachineName>]
```

where:

- *<ServiceClass>*: Must be `IAServer`.
- *<Host>*: Fully qualified host name of the Intelligent Capture Server machine. This can be a fully-qualified *DNS* name or a NetBIOS name. Be aware that NetBIOS names are not guaranteed to be unique in a forest, so an *SPN* that contains a NetBIOS name may not be unique.
- *<Port>*: The port the Intelligent Capture Server is listening on (default: 10099).
- *<MachineName>*: The Microsoft Windows account used to run the Intelligent Capture Server service. When the Intelligent Capture Server runs under Local System account, the <*MachineName*> is the machine name of the Intelligent Capture Server. When the Intelligent Capture Server runs under a domain user account, the <*MachineName*> is the user account name.

Example:

```
1    setspn -A IAServer/prodserver.bigcorp.com:10099
2    setspn -A IAServer/prodserver.bigcorp.com:10099 prodserver
```

Notes

- To add the required *SPN*, you must have permission to write arbitrary SPNs in your domain. By default, only the domain administrator has this permission.
- Per domain, only one SPN may be registered for each Intelligent Capture Server.

2.3 Scalability

The modularity that is built into Intelligent Capture enables customers to configure and reconfigure their Intelligent Capture system to meet their changing needs. Both server and client subsystems are modular and scalable.

2.3.1 Intelligent Capture Server Scalability

When the document capture workload exceeds the capabilities of a single Intelligent Capture Server, scale up the system by adding more Intelligent Capture Servers and creating a ScaleServer group. A ScaleServer group combines multiple Intelligent Capture Servers into a single information capture system. Both attended and unattended modules can connect to the servers in a ScaleServer group, after which they can receive and process tasks from all connected servers. In addition to expanding the workload capacity over a single Intelligent Capture Server, ScaleServer groups can also help to ensure that client modules and their operators spend less idle time waiting for new tasks to arrive. Adjust the number of client modules and Intelligent Capture Servers to achieve the required balance of throughput. The ideal scenario is to have enough server capacity to process as many incoming batches as necessary while having enough client capacity to keep up with, but not exceed, the task processing requirements of the workload.

Most modules are ScaleServer compatible and therefore can connect to all Intelligent Capture Servers in the group simultaneously. Modules that are not ScaleServer compatible can connect to any one Intelligent Capture Server in the ScaleServer group at a time. (No module can connect to multiple arbitrary Intelligent Capture Servers—only to multiple servers that have been configured as a ScaleServer group.) "Appendix—Intelligent Capture Client Modules" on page 189 provides a table of client modules that indicates which modules are ScaleServer compatible.

Additional Intelligent Capture Servers can be added to a ScaleServer group when the Intelligent Capture system is initially configured or at any later time. For more information on managing and licensing ScaleServer groups, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*. For instructions on installing a ScaleServer group, see "Configuring Multiple Intelligent Capture Servers as a ScaleServer Group" on page 81.

Notes

- A ScaleServer group is not a redundant or failover system. ScaleServer technology provides process sharing as well as load balancing capabilities; it does not provide data redundancy.
- ScaleServer technology does not provide batch data sharing.

The Intelligent Capture Server is also scalable by virtue of its side-by-side installation capability. If using high-end server hardware with multiple cores, take advantage of the additional processing power by installing multiple side-by-side instances of the Intelligent Capture Server. This configuration may enable better parallel execution of batches when running on multi-processor machines. The actual

performance benefit depends on the task load and the types of tasks you are processing.

Side-by-side installation also enables multiple instances of the Intelligent Capture Server to be installed in an Active/Active Microsoft Failover Clustering, as explained in "High Availability and Failover" on page 34.

2.3.2 Client Scalability

Intelligent Capture client modules process tasks sent to them from Intelligent Capture Servers. Intelligent Capture design enables multiple modules to simultaneously process different tasks from all in-process batches. This means that production bottlenecks caused by slow modules can be resolved by adding more instances of those modules. Consider several factors when planning the number of each module required.

Volume

You need to consider the volume of incoming paper that must be processed.

Example 2-1:

A high-speed scanner with a skilled operator may be able to scan 20,000 pages per shift, but you may need to process 200,000 pages per 24-hour period. Intelligent Capture enables installing as many ScanPlus (and RescanPlus) machines as required to handle high workloads.

Processing power

You need to consider the amount of processing power the module needs.

Example 2-2:

An *OCR* module requires much more time to process a task (recognize a page of text) than an export module requires to export the same page of text. Intelligent Capture enables adding as many *OCR* modules as necessary to keep up with the system workload.

Time

You need to consider the amount of time an operator requires to process a task.

Example 2-3:

Manual indexing involving many fields that must be manually keyed by an operator takes more time than simple indexing tasks. Also, operator skill and other external factors affect the time required to process each task. Intelligent Capture enables adding as many Completion machines as needed to keep up with the indexing workload.

Additional client modules can be added to the system at any time after the initial installation without negatively impacting production. If using machines with multiple processors, multiple instances of certain modules can be installed as services on a single machine. "Appendix—Intelligent Capture Client Modules" on page 189 provides a table of client modules that indicates which modules may be installed and run as multiple service instances. "Manually Registering a Client Module to Run as a Service" on page 121 explains how to install modules as services using the <*serviceName*> command line argument.

2.4 Security

Various security providers interact with Intelligent Capture at various levels. Planning must include considerations for security and how it affects and secures the system.

Note: Security considerations related to SQL Server and the Intelligent Capture Database are applicable only if your configuration requires that the Intelligent Capture Database be installed.

Table 2-2: Security Considerations for an Intelligent Capture Installation

Element	Security considerations
SQL Server	Enable either SQL Server or Windows authentication. A SQL Server login ID having a SQL Server `dbcreator` role must be used to create the Intelligent Capture Database during the Intelligent Capture Database installation.
Intelligent Capture Database	The Intelligent Capture Database must have the database role membership set to **Public**. Intelligent Capture does not use user-based authentication or authorization for database access; therefore, you do not need to create database users and groups. Choose one of the following options for database access: • Create a SQL Server user account with either SQL Server or Windows authentication enabled. Grant the following permissions to the account: **Connect**, **Delete**, **Execute**, **Insert**, **Select**, and **Update**. Use this account to access the Intelligent Capture Database. This is the recommended approach. • Use the "sa" (system administrator) account. This is generally not recommended, because it gives unrestricted access to the entire SQL Server and all of the data it contains.

Element	Security considerations
Intelligent Capture Server	• The Intelligent Capture Server supports the least-privileged user account (*LUA*) approach in which users, programs, and services are granted only the minimum rights required to carry out assigned tasks. Configuring LUA for the Intelligent Capture Server is done automatically by the Intelligent Capture Server installation program. If this setup needs to be repeated (for example, due to the deletion of the special LUA group created by the setup program), instructions are provided in "Other Issues" on page 182. • The Federal Information Processing Standard (*FIPS*) provides best practices for implementing cryptographic software. The Intelligent Capture Server is designed to operate with Microsoft operating systems that use FIPS-compliant algorithms for encryption, hashing, and signing.

HTTP/HTTPS protocol	The Intelligent Capture Server supports the HTTP/HTTPS protocols. If enabled, use the following syntax:
	`http://<machine_name><[:port]>/<service_name>`
	`https://<machine_name><[:port]>/<service_name>`
	where
	• *<machine_name>*: name of the host machine
	• *<port>*: number of the port for HTTP or HTTPS requests
	– HTTP default: 80
	– HTTPS default: 443
	• *<service_name>*: the Intelligent Capture Server's service name

Element	Security considerations
TCP/IP protocol	The Intelligent Capture Server supports the TCP/IP protocol. TCP is a lower level protocol that lacks the security features of HTTP/HTTPS, so TCP is generally useful only in isolated networks. For either a standalone server or a ScaleServer group, specify the following properties to set server communications: • TCP/IP and port: Specify that the Intelligent Capture Server is to use the TCP/IP protocol and specify 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
Authentication	Intelligent Capture 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 and may use any of the authentication security providers used by Windows: *NTLM*, Kerberos, or Negotiate. In a multiple-domain environment, create trusts between the different domains so that cross-domain authentication can succeed. The minimum trust relationship required is "Nontransitive One-Way External Trust" from the domain with clients that need to authenticate to the domain that has servers which must perform the authentication.

Element	Security considerations
Client privileges	Client software can run under individual domain user accounts or the **Network Service** account. If client modules are run as services under the **Network Service** account, the client machine name must be added to the Module Operators role. Access to client modules can be controlled by using Intelligent Capture user roles and further refined by employing *ACL*s. User roles and *ACL*s are managed in Intelligent Capture Administrator. In addition, Intelligent Capture licensing globally restricts which components can run and how many components can connect to an Intelligent Capture Server at one time.

Element	Security considerations
User accounts	Consider using matching Windows user groups and Intelligent Capture roles for users to simplify permissions control. An administrative user account (as specified during server installation) is added to the **Administrator** role. This **Administrator** role is granted all the permissions to start and use all features of any component, including Intelligent Capture Administrator and all client modules. This default administrator user must create and configure the roles and permissions needed in Intelligent Capture Administrator, and then add users to these roles. This step is necessary to do before users can run client modules in production mode. Consider creating an "Intelligent Capture Supervisors" role with members having specific Intelligent Capture Administrator permissions and full permissions to run client modules, and an "Intelligent Capture Operators" role with members having full permissions to run client modules. Depending on security requirements, break down these roles into additional roles with finer divisions of permissions or members. Intelligent Capture requires that user accounts have passwords. Blank passwords are not supported in any scenario, even on a single-machine installation. **Note:** Default version of these roles with associated permissions are predefined in Intelligent Capture Administrator. Examine these default roles and change the permissions and then add new roles as required. Passwords must not contain "@" symbols because this symbol is used as a delimiter in command line arguments. Servers and client modules running as services can be configured to run under a specific user account or a built-in machine account. As with most software applications, the user installing Intelligent Capture components

Element	Security considerations
	must be a member of the machine's local **Administrators** group. In addition to user credentials and Windows permissions, all modules require that users be assigned to roles to which necessary permissions have been granted. These security roles are managed through Intelligent Capture Administrator.
Firewalls	Users are responsible for configuring firewall software in a compatible manner, as follows: • Ensuring that Intelligent Capture Servers can communicate with the Intelligent Capture Database (if installed). Firewalls in the path of the SQL Server that hosts the Intelligent Capture Database must be configured to pass network traffic on the *TCP* port 1433. **Note:** When installing an Intelligent Capture Server, you can change the port on which it listens for network traffic. The default port is 10099. Specify a different port after installation by specifying the **TcpIpPort** server parameter in the **Server Settings** pane in Intelligent Capture Administrator.

2.4.1 Running Intelligent Capture in a Hardened Environment

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 redundant services, enabling firewalls, blocking unused ports, and all the other details of 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.

2.4.2 Running Intelligent Capture with Minimum Microsoft Windows Permissions

Good security practice includes setting up machines to run applications with the minimum possible permissions. The following are the minimum Microsoft Windows permissions required for Intelligent Capture components:

Intelligent Capture Database (if installed)

User: A SQL Server user account with either SQL Server or Windows authentication. These permissions must also be enabled: **Connect**, **Delete**, **Execute**, **Insert**, **Select**, and **Update**.

Intelligent Capture Servers

User: Must be a member of the **InputAccel_Server_admin_group** group on the server machine. This group is created by the Intelligent Capture Server setup program and is granted the following privileges and permissions, which are the only rights required for the Intelligent Capture Server to function:

- Impersonate a client after authentication
- Load and unload device drivers
- Create global objects
- Full permissions on the Intelligent Capture Server data directory (`c:\ias`, by default) and all of its subfolders and files.
- Full permissions on the `InputAccel` registry key under `MACHINE\SYSTEM\CurrentControlSet\Services\`.
- Permission to activate and execute `DCom` objects

Note: You must set **Local Security Policy** > **Security Settings** > **Local Policies** > **Security Options** > **User Account Control: Run all administrators in Admin Approval Mode** to **Disabled**.

Programs:

- Intelligent Capture Server (`ias64.exe`) writes both the **InputAccel_Server_admin_group** *SID* and the Administrator (SECURITY_NT_AUTHORITY) SID on the *ACL* of all processes, batches, and other Intelligent Capture objects.
- Intelligent Capture Performance Counters (`iaspmdll64.dll`) uses shared memory with explicit permissions to read and write for authenticated accounts.

All modules

By default, the Intelligent Capture installer grants the required access to the specified folders and directories.

Directories:

- **All supported operating systems**: Users must have read/write access to the directory in which `settings.ini` resides, either `C:\Users\<user>\AppData\Local\VirtualStore\ProgramData\EMC\InputAccel` or `C:\ProgramData\EMC\InputAccel`.
- The account running the module must have Read/Write access to directories they are exporting to and to the location of the Recognition project.
- **All operating systems**: Users of modules listed as "Available prior to 6.0" in "Intelligent Capture Modules" on page 189 must have Read/Write access to `c:\Windows\win.ini`.

Registry: Users must have Read/Write access to the registry to enable the logging library to report performance counter information. Without this access, modules will run but will not report performance data. Note that modules new in 7.x (or later) do not require access to the logging library.

All modules listed as "New in 6.x" and "New in 7.0 - 7.7, 16.5, 16.6, 20.2" in "Intelligent Capture Modules" on page 189

User: Client machines must be members of the local **Users** group. Ensure that "Run-as" users have access to the network. To use command line arguments to install, remove, or change service settings, the user must be a member of the **Administrators** group. The account that is assigned to the service through the command line is automatically granted the **Service Logon** right.

Directories: The account running the module must have Read access to the .NET config directory and to other common Microsoft Windows directories such as `c:\Windows\System32`.

ScanPlus and Image Converter modules

Directories: The account running the module must have Read/Write access to the system `Temp` directory.

Standard Import

Directories:

- File System type: The user account must have Read access to watched directories, and must have Write access to watched directories if the files they contain are to be moved or deleted after they are imported.
- Email type: The user account running the module must have Read/Write access to the directory to which emails are copied.

Documentum Advanced Export

Directories: The account running the module must have Read/Write access to the Documentum user directory (`c:\Documentum`, by default) and to the system `Temp` directory.

Web Services Hosting

User: Must run as a named user (not a machine or built-in user). Running under an account with administrative rights simplifies the configuration.

Ports: If run under a non-Administrator account, the Administrator should reserve the ports used by the Hosting service for the named user to establish *HTTP* connections on those ports. Use the `PortReserve.exe` command line utility located in the `Client\binnt` directory of the Intelligent Capture installation directory to reserve these ports.

2.5 Installing Intelligent Capture Across Multiple Domains

The Intelligent Capture setup program is optimized for deploying the servers and clients within a single domain. In this environment, the setup program performs most or all of the required configuration automatically. However, a multi-domain environment is also supported.

In a multi-domain environment, configure the network to create trusts between the affected domains. Every time a cross-machine communication is performed, a security check is made. These security checks must succeed in order for the system to function properly.

The minimum cross-domain trust relationship required is "Nontransitive One-Way External Trust" from the domain with clients that want to authenticate to the domain that has servers that need to perform the authentication. Creating these trusts is an IT responsibility that uses operating system tools, and is beyond the scope of this documentation.

Notes

- To assign users or groups from other domains to Intelligent Capture security roles, Intelligent Capture Administrator must have the privileges 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" privilege 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.

2.6 Installing Intelligent Capture in a Workgroup

Installing Intelligent Capture in a workgroup is supported only in a development or demonstration system; that is, when all components are installed on a single machine. A machine in a Microsoft Windows workgroup must maintain its own list of users and groups, because it does not use the central security database of a domain. A "local user" is a user that has a security account on the local machine. Even though it is running on a single machine, Intelligent Capture still requires users to log in with a valid Microsoft Windows user name and password. Blank passwords are not allowed. For detailed instructions, see "Installing Intelligent Capture in a Development or Demonstration Environment" on page 127.

Note: When logging into a client module, specify a domain. If running Intelligent Capture on a single machine without a domain controller, specify "." or "localhost" in the **Domain** field of the **Login** window.

2.7 High Availability and Failover

Intelligent Capture uses several technologies to ensure high availability and failover protection.

Equipment, components, and strategies

Part of high availability includes choosing components and best practices designed to deal with faults. Examples include:

- High-performance *RAID* arrays for data storage redundancy and hot-swap capabilities.
- Key system components installed on datacenter style rack mount or blade server hardware using redundant power supplies.
- Battery backup/power protection systems to keep systems running or to perform an orderly shutdown if a power outage occurs.
- Remote monitoring and tuning software.
- VMware VMotion in lieu of clustering, enabling movement of virtual machines from one host to another if a system failure occurs.
- Offsite storage for short term, rotating backup of paper that has been scanned in addition to media containing backups of irreplaceable files.

ScaleServer groups

If an Intelligent Capture Server becomes unavailable due to a planned or unplanned interruption, other Intelligent Capture Servers in the same ScaleServer group automatically continue sending tasks to and accepting tasks from client modules. ScaleServer groups provide high availability during hardware and software failures; however, they do not provide failover because the tasks on the interrupted server are not rerouted and cannot be processed until the server again becomes available.

For instructions on installing and configuring ScaleServer groups, see "Configuring Multiple Intelligent Capture Servers as a ScaleServer Group" on page 81.

Modular clients

Client modules can be brought online to supplement or replace existing client modules without disrupting production. For client installation instructions, see "Installing the Intelligent Capture Client Components" on page 59.

Best practices

In addition to the high availability and failover mechanisms designed into Intelligent Capture, we recommend the following best practices for other critical system components when Intelligent Capture is used in mission-critical applications:

- At a minimum, connect the Intelligent Capture Server machine and the Intelligent Capture Database machine to an uninterruptible power supply.
- Configure the SQL Server for high availability by setting up database mirroring or clustering. For information and instructions, see Microsoft recommendations.
- Configure the Intelligent Capture Servers for high availability by using ScaleServer groups and configuring them in an Active/Passive or Active/Active Microsoft Failover Clustering cluster. For instructions, see "Configuring Multiple Intelligent Capture Servers as a ScaleServer Group" on page 81 and "Installing the Intelligent Capture Server in a Microsoft Failover Clustering Environment" on page 83.
- Run unattended client modules as services and configure those services for high availability by enabling automatic restart on failure.

2.8 Disaster Planning

Disaster planning is important for any business-critical application. The extent to which you plan for disaster and disaster recovery depends on your needs, your budget, and the importance of your document capture system to the continuation of your business. At one end of the spectrum is planning for routine backups of critical data, perhaps with offsite storage. At the other end of the spectrum, you might consider having multiple Microsoft Failover Clustering clusters in both local and remote locations, each with its own Storage Area Network (*SAN*), with automatic, real-time *SAN* replication.

Considerations for disaster planning

Some common themes of disaster planning and recovery include:

- Determining what to do in case the current production facility cannot function in any way.
- Planning for continuing production at another facility, possibly using equipment that is not currently available.

- Devising a way to redirect new work to the substitute production site.
- Arranging to re-process a certain quantity of work that may be lost if a disaster occurs.
- Planning for training of additional or replacement personnel to help carry out the plan.
- Periodically testing the disaster recovery plan to ensure everything functions as needed if a disaster occurs.

Pricing

Disaster recovery pricing, which provides licensing and activation for periodic testing and one-time use of a disaster continuation system, is offered.

2.8.1 Creating an Intelligent Capture Disaster Continuation Plan

Disaster recovery planning should include a written plan describing exactly how to restore Intelligent Capture production after a disastrous event.

Key questions

When writing the disaster continuation plan, consider the following questions:

- Who are the key personnel responsible for rebuilding the Intelligent Capture system and restoring production?
- Who will act in your place?
- Where will the documentation be kept?
- Who will provide backup for key team members that may be unavailable?
- How will you train replacement or temporary workers?
- How long will it take to restore full production throughput?
- What will happen if you need to relocate your department to another location?

2.8.2 Disaster Recovery Considerations

Disaster recovery can encompass much more than simple backups and redundancy. If planning to put in place a simple backup plan, consider making both local and off-site backups of the following critical components:

- Directory trees from each of your Intelligent Capture Server `IAS` directories
- Intelligent Capture Database from SQL Server
- Scanner drivers
- License files

- Patches
- Custom server and client software (from your own or third-party developers/ OpenText Global Technical Services)
- Custom client desktop shortcuts
- Client side script source code
- Client `win.ini` and `settings.ini` files

"Irreplaceable Files and Data" on page 135 provides a detailed list of files that should be backed up together with their default locations on server and client machines.

2.8.3 Implementing a Disaster Continuation System

Implementing a robust Disaster Recovery system is complicated, detailed and specific to each customer's environment. Contact OpenText Global Technical Services at My Support (https://support.opentext.com) for help in planning, implementing, and testing a Disaster Recovery environment.

2.9 Licensing and Activation

Intelligent Capture uses a server-based licensing system that enables Intelligent Capture as well as third-party module developers to regulate how their software is used in an Intelligent Capture installation. Licenses are installed on each Intelligent Capture Server. When a client module connects, the Intelligent Capture Server checks for a valid license before allowing the module to operate.

License codes are uniquely keyed to the Server *ID* that the Intelligent Capture Server retrieves from its security key. Each license code specifies a single module and regulates how many copies of the module can concurrently connect to the Intelligent Capture Server, how many pages the module is allowed to process, how long the license is allowed to work, and what extra features are enabled.

The Intelligent Capture Server uses an activation file, which controls the licensing of the Intelligent Capture system. Be aware that each Intelligent Capture Server requires a separate activation step. Contact OpenText Global Technical Services at My Support (https://support.opentext.com) to do any of the following:

- Obtain a new activation code for a new installation.
- Obtain a new activation code after a hardware, software, or configuration change.
- Obtain an **Enter By** extension.
- Initiate a Server ID migration when moving an Intelligent Capture Server to a different machine.

Note: Use activation file (software) security keys with side-by-side Intelligent Capture Server installations. For more information on side-by-side

installations, see "Installing Multiple Instances of Intelligent Capture Servers" on page 79.

To install and manage license codes, and to activate Intelligent Capture Servers using activation files, use Intelligent Capture Administrator. You will typically receive a file containing all of your license codes, which you can import to your Intelligent Capture Server in a single step. You can also manually type license codes one at a time. For more information on licensing and activation, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

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

For more information about the Intelligent Capture REST Services Licensing tool, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

2.9.1 ScaleServer Licensing

Intelligent Capture licensing for ScaleServer enables multiple Intelligent Capture Servers to be configured so that all modules can connect to them. ScaleServer groups are defined and managed in Intelligent Capture Administrator. Each Intelligent Capture Server that is to be a part of a ScaleServer group must have license codes that enable it to participate in the group and to enable the client modules to connect to the group.

The Intelligent Capture Servers within a ScaleServer group share page count and connection licenses to facilitate load balancing.

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.

A ScaleServer license is included with certain levels of Intelligent Capture licensing and is an available option in other license levels. Contact OpenText Global Technical Services at My Support (https://support.opentext.com) if unsure about the features included with your license.

Example 2-4: ScaleServer groups

- Server 1 and Server 2 are each licensed to process 50,000 pages/day, for a total ScaleServer capacity of 100,000 pages/day.
- Three hours before the end of the day, Server 1 has reached its 50,000 page limit, but Server 2 has processed only 25,000 pages.
- Server 1 automatically transfers from the Server 2 license enough page capacity to continue working either until the end of the day or until 100,000 pages have been processed by the Intelligent Capture system in that day.

This is a simple example, but the logic applies to more complex scenarios, where you may have eight Intelligent Capture Servers in a ScaleServer group,

all having different remaining daily page counts. For instructions on setting up ScaleServer groups and managing licenses, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

2.9.2 Licensing for Use in a Microsoft Cluster

Intelligent Capture licensing for clustering enables multiple Intelligent Capture Servers to be configured in an Microsoft Failover Clustering Active/Passive or Active/Active cluster. A standard Intelligent Capture Server license does not enable the server to run as part of a cluster.

For detailed information on configuring multiple Intelligent Capture Server instances in an Microsoft Failover Clustering cluster, see "Installing the Intelligent Capture Server in a Microsoft Failover Clustering Environment" on page 83. For instructions on installing and managing licenses, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

2.9.3 Licensing for Disaster Recovery

Certain levels of Intelligent Capture licensing include licenses for implementing, testing, and using a disaster recovery system. If unsure about whether your licensing level includes a disaster recovery system, contact OpenText Global Technical Services at My Support (https://support.opentext.com). For information on setting up a disaster recovery system, see "Disaster Planning" on page 35. For instructions on installing and managing licenses, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

2.10 Sample Production Installation Configurations

"Production Installation Configurations of an Intelligent Capture System" on page 39 shows the Intelligent Capture configurations that can be used in a small volume deployment, a high volume deployment, and a high-availability deployment.

Note: A complex enterprise installation scenario is discussed in detail in "Installing Intelligent Capture in a Production Environment" on page 47.

Table 2-3: Production Installation Configurations of an Intelligent Capture System

Server/Machine	Small Volume	High Volume	High Availability
SQL Server Machine 1	(Optional) Intelligent Capture Database hosted by SQL Server	(Optional) Intelligent Capture Database hosted by SQL Server	(Required) Intelligent Capture Database hosted by SQL Server installed in a Microsoft cluster

Server/Machine	Small Volume	High Volume	High Availability
SQL Server Machine 2	-	-	(Required) Intelligent Capture Database hosted by SQL Server installed in a Microsoft cluster
Intelligent Capture Server Machine 1	Intelligent Capture Server	Intelligent Capture Server	Intelligent Capture Server installed side-by-side and configured in a Microsoft Failover Clustering ServerActive/Active cluster
Intelligent Capture Server Machine 2	-	-	Intelligent Capture Server installed side-by- side and configured in a Microsoft Failover Clustering Active/ Active cluster
Client Module Machine 1 (a)	• Intelligent Capture Designer • Intelligent Capture Administrator	• Intelligent Capture Designer • Intelligent Capture Administrator	Intelligent Capture Designer
Client Module Machine 1 (b)	-	-	Intelligent Capture Administrator
Client Module Machine 2	• Completion • ScanPlus	ScanPlus	ScanPlus
Client Module Machine 3 (multiple)	Other client modules	Completion	Completion
Client Module Machine 4 (multiple)	-	Other client modules	Web Services Hosting Web Services Coordinator

Server/Machine	Small Volume	High Volume	High Availability
Web Server Machine 5 (Multiple) **Note:** Multiple Intelligent Capture REST Service Web machines can work with the same IA ScaleServer group.	• Intelligent Capture REST Service • Your custom Intelligent Capture REST Service authentication plug-in • Intelligent Capture Web Client	• Intelligent Capture REST Service • Your custom Intelligent Capture REST Service authentication plug-in • Intelligent Capture Web Client	• Intelligent Capture REST Service • Your custom Intelligent Capture REST Service authentication plug-in • Intelligent Capture Web Client
Machine 6 (Storage Device)	Intelligent Capture REST Service and Module Server shared data storage	Intelligent Capture REST Service and Module Server shared data storage	Intelligent Capture REST Service and Module Server shared data storage
Machine 7 (multiple)	Module Server	Module Server	Module Server
Client Module Machine 8 (multiple)	-	-	Other client modules
Client Module Machine 9 (multiple)	-	Other client modules	Other client modules
Client Browser Machine 10 (multiple)	Browser access to Intelligent Capture Web Client	Browser access to Intelligent Capture Web Client	Browser access to Intelligent Capture Web Client
Mobile Devices (multiple) **Note:** Hereafter, *mobile devices* include phones and tablets.	Your custom mobile capture application **Note:** Custom mobile capture applications are developed using the PixTools for Mobile, which is packaged separately from Intelligent Capture.	Your custom mobile capture application	Your custom mobile capture application

Chapter 3

Installation Planning for Intelligent Capture Real Time Services

Many of the same installation planning considerations for an Intelligent Capture system also apply to Intelligent Capture Real Time Services; however, this section describes considerations specific to Intelligent Capture Real Time Services.

3.1 Scalability

For scaling the Intelligent Capture Real Time Services (including Intelligent Capture REST Service, Intelligent Capture Web Client (as well as any other custom clients)), the following guidelines are recommended:

- One Web server for 750 concurrent users.
- One Module Server for 20 concurrent users.
- Each Module Server should have 16 instances of each module type (Extraction, Full Page OCR, Image Converter, Image Processor, Scripting) and have the following:
  - 8 CPUs
  - 24GB RAM
- For batch storage, estimate the number and sizes of the files and images in your typical batch as well as the number concurrent users and then, to ensure reliable performance and account for overhead, double that size.

Example 3-1: How to calculate batch storage

The following batch requires 4GB of storage:

- 200KB per image or file
- 100 images or files per batch
- 100 concurrent users

(200KB x 100 images/files x 100 concurrent users = 4GB)

3.2 Security

The following components are hosted by IIS, which should 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
- Intelligent Capture Web Client

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

3.3 Running with Minimum Permissions

Shared data folder

If you are running multiple instances of Intelligent Capture REST Service and the Module Server, make sure all of them specify the same shared data folder; in addition, the shared data folder must be `read/write/delete/create` accessible from all of the instances.

The following minimum permissions are required for a user account to run the Module Server under it.

- Log on as service.
- Replace a process level token.
- Create global objects.
- Load and unload device drivers.
- Permission to activate and execute DCom objects.

Additionally, the user account must have full permissions to the REST shared data folder.

Application pool identity tasks

For each Intelligent Capture REST Service Web application's **Application Pool** identity, perform the following:

- 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 Microsoft 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 Capture REST 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**.

3.4 High Availability Best Practices

Configure the Intelligent Capture REST Services and Module Servers for high availability by setting up clustering or a Web farm.

To avoid a single point of failure (SPOF), you could also include the shared data folder, which contains temporary image capture files and other state information as well as a shared configuration file, in your high availability setup. For example, you could use disk technologies that offer HA/DR, virtualization (VFS) and scale-out options, which are typical for NAS/SAN systems. In addition, you could use the continuously available file share (CAFS) feature (available with Microsoft Windows 2012 or later) or other similar technologies.

Note: The high availability system must support addressing the shared data folder through an absolute or UNC path.

3.5 Disaster Recovery

Disaster recovery can encompass much more than simple backups and redundancy. If planning to put in place a simple backup plan, consider making both local and off-site backups of the following critical components:

- Intelligent Capture REST Services shared data folder (except for the `Sessions` subfolder)

If you require assistance with disaster planning, contact OpenText Professional Services.

Chapter 4

Installing Intelligent Capture in a Production Environment

This section explains how to install Intelligent Capture and Intelligent Capture Real Time Services into a typical production environment and also presents some complex installation scenarios. This installation includes the option of installing the Intelligent Capture Servers in a clustered environment to ensure high availability.

Note: Intelligent Capture Real Time Services uses the same installer as Intelligent Capture.

Table 4-1: Production Installation of an Intelligent Capture System

Server/Machine	Component to install	User Account	Runs as
Server 1	(Optional in general, but required for Web Services) Intelligent Capture Database hosted by SQL Server. Configuring SQL Server in a clustered environment for high availability is recommended.	N/A	N/A
Server 2a	Intelligent Capture Server	User in the local **InputAccel_Server_admin_group** group	Service
Server 2b	Intelligent Capture Server	User in the local **InputAccel_Server_admin_group** group	Service
Machine 4	Intelligent Capture Designer	Domain user	Application
Machine 5	Intelligent Capture Administrator	Domain user	Application
Machine 6	ScanPlus	Domain user	Application
Machine 7	RescanPlus	Domain user	Application
Machine 7	Completion	Domain user	Application
Machine 8	Identification	Domain user	Application

Server/Machine	Component to install	User Account	Runs as
Machine 9 (multiple)  **Note:** Web Services Coordinator can only be installed on a single machine in the Intelligent Capture system.	(Optional and requires the Intelligent Capture Database) • Web Services Coordinator • Web Services Hosting • Web Services Input • Web Services Output	Domain user	Service only
Machine 10 (multiple)  **Note:** Multiple Intelligent Capture REST Service Web machines can work with the same IA ScaleServer group.	(Optional) • Intelligent Capture REST Service • Your custom Intelligent Capture REST Service authentication plug-in • Intelligent Capture Web Client	Domain user	Web application
Machine 11 (Storage Device)	(Optional) Intelligent Capture REST Service and Module Server shared data storage	N/A	N/A
Machine 12	Module Server	**Network Service**	Service
Machine 13	Image Processor	**Network Service**	Service
Machine 14	NuanceOCR	**Network Service**	Service
Machine 15	Documentum Advanced Export	**Network Service**	Service
Machine 16	• Multi • Image Converter	**Network Service**	Service
Machine 17	Standard Import	**Network Service**	Service
Machine 18	Standard Export	**Network Service**	Service
Machine 19 (multiple)	Other unattended client modules	**Network Service**	Service

Server/Machine	Component to install	User Account	Runs as
Machine 20 (multiple)	Browser access to Intelligent Capture Web Client	Domain user	Browser application
Mobile Devices (multiple)	Your custom mobile capture application **Note:** Custom mobile capture applications are developed using PixTools for Mobile, which is packaged separately from Intelligent Capture.	Customer-defined	Customer-defined

To install Intelligent Capture in a typical production environment:

1. Make sure the servers and machines meet the system requirements outlined in the *Release Notes*. For the best performance, always use the vendor's latest operating system (that Intelligent Capture supports) for all Intelligent Capture components. Furthermore, you should always make sure that you have applied the latest service packs and patches to your supported operating system for all Intelligent Capture components. In addition to meeting the other recommended system requirements, keeping your operating system up-to-date helps to ensure the best performance for your Intelligent Capture system.
2. (Optional) Install Intelligent Capture Database on Server 1. For instructions on installing the Intelligent Capture Database, see "Installing the Intelligent Capture Database" on page 51.
3. Install the Intelligent Capture Server. You have the following options:
   - Install the Intelligent Capture Server on a single machine, Server 2. For instructions, see "Installing the Intelligent Capture Server" on page 54.
   - Install multiple instances of the Intelligent Capture Server on a single machine, Server 2. For instructions, see Installing multiple instances of the Intelligent Capture Server.
   - Install the Intelligent Capture Server on multiple machines, Server 2a and Server 2b, and optionally configure them as a ScaleServer group.
   - Install the Intelligent Capture Servers in a clustered environment and then configure them as a ScaleServer group. For instructions on installing Intelligent Capture Servers in an Active/Passive or Active/Active clustered environment, see "Installing the Intelligent Capture Server in a Microsoft Failover Clustering Environment" on page 83.

Note: The Intelligent Capture Database is required to configure Intelligent Capture Servers as a ScaleServer group and to install the servers in a clustered environment.

4. Install development tools, Intelligent Capture Administrator, attended client modules, Completion, ScanPlus, RescanPlus, and Identification as applications on each machine designated for these modules according to the installation plan. For instructions, see "Installing the Intelligent Capture Client Components" on page 59.

5. (Optional) Install Web Services Coordinator, Web Services Hosting, Web Services Input, and Web Services Output client modules on a separate machine.

6. (Optional) Install the Intelligent Capture REST Service (stand-alone) and any custom applications that use it as follows:

   a. Install and configure the Intelligent Capture REST Service and your custom Intelligent Capture REST Service authentication plug-in on a separate machine.

   b. Create an appropriate location for Intelligent Capture REST Service shared data storage and specify it in the Intelligent Capture REST Service configuration tool.

   c. Deploy your custom applications that use the Intelligent Capture REST Service.

7. (Optional) Install the Intelligent Capture Web Client and Intelligent Capture REST Service as follows:

   a. Install and configure Intelligent Capture Web Client, Intelligent Capture REST Service, and your custom Intelligent Capture REST Service authentication plug-in.

      A custom Intelligent Capture REST Service authentication plug-in provides more flexibility for authenticating users of the Intelligent Capture REST Service. For more information, see *OpenText Intelligent Capture - Scripting Guide (ECPCORE-PSC)*.

   b. Create an appropriate location for Intelligent Capture REST Service shared data storage and specify it in the Intelligent Capture REST Service configuration tool.

   c. Deploy your custom applications that use the Intelligent Capture REST Service.

8. (Required for Intelligent Capture Web Client; optional, otherwise) Install the Module Server on a separate machine.

9. Install the other unattended client modules as services on each machine designated for these modules according to the installation plan.

   Note: For a list of client modules that can be run in unattended mode and as services, see "Intelligent Capture Modules" on page 189.

10. (Optional) Set the UI language for the different Intelligent Capture components.
11. Run Intelligent Capture Administrator. Configure the Web Services Coordinator and Web Services Hosting components. For details, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

4.1 Installing the Intelligent Capture Database

The Intelligent Capture Database is an optional component. To understand the scenarios under which you will need to install the Intelligent Capture Database, see "Database Server Considerations" on page 13.

Before installing the Intelligent Capture Database, obtain and install your own copy of SQL Server to host the database. SQL Server must be configured with the following settings:

- Have a user account that is part of the SQL Server `dbcreator` role.
- Allow *TCP/IP* protocol access through the default port 1433. If TCP/IP is not enabled, then configure SQL Server Express in the SQL Server Configuration Manager to allow TCP/IP protocol access through the default port 1433. Enable TCP/IP protocol for each *IP* address used by the system and then restart the SQL Server Express service. Not configuring the SQL Server Express to allow for TCP/IP access will lead to connection errors when installing the Intelligent Capture Database.
- Enable the appropriate authentication mode in SQL Server Management Studio, and then restart the SQL Server service.

Caution

It is recommended that you disable antivirus software and Data Execution Prevention (*DEP*), and close any open programs before installing the Intelligent Capture Database.

Notes

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

  The *Release Notes* provide more information about supported versions of SQL Server. This document is available from the **Start** menu of your desktop at **All Programs > OpenText Intelligent Capture > Documentation**.
- Due to limitations built into SQL Server Express, it should only be used in low page volume deployments with minimal logging.
- The installer requires an account that is a member of the local **Administrators** group on the machine from which you are running the setup program.

To install the Intelligent Capture Database:

1. Start the Intelligent Capture setup program from the installation media. If the setup program does not start automatically after a few seconds, or if running the installation from a local disk or network share, open the file `autorun.exe` to begin.
2. Select **Install Product** and then from the **Installation Choices** list, select **Step 1 - Install Intelligent Capture Database** and then select the language of the installation and click **Next**.
3. If prompted to install prerequisite applications, click **Install**.
4. Accept the license agreement and click **Continue**.
5. In the **Destination Folder** window, click **Next** to install required files and scripts to the default destination folder or click **Change** to select a new location.
6. In the **Configure Database** window, select the **Create Intelligent Capture (IC) and Information Extraction (IE) Databases** option and type names for the Intelligent Capture and Information Extraction databases.
7. From the **Authentication** field, specify one of the following:

   - **SQL Server Authentication**

     SQL Server administrative login credentials for the SQL Server.

   - **Windows Authentication**

     The Microsoft Windows user account must be a SQL Server account with the appropriate permissions on the database. For more information, see "Creating a SQL Server User Account with Minimum Permissions to Access the Intelligent Capture Database" on page 54.

   Note: If the **Copy Script Only** option is selected, the Database executable and scripts are copied to the target machine but the Intelligent Capture Database is not created. The IADBManager executable must be manually run to create the database. "Appendix—Using the Database Manager Utility" on page 205 provides instructions for manually creating the Intelligent Capture Database. For information about the Information Extraction database, see "Manually Creating the Information Extraction (IE) Database" on page 208.

8. Type valid login credentials for the Intelligent Capture Database and click **Next**.

   You must use a SQL Server login ID with the SQL Server `dbcreator` role.

Caution

Use of non-code page Unicode characters in the setup program may cause data corruption and installation failure. Only specify characters from the code page of the machine running the setup program.

Notes

- If the **Create the Intelligent Capture (IC) and Information Extraction (IE) Databases** option is selected, the local **Database Server**, **SQL Server Port**, and Database names for the Intelligent Capture and Information Extraction databases must be specified. A database name can have only the following characters: a-z, 0-9, _, $, #, @, and first character may only be a-z, 0-9, or an underscore (_). (The default SQL Server port is 1433. For all SQL Server versions, including the Express editions, make sure *TCP/IP* is enabled and a port is set before installing the Intelligent Capture Database.)
- If using a named instance for the SQL Server, be sure to specify the Database Server in this format:

  `[machine_name]\[instance_name]`.
- For SQL Server Express, the default instance name is `SQLExpress`.

9. In the **Configure IE Database Connection** window, type valid login credentials for the Information Extraction database. Click **Next**.
10. Check your settings, and then click **Ready to Install**.

Note: The Intelligent Capture Database and Information Extraction database cannot be installed onto a compressed drive.

11. To verify a successful installation of the Intelligent Capture and Information Extraction Databases, run SQL Server Management Studio, and expand the **Databases** folder in the **Object Explorer** pane. The Intelligent Capture Database (default name: `IADB`) and Information Extraction database (default name: `IEDB`) should appear in the list of databases.
12. Create a user account for SQL Server and set permissions for this user account to run the Intelligent Capture Database. "Creating a SQL Server User Account with Minimum Permissions to Access the Intelligent Capture Database" on page 54 provides the appropriate settings.

Note: You may need to change SQL Server credentials after installing the Intelligent Capture Database. If credentials change, you must run the Data Access Layer Configuration utility, `DalConfig64.exe` (default location: `C:\Program Files\InputAccel\Server\Server\binnt\DalConfig64.exe`), to update the database connections on each server machine. For details about using this utility, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

4.1.1 Creating a SQL Server User Account with Minimum Permissions to Access the Intelligent Capture Database

If the Intelligent Capture Database is created, a SQL Server user account with restricted access must also be created. This user account must then be specified for the DAL registration during the Intelligent Capture Server and Client Components installation.

Caution

At no time should a system administration account be used in production environments for DAL registration. Using an account with full permissions is a security risk.

The production SQL Server user account must be configured with the following:

- The **Default database** must be set to the Intelligent Capture Database.
- The user account must be mapped to the Intelligent Capture Database and the database role membership must be set to **Public**.
- Grant the following permissions to the Intelligent Capture Database:
  - **Connect**
  - **Delete**
  - **Execute**
  - **Insert**
  - **Select**
  - **Update**

4.2 Installing the Intelligent Capture Server

The Intelligent Capture Server is an open integration platform that manages and controls the document capture process by routing document pages along with processing instructions to the appropriate client modules.

Caution

- The machine name of the Intelligent Capture Server must not be longer than 15 bytes; otherwise, client machines will be unable to connect.
- It is recommended that you disable antivirus software and Data Execution Prevention (*DEP*), and close any open programs before installing the Intelligent Capture Server.

This procedure installs a single Intelligent Capture Server and documentation.

Notes

- The installer requires an account that is a member of the local **Administrators** group on the machine from which you are running the setup program.
- Intelligent Capture does not install any versions of Microsoft .NET Framework.

To install the Intelligent Capture Server:

1. Start the Intelligent Capture setup program from the installation media. If the setup program does not start automatically after a few seconds, or if running the installation from a local disk or network share, open the file `autorun.exe` to begin.
2. Select **Install Product** and then from the **Installation Choices** list, select **Step 2 - Install Intelligent Capture Server** and then select the language of the installation and click **Next**.
3. If prompted to install prerequisite applications, click **Install**. The prerequisite software for the Intelligent Capture Server is installed.
4. Accept the license agreement and click **Continue**.
5. (Optional) In the **Database and Failover Options** window, select **Use an external MSSQL Database** if you have installed the Intelligent Capture Database and **Use Microsoft Failover Cluster Environment** if you want to install the server in a clustered environment. Both of these options require that the Intelligent Capture Database is installed. Information on installing the server in a clustered environment is provided in *OpenText Intelligent Capture - Installation Help (ECPCORE-H-IGD)*. If these options are cleared, then the server installs a file-based, internal database.
6. Select one of the following setup types, and then click **Next**:

   - **Typical**: Performs the default installation on the default `C:\` drive.

   Custom: Enables you to select the number of Intelligent Capture instances and the drive to which to install the Intelligent Capture Server application files and the Intelligent Capture Server data files.

Caution

- Although supported, specifying a *UNC* path for the `IAS` folder is not recommended because it causes degradation in server performance. If you do install the `IAS` folder to a UNC path, you may encounter errors. To resolve the error, see the UNC path recommendations in "Installation Errors" on page 176.
- If the `IAS` folder is placed on a network shared drive, then the Intelligent Capture Server must always run under the Local System or an Administrator account.

7. In the **Configure Intelligent Capture Service Accounts** window, select one of the following to specify the credentials to run the server:

   - **Use the built-in Local System account**: Uses the credentials of the built-in Local System account.
   - **Specify a user account**: Uses the credentials entered in the **Username**, **Password**, and **Domain** fields.

   Note: The setup program automatically adds the specified local or domain user to the *LUA* group: **InputAccel_Server_admin_group**, enabling the Intelligent Capture Server to operate with a least-privileged user account. Details of the LUA configuration can be found in "Running Intelligent Capture with Minimum Microsoft Windows Permissions" on page 31.

   Caution
   Local user accounts are supported only when all components are installed on a single machine in a Workgroup instead of a Domain.

   Caution
   Use of non-code page Unicode characters in the setup program may cause data corruption and installation failure. Only specify characters from the code page of the machine running the setup program.

   - Select **Automatically start the Intelligent Capture Server service when the system starts** if you want the Intelligent Capture Server to be started as a service automatically when the system starts, and then click **Next**.

8. (Optional. This window displays only if you specified that you are using an external MSSQL database.) In the **Data Access Layer Registration** window, specify the login credentials for connecting to the SQL Server. The login credentials are one of the following:

   - The SQL Server user account created that provides permissions to access the Intelligent Capture Database.
   - Windows Authentication

     The Microsoft Windows user account must be a SQL Server account with the appropriate permissions on the database. For more information, see "Creating a SQL Server User Account with Minimum Permissions to Access the Intelligent Capture Database" on page 54.

   Note: If the machine where the Intelligent Capture Server is installed also has SQL Server installed, then by default **Register the Data Access Layer with the Intelligent Capture database** is selected and the local database server, default SQL Server port 1433, and Database name are specified.

9. In the **Configure Intelligent Capture Administrator User** window, specify the credentials of a user you want added to the Intelligent Capture **Administrator** role. 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.

   If you want to use Intelligent Capture Administrator to access the Intelligent Capture Server from another domain, then this user account must be a domain user account—not a local Windows account. In addition, this user account must meet the requirements in "Installing Intelligent Capture Across Multiple Domains" on page 33.

   Note: This user does not have to be a Microsoft Windows Administrator.

10. By default, **Start the Intelligent Capture Server service when setup completes** is selected. Clear the check box if you want to start the Intelligent Capture Server service manually when setup completes. Click **Next**.

11. Click **Finish**.

    Note: A log file is written when the installer sets the *LUA* permission and other server environment configurations. Users must check this log file, which is written to the `Server\binnt\iassetenv<timestamp>.log`, if errors occur during installation.

12. To verify that the Intelligent Capture Server has been successfully installed, open the Microsoft **Services** window (click **Start** > **Programs** > **Administrative Tools** > **Services**) and start theIntelligent Capture Server service.

    Caution

    The Intelligent Capture Server stops unexpectedly if the Intelligent Capture Server is running with Microsoft **Data Execution Prevention** (*DEP*) feature enabled. Make sure the DEP feature is disabled on the machine where Intelligent Capture Server is running.

13. To set up the properties for server communications (TCP/IP or HTTPS), see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

4.2.1 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 "Installing Intelligent Capture Servers into Microsoft Failover Clustering" on page 84.

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. Login 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 shutdown.

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

4.3 Installing the Intelligent Capture Client Components

For more information about the client components that you can install, see "Appendix—Client Module Features" on page 197.

Before you begin, do the following:

- Disable antivirus software and Data Execution Prevention (*DEP*), and close any open programs before installing the Client Components.
- Make sure that there are no pending Microsoft Windows updates before you start the Intelligent Capture client installer. If there are pending Microsoft Windows updates, install them first before starting the Intelligent Capture client installer.
- Ensure that the machine does not require to be restarted before you begin the client installation.

The installer requires an account that is a member of the local **Administrators** group on the machine from which you are running the setup program.

Tip: Because of the limited number of printer ports, do not install Intelligent Capture client modules and the Module Server on the same machine.

Note: Intelligent Capture does not install any versions of Microsoft .NET Framework.

To install Intelligent Capture Client Components:

1. Start the Intelligent Capture setup program from the installation media.

   If the setup program does not start automatically after a few seconds, or if running the installation from a local disk or network share, open the file `autorun.exe` to begin.

2. Select **Install Product** > **Installation Choices** > **Step 4 - Install Client Components** and then select the language of the installation.

   You might be prompted to install prerequisite software for the client modules.

3. Select the features to install.

   Each setup type preselects features that are appropriate for the installation scenario. The available features are listed in "Appendix—Client Module Features" on page 197.

   Note: Before installing the Image Converter module with the Virtual Printer feature, the **Print Spooler** service must be running to install the virtual printer.

   a. In **Setup Type**, select a setup type.

b. In the next dialog box, change the preselected features by expanding each available feature and selecting features and sub-features.

Features that are not selected, are marked with a red X.

Note: If third-party software that is required to run the client modules is not already installed, then the**Required Third-party Software** window is displayed. The specified client modules are installed, but will not run until the required third-party software is installed.

4. To specify a user account to use when logging in to the module, select one of the following:

- **Use the built-in Network Service account**: Uses the local machine's **Network Service** account

Note: If you select **Use the built-in Network Service account**, unless all Intelligent Capture components are installed on a single system or the Intelligent Capture Server has been configured to allow anonymous access, you must configure the Intelligent Capture system to use Kerberos authentication, as explained in "Configuring Intelligent Capture to use Kerberos authentication" on page 21

- **Specify a user account**: Uses the credentials specified to run client modules as services.

Caution

Use of non-code page Unicode characters in the setup program may cause data corruption and installation failure. Only specify characters from the code page of the machine running the setup program.

5. If you want the Intelligent Capture client modules to be started as a service automatically when the system starts, select **Automatically start all services when the system starts**.

Caution

If all client modules that can run as services are installed on a single machine, having them all start automatically will significantly impact the startup of that machine.

6. In the **Intelligent Capture Server Connection Information** window, specify the **Server name** and **Server port** of the Intelligent Capture Server to connect to.

Add a semicolon (`;`) after the server name to connect to a ScaleServer group.

To make sure that you have specified the connection correctly, make sure that **Try to contact the server during this installation** is selected. This option enables the setup program to attempt to establish a connection with the Intelligent Capture Server. If the attempt fails, you might want to verify that theIntelligent Capture Server service is started. However, even if the server

connection does not succeed, you can still proceed with the installation of the client modules. That is, restarting the server is not mandatory.

Caution

If the Intelligent Capture Server host name contains Unicode characters from a code page other than the code page of the client machine, do not specify that name in the **Intelligent Capture Server Connection Information** window. The non-code page characters may cause installation errors. Instead, proceed as follows:

- Return to the **Intelligent Capture Server Connection Information** window and for the **Server Name** specify the Intelligent Capture Server machine's *IP* address.
- Proceed with the client installation. The first time you run each client module, specify the correct Intelligent Capture Server name when logging in.
- If you want to configure modules to run as services, use the instructions provided in "Manually Registering a Client Module to Run as a Service" on page 121.

7. (Optional) If you have selected to install the Module Server, see "Installing and Configuring the Module Server" on page 111.

8. Verify that the Intelligent Capture Server service is started on the machine where the Intelligent Capture Server is installed.

9. (Optional) If **Internet Explorer Enhanced security** is enabled, then you must add `127.0.0.1` to Internet Explorer's **Trusted Sites** or **Intranet Zones** for Intelligent Capture Administrator to work properly.

   You could also change `127.0.0.1` to `localhost` in `binnt\CaptivaAdministrator.exe.config` in the following element:

```
1 <setting name="Host" serializeAs="String">
2      <value>127.0.0.1</value>
3 </setting>
```

10. Ensure that the default administrator user logs in to Intelligent Capture Administrator, and then assigns appropriate permissions to users and adds users to Intelligent Capture roles. This is required before users can run client modules in production mode. Without this step, users will be unable to log in and process tasks. For more information, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

Note: An administrative user account (as specified during server installation) is added to the **Administrator** role. This **Administrator** role is granted all the permissions to start and use all features of any Intelligent Capture component, including Intelligent Capture Administrator and all client modules.

11. Verify that the client modules have been installed successfully.

    Start a client module by clicking **Start** > **Programs** > **OpenText Intelligent Capture**, selecting the module type and then the module, and logging in with your Intelligent Capture Server login credentials.

4.3.1 Installing Multiple Instances of Image Converter

To use multiple instances of Image Converter simultaneously, manually install additional instances of the Image Converter module as a service. Each service instance can be installed with a virtual printer; for ease of identification, the name of the printer includes the name of the service instance.

Note: When installing Image Converter, you can optionally install the Virtual Printer feature. The virtual printer is required for the following Image Conversion profile properties:

- **HTML Rendering Engine** is set to **Internet Explorer** or **Microsoft Word**
- **Office Documents Rendering Engine** is set to **Microsoft Office Engine**

If any of the aforementioned properties are set to **Embedded Image Converter Engine**, then the virtual printer is not required. For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.

By default, virtual printers connect to Line Printer Terminal (*LPT*) ports. If all available *LPT* ports are already used by other devices, then installation of the Image Converter instance is not performed and an error message is displayed. However, you can use other available non-LPT ports to connect virtual printers.

When installing Image Converter instance as a service, you can define the required port (for example, one of *COM* ports) to connect the corresponding virtual printer using the *-printerport* command line parameter.

For example, the following command line installs Image Converter as a service and with a virtual printer:

```
imgconv_x86.exe -install:<ImageConverter> -login:<DOM>
\<Administrator>,<PASS>@<XX.XX.XX.XXX> -printerport:<COM1>
```

Parameters are as follows:

- *ImageConverter*—The name of the service.
- *<DOM>|<Administrator>,<PASS>@<XX.XX.XX.XXX>*—The string that defines the domain name\login, and password, accordingly, and the *IP* address of the server you want to log in.
- *COM1*—The name of a port. To install Image Converter without a virtual printer, simply omit the *–printerport* parameter.

Notes

- The maximum number of Image Converter instances with virtual printers that can be installed is equal to the number of ports available for their connections; otherwise, without virtual printers, the maximum number of Image Converter instances that can be installed is unlimited.
- Multiple Image Converter instances cannot be configured to use the same port due to port conflicts.
- If Image Converter is installed as an application and as a service on a single machine, then both instances of the Image Converter module use the same shared virtual printer. If users want to run the Image Converter application and the service simultaneously, be aware that they will try to use the shared virtual printer when processing non-image files. This would cause an error and file processing would not be performed.

4.3.2 Additional Requirements to Run Image Converter as a Service

When run as a service, Image Converter requires the system be set up properly to be able to process non-image files, such as Microsoft Office files, TXT files, and HTML files. If any of the requirements is not met, the processing of these files cannot be started.

Note: If you are using the Embedded Image Converter Engine for processing Microsoft Office files, TXT files, and HTML files, then you do not need to perform any setup. For more information about the Embedded Image Converter Engine, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.

The setup steps depend on the type of user account under which Image Converter is run as a service. It is recommended that you run the service under an administrative user account for processing non-image files.

Notes

- If the client machine has Microsoft Office 2013 or 2016 installed, using an administrative user account is a strict requirement.
- You must set **Local Security Policy** > **Security Settings** > **Local Policies** > **Security Options** > **User Account Control: Run all administrators in Admin Approval Mode** to **Disabled**.

Before running the service under an administrative account

1. Make sure that the following folders exists on the client machine:

   <%SYSTEMROOT%>\SysWOW64\config\systemprofile\Desktop

   <%SYSTEMROOT%>\System32\config\systemprofile\Desktop

Make sure that the `Desktop` folder is assigned the **Write** permission for "Everyone".

2. Run the Component Services utility, navigate to the `SysWOW64` folder (default location `C:\Windows\SysWOW64`). Run comexp.msc.
3. Browse to **Console Root** > **Component Services** > **Computers** > **My Computer**.
4. Right-click **My Computer** and select **Properties**.
5. Select the **Default Properties** tab and set the following:
   - Select **Enable Distributed COM on this computer**.
   - Select **Connect** from the **Default Authentication Level** list box.
   - Select **Identify** from the **Default Impersonation Level** list box.
6. Click **OK** to save the DCOM settings and close the **My Computer Properties** dialog.
7. In the Component Services utility, browse to **Console Root** > **Component Services** > **Computers** > **My Computer**. Select **DCOM Config**.
8. Select the application associated with the non-image file. For instance:
   - For DOC, DOCX, or HTML files (if Microsoft Word is used as a rendering engine for HTML) : select **Microsoft Office Word 97 —2003 Document**
   - For XLS or XLSX files: select **Microsoft Excel Application**
   - For PPT or PPTX files: select **Microsoft Office PowerPoint Slide**

   Right-click the application and select **Properties**.
9. Select the **Identity** tab and enable the **Launching user** option.
10. Click **OK** to save the settings and close the application's **Properties** dialog.
11. In Internet Explorer, navigate to **Tools** > **Internet Options** > **Security** tab and add the following trusted sites:
    - `http://localhost`
    - `https://localhost`

    Set **Security Level** to **Low** for the trusted sites.

    Save the changes.
12. Disable Internet Explorer from using group policies.

Before running the service under a non-administrative account

1. Take steps 1 through 5 that are described for an administrative account.
2. Additionally, select the **COM Security** tab and do the following:

- Under **Access Permissions**, click **Edit Default**.

  Make sure the required user account is added to the list and granted **Local Access** permissions.

- Under **Launch and Activation Permissions**, click **Edit Default**.

  Make sure the required user account is added to the list and granted **Local Launch** and **Local Activation** permissions.

3. Click **OK** to save the settings and close the **My Computer Properties** dialog.
4. Take steps 7 through 9 that are described for an administrative account.
5. Select the **Security** tab and do the following:

   - In the **Launch and Activation Permissions** area: click **Customize** and **Edit**.

     Make sure that the required user account is added to the list and granted the **Local Launch** and **Local Activation** permissions.

   - In the **Access Permissions** area: click **Customize** and **Edit**

     Make sure that the required user account is granted the **Local Access** permissions.

6. Click **OK** to save the settings and close the application's **Properties** dialog.
7. Take steps 11 and 12 that are described for an administrative account.
8. Navigate to the `Temp` folder of the user account under which Image Converter will be run as a service.

   Note: To learn the path to the user account profile, you can query the <*ProfileImagePath*> registry value at:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\[profile id]\`

   For instance, the profile id `S-1-5-20` keeps the profile of the Network Service user account.

   The required `Temp` folder is located at the following path: `[ProfileImagePath]\AppData\Local\Temp`

9. Right-click the `Temp` folder and select **Properties** and the **Security** tab.
10. Add the client machine user to the users list and grant them the **Write** permissions.
11. Save the changes.

4.3.3 Specifying the Temporary Folder for Storing Intermediate Processed Files

The intermediate files generated while processing non-image files are stored in the temporary folder on the local machine where Image Converter is installed.

When processing files, the path to the temporary folder is taken from the <*TemporaryFolder*> variable in the `IMGCONV.exe.config` file. By default, after the Image Converter module installation, the <*TemporaryFolder*> variable is empty and can be changed by customer to any alternate location:`<add key="TemporaryFolder" value="" />`
If the <*TemporaryFolder*> value is empty, the temporary folder location is taken from the <*TEMP*> environment variable.

Note: The default value for the <*TEMP*> environment variable is set to: *`%USERPROFILE%|AppData|Local|Temp`*, and it grants the "full control" permissions to this folder for any user in production who runs Image Converter on the local machine. When specifying your custom temporary folder location in the `IMGCONV.exe.config` file, ensure that all users are granted the required access.

To specify your custom temporary folder location:

1. In the `C:\Program Files\InputAccel\Client\binnt\` folder (or `Program Files (x86)` for 64-bit systems), open the `IMGCONV.exe.config` file.
2. Change the empty <*TemporaryFolder*> variable value, as necessary. Ensure, all production users are granted the required access for this folder.
   For example, from `<add key="TemporaryFolder" value="" />`
   to `<add key="TemporaryFolder" value="C:\Temp\" />`
3. Save the file. The new value will be applied when running the module in production mode.

4.3.4 Additional Configuration Steps for Processing Files Using the Image Converter Module

These configuration settings are mandatory.

4.3.4.1 Processing HTML Files Using Internet Explorer 11

1. Disable Internet Explorer 11 from using group policies.
2. Ensure that the Network Service account that runs Image Converter as a service has Full Control permissions on the temporary folder for storing the processed files. See "Specifying the Temporary Folder for Storing Intermediate Processed Files" on page 66.
3. Run REGEDIT.EXE.
4. Navigate to `HKEY_CLASSES_ROOT`.
5. Add a new key: *`InternetExplorerMedium.Application`*.
6. Add a new child key for *`InternetExplorerMedium.Application`* called *`CLSID`*.
7. Set the value of *`CLSID`* to **{D5E8041D-920F-45e9-B8FB-B1DEB82C6E5E}**.

4.3.4.2 Processing PDF and Microsoft Office Documents with Security Restrictions

When importing batches containing *PDF* or Microsoft Office files with some security restrictions (including password protection) and processing these batches using Image Converter module, beware of the following:

- When merging PDF files with such restrictions, the following error can be displayed: `Exception "PDF Library Error: This operation is not permitted. Error number: 1073938472"`, and the task fails. The set of restrictions that can be processed by Image Converter module depends on the operation with PDF file source (such as split or merge), and the exceptions' messages can differ. To resolve the issue, the input source PDF documents must not have restrictions specified in PDF file properties (for example, not to have password protection).
- For Microsoft Office files with password protection, a pop-up window prompting to type the password can be displayed. The pop-up window is shown only during the **Conversion Timeout** time specified for the Image Conversion profile. If password has not been typed during the specified timeout, the task fails.If some other security restrictions apply, the task also fails.

4.3.4.3 Printing Background Colors for Microsoft Word Documents

By default, Image Converter does not display or print background colors in output Microsoft Word documents. Users must manually enable this feature to print backgrounds.

To enable printing background colors for Microsoft Word Documents:

1. Open the `IMGCONV.exe.config` file from `C:\Program Files\InputAccel\Client\binnt\` (or `Program Files (x86)` for 64-bit systems).
2. Add the following line between the **appSettings** tags:

```
<add key="WordPrintBackgrounds" value="true"/>
```

4.3.4.4 Processing Macro-enabled Microsoft Excel Files

By default, Image Converter disables macros in an Excel file. Users must manually enable this feature to process macros in an Excel file.

To enable processing macro-enabled Excel Files:

1. Open the `IMGCONV.exe.config` file from `Program Files\InputAccel\Client\binnt` (or `Program Files (x86)` for 64-bit systems).
2. Add the following line between the **appSettings** tags:

```
<add key="ExcelMacrosEnabled" value="true"/>
```

Caution

Enabling macros can result in serious security vulnerability.

4.3.5 Downloading ISIS Scanner Drivers

Attended client modules, ScanPlus and RescanPlus, require scanner drivers. ScanPlus and RescanPlus operators can download *ISIS* scanner drivers from each scanner manufacturer's website.

Notes

- Your scanner device may include many advanced features. Intelligent Capture may not support every advanced scanner feature that is available with your scanner device.
- The ISIS scanner driver standard is supported as well as recommended for seamlessly interfacing our scanning software with document scanners. Every ISIS driver must pass thousands of rigorous tests to fully validate its performance, compatibility and reliability to achieve ISIS device certification. This certification process results in fewer hardware support problems and delivers the most solid document scanning interface available on the market. When you are ready to purchase, choose ISIS-certified devices for all

document scanners or MFPs and easily achieve plug-n-play deployment capability.

4.3.6 Registering the SLDRegistration Executable

The Archive Export client module connects to and populates an SAP ECC or SAP NetWeaver system with administrative data and content. The SAP System Landscape Directory (SLD) contains information about installed SAP components. This information facilitates the maintenance of complex SAP system landscapes. To connect to the *SLD* and provide details of the SAP system used with Archive Export, run the `SLDRegistration.exe` executable from the `InputAccel\client\binnt` directory and register information about the Host, Port, and user credentials of the SAP system.

4.4 Installing Information Extraction

After installing the Intelligent Capture client components, you can install Information Extraction. Run this installer only if you have installed one or more of the following modules:

- Classification
- Collector
- Extraction
- Module Server

Important
You cannot upgrade Information Extraction directly from 21.4 to 22.1. You must first uninstall any previously installed instance of Information Extraction before performing the upgrade.

To install Information Extraction:

1. Ensure that you have already installed the Intelligent Capture client components and that any previously installed Information Extraction instance has been uninstalled.

   The Information Extraction installation option appears in the auto-run menu after you mount the DVD image.

2. From the installation choices in the wizard, select **Install Information Extraction**.

3. Read and accept the wizard steps by clicking **Next**.

   Note: The installation location should default to the folder where you installed the Intelligent Capture client components. Do not change this location unless it is incorrect.

4. Click **Finish**.

Tip: You can also install Information Extraction from the command line.

4.5 Activating and Licensing Intelligent Capture

After installing the Intelligent Capture Server and Intelligent Capture Administrator, install security key or activation file to activate the server, install licenses, and begin the activation process.

For details on the server and client licenses required for specific features, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*. For instructions on security keys and licenses and activating Intelligent Capture Servers, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*. You can use it for a limited time while waiting for a response to the activation request.

4.5.1 Licensing the Check Reading Engine

To license the Check Reading engine:

1. Run the SoftLockViewer utility, `SoftlockViewer2.exe`, (default location: `%QSDIR%\Dll\CheckPlus\`) to generate the SoftKey required to retrieve the license for Check Reading engine.
2. Click **Make Request for SoftKey**.
3. In the **SoftKey Request Codes** window, click **Save codes to file**.
4. Send the saved file to OpenText Global Technical Services at My Support (https://support.opentext.com) to request a Check Reading engine license.
5. You receive the license in a `PSK` file. Save the file on the client machine and click **Insert Received SoftKey** in SoftLock in the SoftLockViewer utility, and select the `PSK` file. The **SoftLock information** appears in the SoftLockViewer.

Note: You may notice that the number of field credits is more than the number of checks per year that you ordered. This is because you have the ability to read more than one field for each check and each field represents one credit (the payee line represents two credits).

Caution

Licenses and field credits contained in them only apply on a per-machine basis. You cannot share licenses and field credits across multiple machines.

4.6 Setting the UI Language of Intelligent Capture Components

After successful installation of Intelligent Capture, you may want to set the user interface (*UI*) language for the various components. Depending on the component, the default UI language is determined by the user's regional settings or language of the operating system. The default UI language can be overridden so that the user interface is displayed in a language other than the default UI language.

For a list of supported UI languages, their language codes, and locale IDs, see "Appendix—Localized Languages" on page 201.

Performance counters are installed on the Intelligent Capture Server machine and are available in the language of the operating system where they are installed or English.

Note: Windows Event Log typically displays event logs in the language of the operating system where they are viewed.

Tip: Some messages shown by the Intelligent Capture modules are transferred from the .NET Framework. To localize these messages, install the appropriate version of the .NET Framework Language Pack. For the .NET Framework version required for your Intelligent Capture current version, see the *Release Notes*.

4.6.1 Specifying Default UI Language Settings

The procedure for setting the default *UI* language differs between client modules that were new prior to 6.0 and those that were new in versions 6.x or later.

Client modules new in 6.x or later versions (modules listed as "New in 6.x" and "New in 7.0 - 7.7, 16.5, 16.6, 20.2" in "Intelligent Capture Modules" on page 189) use the language of the operating system as the default UI language. These modules use the locale set on the **Regional Options** tab (**Control Panel** > **Regional and Language Options**) to control the format of date, number, currency, and so on. The default UI language settings for the Intelligent Capture Server and client modules can be overridden. For details, see "Summary of Options for Overriding the Default UI Language" on page 72.

To specify the default UI language for Intelligent Capture Server and for client modules available prior to 6.0:

This procedure applies to setting the default UI language on a machine running Microsoft Windows 7 operating system.

1. Run the Control Panel on the machine running the Intelligent Capture Server or any client module available prior to Intelligent Capture 6.0. (Modules listed as "Available prior to 6.0" in "Intelligent Capture Modules" on page 189)

2. Double-click **Regional and Language Options**.

3. On the **Regional Options** tab, select a locale to set the default UI language and control the format of date, number, currency, and so on. The **Samples** area displays the formatting based on the locale selected. Click **Customize** to make changes.

4. On the **Advanced** tab, select a language drop-down list box. Choose from the "Appendix—Localized Languages" on page 201 in Intelligent Capture . This sets the code page that the Intelligent Capture Server and client modules will use. It must be an appropriate code page for the locale set in the **Regional Options** tab. Typically, the locale specified in the **Regional Options** tab and language specified on the **Advanced** tab must match.

5. On the **Advanced** tab, select the **Default user account settings** check box. This ensures that the changed settings apply for all accounts that are used to run the Intelligent Capture Server or client modules as a service.

4.6.2 Summary of Options for Overriding the Default UI Language

The default *UI* language for the Intelligent Capture Server or client modules can be overridden as summarized in this section. Steps for each override option is described in "Procedures to Override the UI Language" on page 73.

Table 4-2: Globalization and UI Language Settings for Intelligent Capture Components

Intelligent Capture component	Globalization settings (for example, date, number, currency formatting) determined by	Default UI language determined by	Default UI language overridden by
Intelligent Capture Server	User's regional settings	User's regional settings	Specifying the UI language in the: • `Win.ini` file • `Setscan.ini` file
Client modules that were available prior to 6.0 (Modules listed as "Available prior to 6.0" in "Intelligent Capture Modules" on page 189)	User's regional settings	User's regional settings	Specifying the UI language in the: • `Win.ini` file • `Setscan.ini` file

Intelligent Capture component	Globalization settings (for example, date, number, currency formatting) determined by	Default UI language determined by	Default UI language overridden by
Client modules that are new in releases 6.x or later	Regional settings of the operating system	Language of the operating system **Note:** For Intelligent Capture Administrator users: On a Windows 8 / Internet Explorer 10 system, users must manually set the language to Simplified Chinese for the UI to display in that language: Use REGEDIT.EXE, navigate to regedit -> HKEY_CURRENT_USER -> Internet Explorer -> International -> AcceptLanguage -> and change the value to zh-cn.	Specifying the UI language through: • Command line argument • `settings.ini` file • `Setscan.ini` file • Multilingual User Interface (MUI) Pack

4.6.3 Procedures to Override the UI Language

This section details the steps involved in overriding the default *UI* language of the Intelligent Capture Server and client modules.

Prerequisites for successfully overriding the default UI language:

- Make sure new UI language is supported by the Windows code page specified in the **Advanced** tab of the **Regional and Language Options** window of the Control Panel.
- Make sure the **Regional Options** tab lists the appropriate locale. This is required to display the correct format of date, number, currency, and so on.

To specify a command line argument to set the UI language:

- On the client machine where a module new in version 6.x or later is installed, add the following parameter to the command line arguments used to start the module:`-language:<language code>`

  where <language code> represents a language code for the languages supported in Intelligent Capture.

  The following examples assume that the ScanPlus module is installed at the default location.

  Example 4-1: Start the ScanPlus module with the UI language set to English-United States

  ```
  "C:\Program Files (x86)\InputAccel\Client\binnt\x64\
  QuickModuleHost.exe" -modulename:Emc.InputAccel.Scan
   -language:en-us
  ```

  Example 4-2: Start the ScanPlus module with the UI language set to Portuguese-Brazil

  ```
  "C:\Program Files (x86)\InputAccel\Client\binnt\x64\
  QuickModuleHost.exe" -modulename:Emc.InputAccel.Scan
   -language:pt-br
  ```

  Example 4-3: Start the ScanPlus module for production connecting to the "Baltimore1" and "bermuda" servers with the domain name "honor", the user name "johndoe", the password "password99", and the UI language set to Portuguese

  ```
  "C:\Program Files (x86)\InputAccel\Client\binnt\x64\
  QuickModuleHost.exe" -modulename:Emc.InputAccel.Scan
   -login:honor\johndoe,password99@Baltimore1;bermuda
   -language:pt
  ```

To specify the UI language in the settings.ini file:

1. On the client machine where a module is new in versions from 6.x or later is installed, open the `settings.ini` file.

2. In the [INPUTACCEL] section, specify the UI language in the format:`language=<language code>`

   where <language code> represents a language code for the languages supported in Intelligent Capture.

   Example:

- `language=en-us` (to set the UI language to English-United States)
- `language=pt-br` (to set the UI language to Portuguese-Brazil)
- `language=pt` (to set the UI language to Portuguese)

To specify the UI language in the setscan.ini file:

On the machine where the Intelligent Capture Server or any Intelligent Capture client module is installed, open the `setscan.ini` file. The default location is `c:\windows`.

- In the [OPTIONS] section, specify the *UI* language in the format: `iLanguage=<Locale ID>`

  where <Locale ID> represents the locale ID for the languages supported in Intelligent Capture.

  Example:

  - `iLanguage=1033` (to set the UI language to English-United States)
  - `iLanguage=1046` (to set the UI language to Portuguese-Brazil)

To specify the UI language in the win.ini file:

1. On the machine where the Intelligent Capture Server or a client module available prior to the Intelligent Capture 6.0 release is installed, open the `win.ini` file.
2. In the [INPUTACCEL] section, specify the UI language in the format: `Locale=<Locale ID>`

   where <Locale ID> represents the locale ID for the languages supported in Intelligent Capture.

   Example:

   - `Locale=1033` (to set the UI language to English-United States)
   - `Locale=1046` (to set the UI language to Portuguese-Brazil)

To specify the UI language using the Windows MUI Pack:

A MUI Pack is available in the English version of supported operating systems. The MUI Pack will not install on non-English versions of the operating system. See Microsoft documentation on how to install the MUI Pack.

Note: This procedure assumes you are running the English version of the Windows 7 operating system and have installed the MUI Pack.

1. Run the Control Panel on the machine running the any client module new in versions from 6.x or later.
2. Double-click **Regional and Language Options**.

3. On the **Languages** tab, select the required language from the **Language used in menus and dialogs** list box.

4.7 Providing the online help on a local help server (Private Help Server)

The online help for this product is delivered using the OpenText Global Help Server (GHS) system, which provides your users with live access to the latest version of the help. If you cannot use the GHS system, for example, if your site does not have Internet access, you can install the OpenText Private Help Server (PHS), a local version of the help system that can host your OpenText product online help on your organization's network. After the PHS is installed, you can then configure your OpenText products to forward all online help requests to your PHS. For detailed information about installing the PHS, see *OpenText Help System - Private Help Server Administration Guide (OTHS-AGD)*.

Notes

- The Private Help Server can support multiple OpenText products. If the Private Help Server has already been installed within your organization to support another OpenText product, you can add additional OpenText product online helps to that installation.
- If you are replacing a previous PHS installation, see *OpenText Help System - Private Help Server Administration Guide (OTHS-AGD)*.
- If the server you want to use for the PHS installation cannot connect to the Internet, see *OpenText Help System - Private Help Server Administration Guide (OTHS-AGD)*.

Once the PHS is installed or upgraded, you can use its Online Help Deployer to download online helps from the GHS system by entering the help deployment codes listed below. For more information about using the codes, see *OpenText Help System - Private Help Server Administration Guide (OTHS-AGD)*.

Table 4-3: Help deployment codes

Code	Product
ECPCORE220200-IGD	OpenText™ Intelligent Capture CE 22.2

To enable Intelligent Capture to redirect help requests from the Global Help Server (the default configuration) to the Private Help Server (optional), you must specify the Private Help Server's URL. During the installation of Intelligent Capture components like the database, server, Web component, or client component, the install wizard provides the option to add the Private Help Server URL if you opt not to use the Global Help Server.

The Private Help Server URL can be either an IP address or a DNS and should be specified using a root URL that includes the path segments to the actual API endpoint of the GHS/PHS server. For example:

Example 4-4: Private Help Server URL

```
http(s)://myhelp.company.com/OTHelp/mapperpi
```

If you decide to use a Private Help Server after the installation of Intelligent Capture is completed, you can either re-run the installer or modify the configuration file.

To configure the PHS in the configuration file

Caution

Perform this procedure only if you have requisite knowledge of modifying configuration files. If you enter the URL incorrectly, users will not be able to access help on the Private Help Server.

1. Navigate to *<installationDrive>*`\ProgramData\OpenText\Capture`

   where <*installationDrive*> represents the drive where Intelligent Capture is installed.

2. Open the configuration file using a text editor.

3. In the `PrivateGHSUrl` parameter, type the root URL of the Private Help Server between the quotation marks (“”). For example,

   `PrivateGHSUrl = "https://`*<myhelp.company.com>*`/OTHelp/mapperpi"`

   where <*myhelp.company.com*> represents the DNS or IP address of your PHS.

4. Save and close the configuration file.

5. Restart the client module(s) in which the help calls are made.

Chapter 5

Additional Installation and Configuration Options

This section discusses additional installation and configuration options for Intelligent Capture andIntelligent Capture Real Time Services.

Note: Intelligent Capture Real Time Services uses the same installer as Intelligent Capture.

5.1 Installing Multiple Instances of Intelligent Capture Servers

Multiple instances of the Intelligent Capture Server can be installed on a single machine (also called a side-by-side installation). A maximum of eight instances of Intelligent Capture Server can be installed; although in typical installations, one Intelligent Capture Server per four or eight cores is optimal. Variations in how systems are configured, the types of hardware used, and customer-specific batch processing needs make each situation unique, requiring experimentation to find the best balance between number of processors per instance of the Intelligent Capture Server.

Performance benefits of side-by-side installation include:

- Each Intelligent Capture Server instance runs its .NET runtime within its server process, enabling better parallel execution of batches when running on multi-processor machines.

  The VBA runtime is a 32-bit application and as such runs outside of the Intelligent Capture Server process. Furthermore, the VBA runtime is loaded only when processes require it.

- Enables Intelligent Capture to be installed in an Active/Active clustered environment.

Notes

- Side-by-side installation requires that an Intelligent Capture Database is installed.
- Side-by-side installation is required when installing the Intelligent Capture Server in an Active/Active clustered environment.
- ScaleServer groups normally provide some degree of business continuation if a server failure occurs. However, if all members of a ScaleServer group are installed on the same physical machine, then a single point of failure will take out the whole system. So, do not install all members of a ScaleServer group on a single machine if you intend to ensure high availability.

- The installer requires an account that is a member of the local **Administrators** group on the machine from which you are running the setup program.

To install multiple instances of Intelligent Capture Servers:

1. From the **Installation Choices** list, select **Step 2 - Install the Intelligent Capture Server**. Click **Next** and follow the installation wizard.
2. In the **Database and Failover Options** window, select **Use an external MSSQL Database** and optionally select **Use Microsoft Failover Cluster Environment** if you want to install the server in a clustered environment. Information on installing the server in a clustered environment is provided in "To install Intelligent Capture Server on the first cluster node:" on page 86
3. Choose a custom installation and click **Next**.
4. Select the number of Intelligent Capture Server instances to install, and then click **Next**.
5. For each instance, click **Change** to specify a unique location for data files for each Intelligent Capture Server, and then click **Next**.

   Note: Each instance of the Intelligent Capture Server must have its own principal folder. Each instance is installed on its own directory. It is recommended that for best performance the specified directories be on separate physical hard disks and the directories reside on an *NTFS* partition.
6. In the **TCP/IP Settings** window, specify the **IPV4 address** and **IPV6 address** and **Port** for each server instance. To simplify client module connections, it is recommended that you use the default port for all server instances.
7. The **Configure Intelligent Capture Service Accounts** window displays, prompting the user for the "run-as" credentials to use for new instances being installed. Click **Next**. Specify whether you want the Intelligent Capture Server to be started as a service automatically when the system starts.
8. In the **Data Access Layer Registration** window, specify the login credentials for connecting to the SQL Server. This is the SQL Server user account created that provides permissions to access the Intelligent Capture Database. Click **Next**.

   Note: If the machine where the Intelligent Capture Server is installed also has SQL Server installed, then by default **Register the Data Access Layer with the Intelligent Capture database** is selected and the local database server, default SQL Server port 1433, and Database name are specified.
9. Click **Install** and then click **Finish** to complete the installation.

   Notes

   - If you choose to start the Intelligent Capture Server as a service automatically when the system starts, the setup program configures

only the first Intelligent Capture Server instance to automatically start. All other instances of the Intelligent Capture Server are configured to run as services but are not configured to start automatically. Use the Service Control Manager to configure these additional instances to start automatically.

- Before running the other instances, license the servers for a side-by-side operation. Without the proper feature code, multiple servers will not startup on the same machine.
- With multiple instances of the Intelligent Capture Server installed in an Active/Active clustered configuration, you will not be able to run both of them on the same node at the same time. You must run both the Intelligent Capture Server on separate nodes until after you have licensed them. If you attempt to run both servers on the same node at the same time, one of them will not start (due to a lack of a server license containing feature code S) and Microsoft Failover Clustering will automatically move the resources for that server to the other node and start it up there.

10. Activate and license all installed instances of the Intelligent Capture Servers.
11. To verify that multiple instances of the Intelligent Capture Server are installed correctly:
    a. Start any module in production mode.
    b. When logging on, specify one of the Intelligent Capture Servers and make sure the module connects.
    c. Repeat these steps for each Intelligent Capture Server instance.

5.2 Configuring Multiple Intelligent Capture Servers as a ScaleServer Group

A ScaleServer group of Intelligent Capture Servers consists of two to eight Intelligent Capture Servers connected to the same network, and licensed and configured to work together as a single information capture system. The installation process for each Intelligent Capture Server is the same as when installing a single Intelligent Capture Server. An Intelligent Capture Database is required to configure Intelligent Capture Servers as a ScaleServer group.

ScaleServer technology uses a combination of licensing, server configuration parameters, and technology in the Intelligent Capture Servers themselves. To configure a ScaleServer group, obtain a server license that enables the ScaleServer technology. To learn more about the licensing feature codes for ScaleServer groups, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)* .

Notes

- Client modules cannot connect to multiple independent Intelligent Capture Servers – they can only connect to multiple servers that are part of a

ScaleServer group. For a list of client modules that are ScaleServer compatible, see "Intelligent Capture Modules" on page 189.

- All Intelligent Capture Servers within a ScaleServer group must access the same Intelligent Capture Database.

To configure a ScaleServer group:

1. Install the required hardware and software on each Intelligent Capture Server machine. For details, see the *Release Notes*, available from My Support (https://support.opentext.com).
2. Install the Intelligent Capture Database software.
3. Install the Intelligent Capture Server software on each server machine.
4. Install Intelligent Capture Administrator from the client components setup program.
5. Run the Intelligent Capture Administrator module and do the following to configure the ScaleServer group:

   a. For each installed Intelligent Capture Server, be sure to install and activate the Activation File (*CAF* file).

   b. Install valid ScaleServer licenses/feature codes on each Intelligent Capture Server that is to be part of the ScaleServer group.

   

   Note: Feature codes are established when the Intelligent Capture Server license codes are installed. For details on server feature codes, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

   c. Specify a ScaleServer group name and add a list of Intelligent Capture Servers in the group.

   d. Make sure the same users are in the **InputAccel_Server_admin_group** group on all Intelligent Capture Servers in the ScaleServer group.

   For information on activating Intelligent Capture Servers, installing license codes, adding users and groups, and specifying a ScaleServer group, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)* .

   

   Note: When users running client modules connect to a ScaleServer group, they must specify the Intelligent Capture Server machine name, not "localhost" or an *IP* address.

6. To verify that the ScaleServer group is functioning correctly:

   a. Start a ScaleServer-compatible module in production mode and connect to the ScaleServer group. For a list of modules that are ScaleServer-compatible, see "Intelligent Capture Modules" on page 189 .

b. Run Intelligent Capture Administrator and verify that the client module is logged into all servers in the ScaleServer group. For more information, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

5.3 Installing the Intelligent Capture Server in a Microsoft Failover Clustering Environment

This section explains how to install Intelligent Capture within Microsoft Failover Clustering. For a list of supported Microsoft Failover Clustering environments, see the *Release Notes*.

Intelligent Capture supports one Intelligent Capture Server running in an Active/Passive mode, or two servers running in an Active/Active mode. When two Intelligent Capture Servers are used, they can be configured as a ScaleServer group or they can be used independently.

Administrators must run the Failover Cluster Manager for all cluster configuration tasks, including defining each virtual server and its failover/fallback rules. For more information about the Failover Cluster Manager, see the Microsoft documentation.

Make sure that the Intelligent Capture Servers have enough time to shut down in a cluster. For more information, see Step 2.

Note: Intelligent Capture has been tested on a Microsoft Failover Clustering cluster of two nodes. Other configurations may work, but are not officially supported.

5.3.1 Requirements for Intelligent Capture Server in Microsoft Failover Clustering

The Microsoft Failover Clustering and Intelligent Capture Server environments must meet the requirements in this section.

General requirements

The Microsoft Failover Clustering environment must be configured according to Microsoft best practices. For more information, see technet.microsoft.com (http://technet.microsoft.com/). In particular, make sure that your Microsoft Failover Clustering environment meets these requirements:

- The clustered servers must have passed–without errors–the Microsoft Cluster Validation Wizard.
- At least two separate and identically configured node servers with the supported Windows Server version set up in a cluster configuration.
- The Intelligent Capture Database is installed on a server other than the Intelligent Capture Servers.
- The clustered servers include shared storage that is certified as compatible for use in Microsoft Failover Clustering.

- All machines are members of the same domain.
- On Windows Server 2012 and Windows Server 2012 R2, in addition to the Microsoft Failover Clustering feature, the following features in **Remote server Administration Tools** > **Feature Administration Tools** > **Failover Clustering Tools** are required to register the Intelligent Capture Server cluster resource *DLL*s with the cluster:
  - **Failover Cluster Automation Server**
  - **Failover Cluster Command Interface**

Intelligent Capture Server requirements

Before configuring Intelligent Capture Server in Microsoft Failover Clustering, you must make sure that each Intelligent Capture Server in the cluster meets the following requirements:

- Cluster disk for the `\IAS` data directory.
- Static IP address that clients use to access the Intelligent Capture Server as a clustered application.
  - Windows Server 2012, Windows Server 2012 R2: When both IPv4 and IPv6 protocols are enabled, only a single static IPv4 address is required, and the cluster can automatically create a corresponding IPv6 address if necessary.
- Intelligent Capture Server running under either the Local System account or a domain user account that is a member of the local Administrators group on both cluster nodes. Use of a LUA account for running the Intelligent Capture Server is not supported in the Microsoft Failover Clustering environment.
- A cluster *CAF* file for each Intelligent Capture Server to be installed into the cluster; for example, for two servers in an Active/Active installation, you must have two CAF files.

5.3.2 Installing Intelligent Capture Servers into Microsoft Failover Clustering

Although these instructions apply to the installation of two Intelligent Capture Servers into an Active/Active cluster, you can still use them for the installation of a single Intelligent Capture Server into an Active/Passive cluster. To use these instructions for installing a single Intelligent Capture Server into an Active/Passive cluster, ignore references to the second server instance, second application group, or second cluster disk. Furthermore, any significant differences between Active/Active cluster and Active/Passive cluster installation steps are specifically mentioned.

Note: The installer requires an account that is a member of the local **Administrators** group on the machine from which you are running the setup program.

To install Intelligent Capture Servers into Microsoft Failover Clustering:

1. Set up the cluster environment according to Microsoft and Intelligent Capture Server requirements.
2. Define the cluster resources.
3. To verify that both Intelligent Capture Server cluster disks are accessible from the first cluster node.
4. To install Intelligent Capture Server on the first cluster node.
5. To register the Intelligent Capture Server cluster resource DLLs with the cluster.
6. Move both cluster disks to the second node and install the Intelligent Capture Server on the second cluster node.
7. Complete the Intelligent Capture Server cluster application configuration.
8. Complete additional configuration of server parameters in Intelligent Capture Administrator.
9. To activate and license the Intelligent Capture Servers on both cluster nodes.

To define the initial cluster resources for running in a cluster:

1. Using Failover Cluster Manager, define the initial cluster resources for running in a cluster.
2. Create preliminary application resource groups for each Intelligent Capture Server installed in the cluster.

   As a best practice, create these application resource groups with a single disk resource allocated, then install the Intelligent Capture Server on both cluster nodes, and finally complete the remainder of the configuration by adding the remaining resources of *IP* address, *DNS* name, and Intelligent Capture Server resource type.
3. Connect to the cluster using the Failover Cluster Manager snap-in.
4. In the Failover Cluster Manager console tree in the left pane, click **Storage**.

   The available cluster disks are displayed under **Available Storage**. There should be one cluster disk available for each Intelligent Capture Server to be installed. For example, Active/Active requires two dedicated cluster disks.
5. On Windows Server 2012 or 2012 R2, right-click **Roles** and select **Create Empty Role**. A new role named **New Role** is created.
6. Rename the application to indicate that it is the first Intelligent Capture Server.

   This name is used only for display purposes in the cluster administration user interface.
7. Repeat steps 5 and 6 of the current procedure to create a second application (for Active/Active cluster) and rename it to indicate it is the second Intelligent Capture Server.

8. Edit the **Properties** of these new applications/roles to define the preferred owners on each application/role. Typically, the first Intelligent Capture Server should have a preferred owner of node 1, and the second Intelligent Capture Server a preferred owner of node 2.

9. Add storage to each of these applications by adding the appropriate cluster disk resource to each application/role. Under **Roles** (on Windows Server 2012 and 2012 R2), select the application/role, right-click and select **Add Storage**, and select the check box for the first Intelligent Capture Server cluster disk (for example, drive R). Repeat the process for the second Intelligent Capture Server application/role if creating an Active/Active cluster (for example, add drive S as the storage on the second Intelligent Capture Server application/role).

10. Move both applications/roles to the first node so they are owned by the first node.

Note: In Active/Passive cluster, only one application/role exists, and it should be owned by first node.

To verify that both Intelligent Capture Server cluster disks are accessible from the first cluster node:

1. Start Windows Explorer.

2. Verify that both Intelligent Capture Server cluster disks are accessible from the first node. In the case of Active/Passive cluster, only one Intelligent Capture Server cluster disk exists.

To install Intelligent Capture Server on the first cluster node:

1. On the first node, start the Intelligent Capture setup program from the installation media.

   If the setup program does not start automatically after a few seconds, or if running the installation from a local disk or network share, run `autorun.exe`.

2. Select **Install Product** > **Installation Choices** > **Step 2 - Install Intelligent Capture Server** and follow the instructions.

3. In addition to the usual options, select the following options for configuring Intelligent Capture Server with Microsoft Failover Clustering:

Option	Action
Database and Failover Options	Select the following options: **Use an external MSSQL Database** **Use Microsoft Failover Cluster Environment**
Setup Type	Select **Custom**.

Option	Action
Number of Intelligent Capture Server instances	• For an Active/Active cluster: 2 • For an Active/Passive cluster: 1
Choose Install Folder	Select a local drive; that is, do not install Intelligent Capture Server application files onto the cluster disk.
Choose Data Files Install Folder	For each Intelligent Capture Server's `\IAS` data directories, select its associated cluster disk (do not select a local drive).
Configure Cluster Settings	• For an Active/Active configuration, enter the following: – Two IPv4 addresses and port numbers. For the port numbers, use the same value for both of your Intelligent Capture Servers. – (Optional) Two IPv6 addresses and same port numbers as for the IPv4 addresses. • For an Active/Passive configuration, enter the following: – The IPv4 address and port number. – (Optional) The IPv6 address and same port number as for the IPv4 address. **Notes** • The IPv4 addresses that you enter are static addresses, which are dedicated for use only by each Intelligent Capture Server application. These addresses are not the same ones that are used by the cluster nodes themselves. • If you do not specifically require IPv6 support, you can leave these IPv6 address fields blank (however, do not leave the port number fields blank). IPv6 address support can be added at a later time.
Configure Intelligent Capture Service Accounts	You can specify the user account under which the Intelligent Capture Server service will run as either **Local System** or for a domain user account. The domain user account must be a member of the Windows Administrators group on each cluster node where the server runs.

Option	Action
Automatically start the Intelligent Capture Server service when the system starts	Clear this option. The service startup mode for the Intelligent Capture Server services must be set to **Manual** when running it in a cluster.
Start the Intelligent Capture Server service when setup completes	Clear this option. The Intelligent Capture Server should not be started outside of the cluster control.

To register the Intelligent Capture Server cluster resource *DLL*s with the cluster:

1. On one node, in a command prompt (running as Administrator), execute the following file for each Intelligent Capture Server:

   ```
   C:\Program Files\InputAccel\Server\<Server#>\binnt\
   CreateIAResType.bat
   ```

   where <*Server#*> is the directory for each Intelligent Capture Server.

   `InputAccel` resource type is created for the first Intelligent Capture Server and `InputAccel2` resource type is created for the second one.

   Note: For more information about running `CreateIAResType.bat`, simply execute it.

2. To ensure that the Intelligent Capture Servers have enough time to shut down, set the `ShutdownTimeoutInMinutes` cluster property.

   If the `ShutdownTimeoutInMinutes` cluster property was set to less than 20 minutes, then `CreateIAResType.bat` sets this property to 20 minutes. Typically, Intelligent Capture Server shuts down within 30 seconds; however, depending on the server load, the shutdown process could take 20 minutes or more. In this case, unsynchronized batches could lose data because Microsoft Failover Clustering terminates services that take longer to shut down than the time specified in `ShutdownTimeoutInMinutes`.

   To verify the value of the `ShutdownTimeoutInMinutes` cluster property, execute the following command:

   ```
   cluster /properties
   ```

   To set the value of `ShutdownTimeoutInMinutes`, execute the following command:

   ```
   cluster /properties ShutdownTimeoutInMinutes=<N>
   ```

   where:

   <*N*> is the maximum number of minutes required by the slowest service running in the cluster to gracefully shutdown.

To move both cluster disks to and install the Intelligent Capture Server on the second cluster node:

1. In **Failover Cluster Manager,** under **Roles** (on Windows Server 2012 and 2012 R2), move the Intelligent Capture Server applications to the second node.

   All Intelligent Capture Server applications in the cluster must be owned by the second node.

   Note: Only one application/resource group for Active/Passive cluster exists.

2. On the first node, stop the Failover Cluster Manager application.

3. To install Intelligent Capture Server on the second node, repeat the "To install Intelligent Capture Server on the first cluster node:" on page 86 procedure.

To complete the Intelligent Capture Server cluster application configuration:

1. Stop and restart the Failover Cluster Manager.

   Note: You can use Failover Cluster Manager on either node.

2. Add a **Client Access Point** resource.

   This resource specifies the Intelligent Capture Server's *IP* address and Network Name.

   - For Windows Server 2012 and 2012 R2, under the console tree in the left pane, select **Roles**, and then right-click each Intelligent Capture Server role and select **Add a resource > Client Access Point**.

   Enter the following information:

   - **Name**: The Network Name (host name) by which this Intelligent Capture Server is accessed over the network by client modules and Intelligent Capture Administrator.
   - **Address**: Enter the static IPv4 address that is used to access this Intelligent Capture Server. This is the same address which you entered during Intelligent Capture Server installation, and will be registered with the *DNS* with the network name you just entered.
   - Once Client Access Point resource is configured, right-click the **Name** resource and select **Properties**.
   - Under the **Dependencies** tab, if there are two *IP* address resources listed (IPv4 and IPv6 address) with an `OR` operator, change the operator to `AND`. This will ensure that the network name resource is registered with the *DNS* using both IP addresses.
   - Verify that the Network Name resource can be brought online.
   - If IPv6 protocol was enabled, a corresponding IPv6 address was automatically generated by the cluster. Once resources are online, you can

view the value of the IPv6 address resource that was just created. If you wish to use IPv6 protocol for the Intelligent Capture Server, write down the address. It can be manually entered through the Intelligent Capture Administrator module at a later time.

- Repeat these steps for the second Intelligent Capture Server if installing Active/Active.

3. Right-click the Intelligent Capture Server application/role and select **Add a resource > More resources… > Add InputAccel**, but do not make this resource online. This step adds the Intelligent Capture Server to the clustered application/role.

   To add a second Intelligent Capture Server, right-click the second Intelligent Capture Server application/role and select **Add a resource > More resources… > Add InputAccel2**.

Caution

A message `The resource type Add Intelligent Capture is not configured on all nodes. Do you wish to continue and create the resource?` indicates the Intelligent Capture Serversare not installed on both nodes.

4. Edit the **Properties** of the **New InputAccel** resource as follows:

Tab	Action
General	Change the name of the first and second servers to **InputAccel** and **InputAccel2**, respectively.
Dependencies	Insert the following dependent resources for this Intelligent Capture Server: • **Cluster disk** • **Name**
Policies	Until the Intelligent Capture Server is fully licensed and operational, it is recommended that you change the setting of **Response to resource failure** to **If resource fails, do not restart**. **Note:** This setting can be reconfigured later as required. Select any other required settings.
Advanced Policies	Ensure that both nodes are enabled as possible owners.

5. Make the Intelligent Capture resource online.

Note: You must make at least one attempt to bring the Intelligent Capture resource online before you can edit the parameters in Intelligent Capture Administrator.

6. For an Active/Active cluster installation, repeat all these steps to configure the second Intelligent Capture Server, but use a different name and static *IP* address, and select the resource type as **InputAccel2**.

7. Verify that you can move each Intelligent Capture Server application back and forth between the nodes and make it online.

Note: In the case of Active/Active cluster installation, until you have installed the *CAF* files and correctly licensed these servers, you cannot make both Intelligent Capture Server resources online on the same node at the same time. You can make them both online simultaneously as long as they are on different nodes. Once they are licensed, this restriction no longer applies and both can run on the same node.

To complete additional configuration of server parameters in Intelligent Capture Administrator:

1. Install Intelligent Capture Administrator on a separate machine.

2. Make both Intelligent Capture Servers online simultaneously on different nodes. In the case of Active/Passive cluster, bring the Intelligent Capture Server online on either node.

3. Log in to any of the Intelligent Capture Servers using the Intelligent Capture Administrator module.

4. Navigate to the **Systems** pane and click **View Servers**. You should see the two Intelligent Capture Servers (or in the case of Active/Passive cluster, just one Intelligent Capture Server) listed here. The names of these servers should match the **Network Name** that was configured for each server in the cluster. Delete additional machine names for either of the cluster nodes.

5. Double-click each of the Intelligent Capture Server names to bring up the **Server Settings** screen for that server. Enter the following values under the **Startup Setting** column and click **OK** after making all the changes to these values.

   - Ensure the **TcpIpPort** value is set to the default value of 10099 (on both servers) unless there is a specific need to use a different port.
   - The **TcpIpAddress** value should contain the static IPv4 address resource assigned to this Intelligent Capture Server in the cluster.
   - The **TcpIpv6Address** is likely to be blank. To use IPv6 protocol (whether as an alternative to IPv4, or in addition to IPv4), enter the static IPv6 address assigned to this Intelligent Capture Server in the cluster. If this address was generated automatically by the cluster configuration, review the *IP* address properties for this resource in the Failover Cluster Manager snap-in. If you manually entered the IPv6 address during cluster configuration, enter the same address.

- The **DisableIPv4** value must be **0**, unless required to disable IPv4 protocol.
- The **DisableIPv6** value must be **0** if you intend to use IPv6 protocol and **1** otherwise.
- In a two Intelligent Capture Servers installation into an Active/Active cluster, enter the appropriate values for both servers.

6. If you made any changes, be sure to click **OK** to save them, then restart all Intelligent Capture Servers. If no changes were made, you do not need to restart the Intelligent Capture Servers.

To activate and license the Intelligent Capture Servers on both cluster nodes:

To activate and license the Intelligent Capture Server in a cluster, you must activate each Intelligent Capture Server twice, once for each node in the cluster using Activation IDs.

Note: For an Active/Passive cluster environment, you require a single activation (*CAF*) file for the single Intelligent Capture Server. For an Active/Active cluster environment, you require two activation files for the two Intelligent Capture Servers.

1. Run Intelligent Capture Administrator and log in as the administrative user (member of Administrators role).
2. From the navigation panel, select **Licensing / Security**, and then select **View Server Activations**. The **Server Activations** pane displays all Intelligent Capture Servers listed with their network names followed by their service names, for instance IASERVER1 (InputAccel) and IASERVER2 (InputAccel2). The Server ID is displayed as **0** and the state is set to **Not Activated**.
3. On the **Server Activations** pane, select the first server (IASERVER1 for example) and **Browse** to the location of the cluster CAF file intended for the first server, and select the CAF file.

   Note: A CAF file that is not intended for a cluster cannot be installed in a cluster environment.

4. Repeat the previous step for the second server (for an Active/Active cluster). The Intelligent Capture Servers display an activation state of **Initial Grace Period**.

   Notes

   - You cannot use the same *CAF* file for both servers in an Active/Active cluster environment.
   - To activate the Intelligent Capture Server in an Active/Passive cluster environment, you require a single activation (CAF) file that provides the **Server ID** for the single Intelligent Capture Server. You also require two **Profile ID**s. To activate the Intelligent Capture Servers in an Active/Active cluster environment, you require two activation (CAF) files that

provide two **Server ID**s for the two Intelligent Capture Servers. You also require four **Profile ID**s. To obtain these Profile IDs, each Intelligent Capture Server must be run on each clustered node, as the Profile ID is different on each node.

5. Import license codes for both servers. Do this before continuing with activation and moving servers between nodes.
6. From the Failover Cluster Manager, start IASERVER1 on Node 1 and IASERVER2 on Node 2.
7. From Intelligent Capture Administrator navigate to the **Server Activations** page.
8. Select IASERVER1, and then click **Activate Server**. Note the **Server Serial Number** and **Profile ID**. Repeat for IASERVER2 (for an Active/Active cluster).
9. Use Failover Cluster Manager to move each Intelligent Capture Server to the other node. Now repeat steps 6–7 and obtain the second set of Serial Numbers and Profile IDs.
10. From the **Server Activations** page, click the link to open OpenText My Support (https://support.opentext.com) and request activation keys for the four Profile IDs. For each profile ID, provide the Server Serial Number.
11. When you receive the activation keys, you can activate the Intelligent Capture Server for each node. Run Intelligent Capture Administrator and navigate to the **Server Activations** page.
12. Select the Server name, and click **Activate Server**. The **Activate Server** window displays.
13. Type the activation key for the first Intelligent Capture Server Profile ID, and then click **OK**. The **State** column for the server displays "Activated".
14. Repeat steps 12–13 for the second Intelligent Capture Server.
15. Run Failover Cluster Manager to move each Intelligent Capture Server to the other node.
16. Repeat steps 10–14 to activate the Intelligent Capture Servers on the other node.
17. Use the Failover Cluster Manager to move the Intelligent Capture Server applications to the other node again and verify that they remain activated in Intelligent Capture Administrator. In Active/Active cluster, move the Intelligent Capture Server applications so that both servers are running on Node 1, verify they are activated, then move both applications to Node 2, and verify again they are activated.

5.4 Installing Intelligent Capture Web Client and Intelligent Capture REST Service

You install both Intelligent Capture Web Client and Intelligent Capture REST Service as a single Web site on Microsoft IIS. In turn, multiple instances of Intelligent Capture Web Client and Intelligent Capture REST Service can run in a Web farm.

Intelligent Capture Web Client adds value to your document capture operations by providing an easy-to-use, Web-based capture application that you can run in your browser at branch offices and other remote locations.

The Intelligent Capture REST Service Web application is a JSON REST web service that provides batch creation and Module Server processing features.

Note: No load-balancing is inherently performed among multiple instances of Intelligent Capture REST Service in a Web farm.

Prerequisites

- See "IIS Roles Enabled with Intelligent Capture Web Components" on page 187.
- Because WebDAV blocks the `DELETE` HTTP verb that Intelligent Capture Web Client uses, either do not install the WebDAV IIS feature or remove the WebDAV module from the Intelligent Capture Web Client web site. Otherwise, if the `DELETE` HTTP verb is blocked by WebDAV, then user logout does not occur and resources, such as a license consumed by the user, are not freed until the session expires.
- Intelligent Capture client applications, such as Intelligent Capture Web Client and custom applications, require the Intelligent Capture REST Service.
- Intelligent Capture Web Client requires the following additional Intelligent Capture components:
  - Intelligent Capture Server
  - Module Server

    See "Installing and Configuring the Module Server" on page 111.
- For OAuth Client configuration within OTDS, the following requirements must be met:
  - The OAuth Client must have permissions to add application roles.
  - The sign-out URL must point to the Intelligent Capture Server's session endpoint (`https://server/cp-rest/session`) and use the verb **Delete**.
  - The redirect URL must allow redirects to the Intelligent Capture Server`https://server`.

Note: The REST server copies the roles from the Intelligent Capture Server to the OTDS. All changes to roles must be done on the Intelligent Capture Server. Changes made to the OTDS are overwritten when synchronized.

Procedure

If you want to configure Windows single sign-on (SSO) authentication in Intelligent Capture Web Client, see "Configuring Windows Single Sign-on (SSO) Authentication in Intelligent Capture Web Client" on page 109 before starting this procedure.

1. On the first IIS machine in the Web farm, perform the following tasks:

    a. Install Intelligent Capture Web Client and Intelligent Capture REST Service by running the Intelligent Capture setup program and, on the **Installation Choices** list, selecting **Step 2 - Install Web Components** > **Intelligent Capture Capture Web Client (CWC) and REST** and following the instructions.

    The following are guidelines for the **Configure the Intelligent Capture Web Client** dialog box.

Web site name	The name of the web site used in the IIS Server.
IP Address to use for this web site	This value sets Intelligent Capture and REST Service's **Site Bindings**> **IP Address**. See the Microsoft IIS documentation for guidelines on selecting an IP address. Both Intelligent Capture Web Client and Intelligent Capture REST Service use the same IP address and port; however, they use different contexts in their URLs.
TCP port that this web site should use	This value sets Intelligent Capture and REST Service's **Site Bindings**> **Port**. See the Microsoft IIS documentation for guidelines on selecting an IP address. Even if the specified *TCP* port is in use by an existing IIS website (for example, the built-in IIS default website), the Intelligent Capture REST Service and Intelligent Capture Web Client Web site is still created. However, you must stop the existing Web site and start the Intelligent Capture REST Service and Intelligent Capture Web Client one instead.

Make Intelligent Capture Web Client web site online after installation	If you are installing Intelligent Capture Web Client and Intelligent Capture REST Service in a production environment, do not start Intelligent Capture Web Client and the Intelligent Capture REST Service immediately; otherwise, users might inadvertently access an incomplete configuration.
Public URL in absolute format <http|https>://<hostname>/<path>	The URL that users are to use to call Capture Web Client. It sets **IIS Management Console** > **Intelligent Capture Capture Web Client and REST Services** > **Application Settings** > **SaaSPublicBaseURL**. The format is as follows: `[http|https]://<servername>:<port>` <*servername*> is the server name or its IP address. <*port*> is the port number.

Intelligent Capture Web Client shared data folder	This folder contains temporary image capture files and other state information as well as a shared configuration file. For better performance, it is recommended that this folder reside on a high performance disk (such as SAN) separate from the Intelligent Capture REST Service and Module Server machines. If you are running multiple instances of Intelligent Capture REST Service and the Module Server, make sure all of them specify the same shared data folder; in addition, the shared data folder must be `read/write/delete/create` accessible from all of the instances. Make sure that the file store, on which the shared data folder resides, has enough space to store temporary image files being uploaded. In general, the file store should have 20 times the maximum amount of image file data that you expect to be uploaded and remain resident on the file store at any one time. To estimate this size, use the following formula: `<MaxConcurrentUsers> * <MaxBatchSizeBytes> * 20` where: • *<MaxConcurrentUsers>* – the maximum number of users that are logged in at any one time. The maximum number of users includes ones who have not logged off even though they may not be currently uploading image files. **Note:** User sessions are cleaned up after the user is logged off or after the session timeout value specified for Intelligent CaptureREST Service. • *<MaxBatchSize>* – the maximum amount of image data that is to be uploaded in a batch by a single user. For example, if you expect a maximum of 500 users to connect at any time and you expect those users to create a batch up to a maximum of 10 MB, then the

	sizing guideline is: 500 * 10MB * 20 = 100 GB.

b. Configure settings that apply to all Intelligent Capture REST Service Web sites in the entire Web farm by selecting **Start** > **OpenText Intelligent Capture**> **REST Service Config** and following the instructions.

Notes

- You can also run REST Service Config from the command line. For more information, see "Running CaptivaRestServerConfig.exe from the Command Line" on page 105.
- To change the current configuration settings, select the shared data folder. The current configuration settings are loaded from the shared configuration file.

Data Folder	This folder is a shared data folder that contains temporary image capture files and other state information as well as a shared configuration file. For more information, see the **Intelligent Capture Web Client shared data folder** property in the previous step.
Web Server	
Session Timeout (Minutes)	The timeout for user sessions. If you do not want them to time out, specify a very large number. The minimum is 5 minutes.
Maximum Intelligent Capture Server Connections	The maximum number of simultaneous connections from the Web server to the Intelligent Capture Server.
Intelligent Capture Server Message Timeout (Seconds)	Valid values are between 20 – 300 seconds, inclusive.

Authentication Mode	Select the user authentication method as follows: • **Windows**: Use Windows authentication on the Web server machine. For each Intelligent Capture REST Service user (which includes both Intelligent Capture Web Client and custom application users) perform the following: – Assign a Windows user account on Intelligent Capture REST Service's Web server so that their Windows access token can be used to validate their permissions on the Intelligent Capture Server. – Assign other permissions as described in "Setting Up Required Intelligent Capture Permissions for Intelligent Capture Web Client and REST Application Users" on page 103. **Notes** ○ The user's Windows user account must be in a domain that the Web server trusts. • **Custom**: Use your own custom authentication plug-in. Your custom authentication plug-in must return roles that would provide Intelligent Capture permissions as required for processing tasks, creating batches, or administering licenses. For more information, see *OpenText Intelligent Capture - Scripting Help (ECPCORE-H-PSC)*. • **OpenText Directory Services**: Use the OpenText Directory Services (OTDS). The **OpenText Directory Services** tab is displayed. On the **OpenText Directory Services** tab, set up the properties that correspond to the OAuth2 authentication handler properties in the OTDS administration client. You use the OTDS administration client as follows: – Generate the client ID and secret for the OAuth2 authentication

	handler that corresponds to the Web Client or a REST Service custom client. – Set the redirect URLs for the OAuth2 authentication handler to point to Web Client. – Set Web Client privileges to allow editing of OTDS roles. Intelligent Capture roles are synchronized (via the REST server) to OTDS **Application Roles** in a new **Intelligent Capture Roles** partition. Intelligent Capture departments are synchronized (via the REST server) to OTDS **Application Roles** in a new **Intelligent Capture Departments** partition. For more information, see *OpenText Directory Services: OpenText Administration Client Help*.
Module Allocation Timeout (Seconds)	The maximum number of seconds that an Intelligent Capture REST Service request waits to be processed by a Module Server service module instance.
Minimize User Interaction	Do not display hints when a user logs into Intelligent Capture Web Client for the first time. In addition, in the **Review** step, the review entry dialog boxes are hidden and **Next** becomes **Submit** (which immediately submits the batch or prompts the user if issues remain).
Task Waiting Timeout (Minutes)	The maximum number of minutes that an Intelligent Capture REST Service task waits to be processed by a Module Server service module instance.
Debug Tracing	Enables/disables debug tracing.
Enable at-rest encryption	Enables (default) or disables the encryption of user session files, that is, scanned pages and imported images uploaded and downloaded by users. Before enabling or disabling encryption, make sure that all users are logged off of the Intelligent Capture REST Services system and then restart the system, including Intelligent Capture REST Services on IIS and Module Server instances.

Enable Transport Security	Enables secure connections between the Intelligent Capture REST Services on IIS and Module Server instances. The IIS worker process and the Module Server and its instances must all run in the same domain and use the same domain identity account.
Intelligent Capture Server	
Server	The host name (or IP address) of an Intelligent Capture Server or Intelligent Capture Servers in a ScaleServer group.
Connect to server group	Specifies to connect to the servers in a ScaleServer group as specified in **Server**. For more information, see *OpenText Intelligent Capture - Common Production Tasks Guide (ECPCORE-UMD)*.
User and **Password**	An Intelligent Capture Server user name in the Intelligent Capture Administrators role (and which is also a Windows domain user) and password. The format for the user name is *<DOMAIN>**<username>*. Specify * (asterisk) to use the Intelligent Capture Web Client and Intelligent Capture REST Service website's IIS application pool identity.
Service Modules	See "Configuring Service Modules" on page 113.
OpenText Directory Services **Note:** Displayed when **Authentication Mode** is set to **OpenText Directory Services**.	
Oauth Url	The URL to the OTDS authentication handler.
Client Id	The client ID of the OTDS authentication handler.
Client Secret	The client secret of the OTDS authentication handler.

c. At this time, you could configure this IIS instance as instructed in Step 2 before installing and configuring Intelligent Capture Web Client and Intelligent Capture REST Service on other IIS instances in the Web farm.

2. To configure every IIS machine–including the first one–in the Web farm, perform the following:

a. In the **IIS Management Console**, for **Application Settings** for the **Intelligent Capture Capture Web Client and REST Services** site (default name), change **CaptivaSharedDataDirectory** to the shared data folder.

Note: (Optional) You can also change the following entries:

- **CaptivaRestServerName**: A string that is displayed in diagnostic tracing information on the server. It should be a unique name across all Intelligent Capture REST Service Web sites associated with the same shared data storage. By default, Intelligent Capture REST Service constructs a unique name for the service as a combination of the machine name plus the Web site name.
- **CaptivaAuthPlugin**: The full path to your custom Intelligent Capture REST Service authentication plug-in.
- **SaaSPublicBaseURL**: You should specify the URL that users are to use to call Capture Web Client in the following format:

  ```
  [http|https]://<servername>:<port>
  ```

  <servername> is the server name or its IP address.

  <port> is the port number.

  The **SaaSPublicBaseURL** value is the part of the URL that is in front of the `/cp-rest` context.

  It also specifies a Web server's URL to use as absolute links in the JSON response. If you are using a Web farm, then you could specify the URL of the virtual load balancing server; otherwise, the URL could be different from one request to another because the URL of the specific Web farm machine that is processing a particular response would be used.

b. For the `CaptivaCWCAndRestAppPool` **Application Pool** identity, perform the following:

- 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 Capture REST Service works with performance counters for special tracing and reporting purposes.

Note: Although not necessary, adding the identity to the `Administrators` group provides more than sufficient permissions.

- Add the identity to the Intelligent Capture `Administrators` role so that it has the necessary permissions on the Intelligent Capture Server.

c. Configure the SSL certificate and HTTPS binding in the **IIS Management Console** by adding these bindings in **Sites** > **Intelligent Capture Capture Web Client and REST Service** > **Actions** > **Bindings**.

Note: Do not block any **HTTP Verbs** under **Request Filtering**.

3. On every IIS machine–you have already completed this step for the first machine–in the Web farm, install Intelligent Capture Web Client and Intelligent Capture REST Service by running the Intelligent Capture setup program and on the **Installation Choices** list and selecting **Step 2 - Install Web Components** > **Intelligent Capture Capture Web Client and REST** and following the instructions.

   For details, see Step 1.a.

4. License Intelligent Capture Web Client and Intelligent Capture REST Service.

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

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

5. (Optional) Localize and rebrand the Intelligent Capture Web Client user interface with your own application and company names.

   For more information, see "Localizing and Rebranding the Intelligent Capture Web Client User Interface" on page 107.

5.4.1 Setting Up Required Intelligent Capture Permissions for Intelligent Capture Web Client and REST Application Users

Note: You can enable the operator to select a specific batch to process instead of only being able to select the next available task from any batch by assigning the required permissions in the "To Process a Single Batch on Capture Web Client (CWC)" column.

Table 5-1: Required Intelligent Capture Permissions for Intelligent Capture Web Client and REST Application

Permission	Log in to the REST Service	To Create Batches on REST Service	To Log in to Capture Web Client	To Create Batches on Capture Web Client	To Process All Batches on Capture Web Client	To Process a Single Batch on Capture Web Client	To Administer REST and Capture Web Client Licensing (from the License Administration page)
`Server.Login`	Required	Required	Required	Required	Required	Required	Required
`DWebClient.Login`	N/A	N/A	Required	Required	Required	Required	Required
`DBWEBCLNT ModuleLic`	N/A	N/A	N/A	N/A	Required	Required	N/A
`System.BatchRead`	Required	Required	Required	Required	Required	Required	Required
`System.BatchModify`	Required	Required	Required	Required	Required	Required	Required
`System.ProcessRead`	Required	Required	Required	Required	Required	Required	Required
`System.ServerRead`	N/A	N/A	N/A	N/A	Required	Required	N/A
`Server.Create.Batch`	N/A	Required	N/A	Required	N/A	N/A	N/A
`DWebClient.RunSingleBatch`	N/A	N/A	N/A	N/A	N/A	Required	N/A

Permission	Log in to the REST Service	To Create Batches on REST Service	To Log in to Capture Web Client	To Create Batches on Capture Web Client	To Process All Batches on Capture Web Client	To Process a Single Batch on Capture Web Client	To Administer REST and Capture Web Client Licensing (from the License Administration page)
`Captiva Administrator`	N/A	N/A	N/A	N/A	N/A	N/A	Required

5.4.2 Running CaptivaRestServerConfig.exe from the Command Line

If you want to deploy the same settings to a different Web farm or environment (such as production or testing), you can use the command line and a text file. For help on the syntax, execute the following command:

```
C:\Program Files (x86)\InputAccel\WebComponents\binnt\CaptivaRestServerConfig.exe -h
```

(The default path is shown. You must run the command as administrator.)

In the text file, you specify the following options, which map to the corresponding **REST Service Config** fields:

Option	Field
IAUser	**Intelligent Capture Server > User**
Password	**Intelligent Capture Server > Password**
Url	**Intelligent Capture Server > Server**
IAScaleServer	**Intelligent Capture Server > Connect to server group**
UserSessionTimeoutSec	**Web Server > Session Timeout**
IAConnectionPoolSize	**Web Server > Maximum Intelligent Capture Server Connections**
IARequestTimeoutSec	**Web Server > Intelligent Capture Server Message Timeout**
AuthMode	**Web Server > Authentication Mode**
ModuleAllocationWaitSec	**Web Server > Module Allocation Timeout**

Option	Field
MinimumUserExperience	**Web Server > Minimize User Interaction**
TaskWaitingTimeoutSec	**Web Server > Task Waiting Timeout**
WebserverDebugTrace	**Web Server > Debug Tracing**
FPOCR_Instance_Count	**Service Modules > Full Page OCR > Instance Count**
FPOCR_Recycle_In_Hours	**Service Modules > Full Page OCR > Recycle in Hours**
FPOCR_Debug_Tracing	**Service Modules > Full Page OCR > Debug Tracing**
IMGCONV_Instance_Count	**Service Modules > Image Converter > Instance Count**
IMGCONV_Recycle_In_Hours	**Service Modules > Image Converter > Recycle in Hours**
IMGCONV_Debug_Tracing	**Service Modules > Image Converter > Debug Tracing**
CPIMGPRO_Instance_Count	**Service Modules > Image Processor > Instance Count**
CPIMGPRO_Recycle_In_Hours	**Service Modules > Image Processor > Recycle in Hours**
CPIMGPRO_Debug_Tracing	**Service Modules > Image Processor > Debug Tracing**
CPEXTRAC_Instance_Count	**Service Modules > Extraction > Instance Count**
CPEXTRAC_Recycle_In_Hours	**Service Modules > Extraction > Recycle in Hours**
CPEXTRAC_Debug_Tracing	**Service Modules > Extraction > Debug Tracing**
ClientNoop_Instance_Count	**Service Modules > Scripting > Instance Count**
ClientNoop_Recycle_In_Hours	**Service Modules > Scripting > Recycle in Hours**
ClientNoop_Debug_Tracing	**Service Modules > Scripting > Debug Tracing**

5.4.3 Localizing and Rebranding the Intelligent Capture Web Client User Interface

You can localize Intelligent Capture Web Client user interface elements such as page and section titles, menu items, button names, and tool tips as well as informational, warning, and error messages.

You can rebrand the Intelligent Capture Web Client user interface with your own application and company names, which are displayed on the login page and at the top of every Intelligent Capture Web Client page.

Localized and branding strings are contained in locale-specific resource files. When Intelligent Capture Web Client is started, all resource files corresponding to the locale setting in the browser are loaded. Third-party applications could specify the corresponding locale code in the URL's `culture` query string. The default and fallback locale code is `en-US`.

Note: The following kinds of strings cannot be localized using the Intelligent Capture Web Client localization mechanism:

- Messages that originate from the Cloud Capture Toolkit.
- The values displayed within fields are dependent on the language of the value.
- **Form** pane field names are controlled by the Document Type.

Locale-specific resource files (including US English) are packaged in theIntelligent Capture Web Client as follows:

Language	Locale Code
English (Default)	`en-US`
Chinese (Simplified)	`zh-CN`
French	`fr-FR`
German	`de-DE`
Italian	`it-IT`
Japanese	`ja-JP`
Korean	`ko-KR`
Portuguese (Brazilian)	`pt-BR`
Russian	`ru-RU`
Spanish (Spain)	`es-ES`

5.4.4 Creating Resource Files

For each applicable locale, you create a locale resource file and, optionally, a branding string override resource file, which overrides branding strings in the locale resource file. You can create a branding string override resource file for any locale that is packaged with the Intelligent Capture Web Client or for new locale resource files that you create.

Locale resource file

This resource file contains both localized and branding key-value pairs.

Locale-specific file name and default path

`C:\inetpub\captiva\cp-swc\strings\<language>-<country>.js`

<language>	An ISO 639, two-letter, lowercase language code.
<country>	An ISO 3166, two-letter, uppercase country code. **Note:** If *<country>* is not specified, then omit the hyphen (-).

Syntax

Strings that are displayed in the user interface are specified as key-value pairs. See the default file, `en-US.js`, for examples of valid syntax.

Notes

- Only the key-value pairs specified in the default locale resource file, `en-US.js`, can be localized using the Intelligent Capture Web Client localization mechanism.
- The fallback locale file is `C:\inetpub\captiva\cp-swc\strings\en-US.js`; that is, if a key is not found in a locale file, then the key's value in the `en-US.js` file is displayed. However, if the key is missing from `en-US.js` or the JavaScript in this file is invalid, then `[<key>=NA]` (where *<key>* is the name of the key) is displayed instead of the key's value.

Branding string override resource file

This resource file contains branding key-value pairs that override the same branding key-value pairs specified in the identically named file in `C:\inetpub\captiva\cp-swc\strings` (default path).

Locale-specific file name and default path

`C:\inetpub\captiva\cp-swc\branding\strings\<language>-<country>.js`

<language>	An ISO 639, two-letter, lowercase language code.
<country>	An ISO 3166, two-letter, uppercase country code. **Note:** If *<country>* is not specified, then the hyphen (-) must be omitted.

Note: This file must have the same name as the corresponding file in `C:\inetpub\captiva\cp-swc\strings` (default path).

Syntax

Strings that are displayed in the user interface are specified as key-value pairs. See the default file, `en-US.js`, for examples of valid syntax.

Note: The only branding key-value pairs that can be overridden are specified in `C:\inetpub\captiva\cp-swc\branding\strings\en-US.js` (default path).

5.4.5 Configuring Windows Single Sign-on (SSO) Authentication in Intelligent Capture Web Client

You can configure Windows single sign-on (SSO) authentication (also known as "pass-through login") in Intelligent Capture Web Client for Windows domain users.

The following restrictions apply:

- For Windows single sign-on (SSO) authentication, Google Chrome and Microsoft Edge (Chromium based) are supported. You must use NTLM as the only provider (IIS > Authentication > Providers).
- Only an intranet is supported.
- Proxy servers are not supported.
- All client browser machines, the IIS Web server, and Intelligent Capture Server must all be on the same Windows domain and have full access on it.
- The host name in the URL provided to the client browser must be the same as the one in the Intelligent Capture REST Service's `web.config` file's `RestServiceURL` property.

  Note: If you use an IP address, then the IP address must be specified in Internet Explorer's **Local intranet** > **site** property.
- To provide the same security context in a Web farm with a load balancer, the load balancer must maintain affinity with the appropriate Web server.
- The browser would not usually run in Administrator mode because of UAC. Therefore, use an account that is different from the Windows Administrators

group to grant Intelligent Capture permissions for the Intelligent Capture Web Client browser users.

5.4.6 Setting Query String Parameters When Calling Intelligent Capture Web Client

You can set options in the Intelligent Capture Web Client URL by using the following query string parameters.

Note: Unless otherwise noted, these parameters can only be set for `Home.aspx`.

Parameter	Description
appvalues	Root level values (level 7) to use in the batch. The format is a comma-delimited list of name-value pairs (in which a colon separates the name and value). The syntax is as follows: `appvalues=<name1>:<value2>,<name2>:<value2>`
autologout	Set to `true` to automatically log the user out after submitting the current batch and immediately prior to displaying the batch name in the batch submission status panel. By default, the user is returned to the login page (`login.aspx`). To redirect the user to a specific URL, specify *logoutret*. **Note:** Line-of-business applications can take advantage of this parameter.
cptvticket	A valid CPTV ticket to be used when retrieving protected pages. If the CPTV ticket is invalid, then the user is redirected to the login page (`login.aspx`).
culture	A culture code used to override the culture (for any page, not only `Capture.aspx`) specified in the `Accept-Languages` header.
eai	The *extraAuthInfo* parameter (for the custom server-side authentication plug-in) in the login call to the REST service.
logoutret	The URL to which to redirect the user when the user logs out manually or is automatically logged out of Intelligent Capture Web Client; however, the user is not logged out from the REST service. **Note:** Line-of-business applications can take advantage of this parameter.

Parameter	Description
profile	Name of a capture profile.
scannerlock	Set to `true` to lock the scanner settings so that users cannot change them in Intelligent Capture Web Client. For example, if you do not want users to change the scanner settings that were set by a capture profile, then you would use this parameter. **Note:** Setting *scannerlock* to `true` does not reset existing scanner settings. Therefore, if a user has already changed scanner settings, then you might want the user to delete the entire browser cache to remove those settings. You can also select the **Scanner Lock** option for the **Distributed Capture** import profile in Intelligent Capture Designer.

5.5 Installing and Configuring the Module Server

The Module Server is a Windows service that provides classification and extraction, full-page OCR, image conversion, and image processing features.

A Module Server Windows service manages a set of service modules and can be scaled up to meet demand.

5.5.1 Installing the Module Server

Note: Because of the limited number of printer ports, do not install or run any Intelligent Capture client modules, other than the required ones, and the Module Server on the same machine; in addition, set each required Intelligent Capture client module's Windows Service's **Startup Type** to **Manual**.

Tip: Because of potential format differences in date/time and numeric values, it is a best practice to set all Module Server machines within the same Web farm to the same locale.

To install the Module Server:

1. For each instance, run the Intelligent Capture setup program and on the **Installation Choices** list, select **Step 4 - Client Components** and follow the instructions. Optionally, you could install a virtual printer.

   For **Data Folder**, specify the shared data folder. All instances of the Module Server and Intelligent Capture REST Service must specify the same shared data folder. For more information, see Client Web Capture shared data folder.

- After installation, you can change the Module Server shared data folder as follows:
  - Specify the shared data folder in the `dataDirectory` parameter in the Module Server's Windows Service **Properties** > **Start parameters** and restart the Module Server Windows service. The syntax for the `dataDirectory` parameter is as follows:

    ```
    -DataDirectory:<sharedDataDirPath>
    ```

    `C:\ProgramData\EMC\InputAccel\CPMODSRV\Config\CPMODSRV.config` (default) is created and the new path is saved in `CPMODSRV.config`.

    Note: `CPMODSRV.config` is not created when the Module Server is first installed.
  - After `CPMODSRV.config` has been created, you can change the value of the `dataDirectory` parameter directly in `CPMODSRV.config` and restart the Module Server Windows service.

2. (Optional) To change the defaults of the Module Server service modules, select **Start** > **OpenText Intelligent Capture**> **REST Service Config** and make changes on the **Service Modules** tab:
   - **Instance Count**: Maximum number of instances to run on a single machine.

     Note: If you have installed virtual printers, then the maximum number of Image Converter service instances specified in this property is overridden by the number of installed virtual printers.
   - **Recycle in Hours**: Number of hours after which an instance is restarted.
   - **Debug Trace**: Whether to enable debug tracing.

   For more information, see "Configuring Service Modules" on page 113.
3. (Optional) Virtual printers can be installed and uninstalled for the Image Converter service.

   To run `VirtualPrinterInstaller.exe`, the Image Converter module's **Virtual Printer** feature is required.

   To install or uninstall virtual printers, execute `\Client\binnt\VirtualPrinterInstaller.exe` as follows:

   ```
   VirtualPrinterInstaller.exe [-printerPort:<Printerport> | -uninstall]
   ```

   where:

`-printerPort:<PrinterPort>`	Specifies the particular port to which to install a virtual printer at <*PrinterPort*>. For example, to install a virtual printer that uses COM1: `VirtualPrinterInstaller.exe -printerPort:COM1`
`-uninstall`	Uninstalls all except for one virtual printer, just in case it is required by the Image Converter service.

5.5.2 Configuring Service Modules

You can configure the set of service modules running under a machine's Module Server by creating a configuration for them. Each configuration specifies the instance count, recycle period, and debug tracing mode of the Module Server's service modules. If you want multiple Module Servers to all have the same configuration settings, then you can put them into the same group.

To configure service modules:

1. Select **Start** > **OpenText Intelligent Capture**> **REST Service Config** and, on the **Service Modules** tab, create configurations in the following ways:

   - Add a single configuration by clicking **Add** > **Configuration**.
   - Add configurations to a group by first clicking **Add** > **Group** to create a group or selecting an existing group and then clicking **Add** > **Configuration**.

   Note: You can also delete configurations.

2. To specify the machine for each configuration, in the **Type** field, select **Name** (the NetBIOS name), **IP Address**, or **IP Range** and then specify its corresponding value in the **Server Name**, **Server IP Address**, or **IP Address Range** fields.

   Wildcards can be used in the **Server Name** and **Server IP Address** fields only:

? (question mark)	Matches, one time only, any single character in the machine name or any single digit in the IP address.
***** (asterisk)	Matches, zero or more times, any single character in the machine name or any single digit in the IP address.

   Note: If a matching configuration (by name or IP address) is not found for a Module Server, the **Default** configuration is used.

3. For each configuration or group, specify values for the following.

Note: Because all configurations in a group share the same values, you can only change these values at the group level.

- **Instance Count**: Maximum number of instances to run on a single machine.

  Note: If you have installed virtual printers, then the maximum number of Image Converter service instances specified in this property is overridden by the number of installed virtual printers.

- **Recycle in Hours**: Number of hours after which an instance is restarted.
- **Debug Trace**: Whether to enable debug tracing.

5.6 Installing Advanced Cloud OCR

Advanced Cloud OCR is a separate MSI and is available for download from the Intelligent Capture 21.4 (or later) product download site. The installer uses the standard Intelligent Capture installation folders for its destination.

Before installing Advanced Cloud OCR, ensure that you meet the following prerequisites:

- Your system must already have an installation of Intelligent Capture 21.4 (or later) prior to installing Advanced Cloud OCR.
- For the OCR engine to work, you will need a personalized license that can be obtained from Google Cloud Platform (GCP) subscription. In your GCP subscription, add Cloud Vision API to get your service account and credentials (keys). For details on how to set up Cloud Vision API and to get the credentials (contained in a JSON file), see https://cloud.google.com/vision/docs/setup.

  Note: OpenText does not provide Google licenses or credentials.

To install Advanced Cloud OCR:

1. Download the installer from the Intelligent Capture 21.4 (or later) product download site.
2. Follow the steps in the installer wizard.
3. In Windows, add an environment variable for the Advanced Cloud OCR engine:

   1. Using Windows Search, to open the Environment Variables dialog, search for **Edit environment variables for your account**. If you open the System Variables dialog, click the **Environment variables** button.
   2. To add a new system variable, click **New**.
   3. In the Variable name field, type `GOOGLE_APPLICATION_CREDENTIALS`.
   4. In the Variable value field, type the path to your credential file.

5. Click **OK**.

4. In Recognition Designer, add the Advanced Cloud OCR engine:

    1. Click **Tools**.
    2. Select **OCR/ICR Engine**.
    3. Click **New**.
    4. Click **Custom OCR**.
    5. Type the preferred name for how the engine will be displayed.
    6. From the list, select **Advanced Cloud OCR**.

The Advanced Cloud OCR engine is now available to use.

5.6.1 Setting a Region for Processing Advanced Cloud OCR

The standard processing region is global. If you have data that must not leave your region, you can set a specific region by adding an environment variable. As of the point of writing, the following regions are available:

- **EU**: eu-vision.googleapis.com
- **US**: us-vision.googleapis.com

For a list of all available regions, visit https://cloud.google.com/vision/docs/ocr#regionalization.

To set a region for processing Advanced Cloud OCR:

1. Using Windows Search, to open the Environment Variables dialog, search for **Edit environment variables for your account**. If you open the System Variables dialog, click the **Environment variables** button.
2. To add a new system variable, click **New**.
3. In the Variable name field, type `VISION_API_URL`.
4. In the Variable value field, enter the link of the desired region.
5. Click **OK**.

The Advanced Cloud OCR engine is now configured to use the specified processing region.

5.7 Installing the Intelligent Capture Asian Language Add-on

The Intelligent Capture Asian Language Add-on is a separately purchased option and adds the following languages to the Advanced OCR/ICR engine:

- Chinese (Simplified)
- Chinese (Traditional)
- Chinese (Traditional, Hong Kong)
- Japanese
- Korean
- Thai

Furthermore, because the following modules use the Advanced OCR/ICR engine, they can also use the aforementioned languages:

- Completion
- Identification
- Extraction
- Classification
- Standard OCR

A compatible version of Intelligent Capture is required. For more information, see the *Release Notes*.

To install the Intelligent Capture Asian Language Add-on:

1. Run the installer on the same machine on which the Advanced OCR/ICR engine is installed and follow the instructions.

   Note: You can also run the installer as a standard Windows silent install (that is, using the `/qn` option).

2. Restart Intelligent Capture Designer and all modules that use the Advanced OCR/ICR engine.

5.8 Unattended Installations

The Intelligent Capture installers enable unattended and silent installations and upgrade of components. Unattended installations and upgrade are performed without user interaction during its progress. It also enables users to perform remote installations of Intelligent Capture. A silent installation does not display messages or windows during its progress. A command line is used to specify the features to install and the configuration settings. The command line consists of variables known as "installer properties" which define the features to install and the configuration of the installation. The installer properties are simple key/value pairs specified with *<PROPERTY=VALUE>* syntax.

Installation order for silent installations

Install Intelligent Capture components in the following order when performing a silent installation or upgrade:

1. (Optional) Intelligent Capture Database
2. Intelligent Capture Server
3. (Optional) Intelligent Capture Web components
4. (Optional) Module Server
5. (Optional) Intelligent Capture Web Client and Intelligent Capture REST Service
6. Intelligent Capture client components

For examples of command lines that silently install or upgrade Intelligent Capture, see Command line instructions.

5.8.1 Understanding Installation Command Line Arguments

The following command line arguments are available when installing Intelligent Capture features in unattended or silent mode:

Table 5-2: Intelligent Capture Installation Command Line Arguments

Argument	Description
`Setup.exe`	Use the `Setup.exe` installation executable located on the installation media. Access these directories where the Intelligent Capture Microsoft Installer (MSI) files reside: • `Databases\setup.exe`: Installs the SQL database. • `Server\setup.exe`: Installs the Intelligent Capture Server. • `Clients\setup.exe`: Installs the Intelligent Capture client modules. • `WebComponents\setup.exe`: Installs Intelligent Capture Web Client and Intelligent Capture REST Service.
`/s`	InstallShield argument that executes a silent setup.
`/v`	InstallShield argument that passes command line options and values of public properties to `msiexec.exe`. The entire MSI argument line must be enclosed in quotes immediately following the `/v` switch. For example, enable logging of installer messages to the file `c:\temp\logfile.txt` as follows: `setup.exe /v"/l*v "c:\temp\logfile.txt""` `/v` is an InstallShield argument and the `/l*v` are `msiexec.exe` arguments. Include the "*" wildcard parameter (encompasses all parameters except the verbose parameter) along with the `v`, or verbose, parameter to create a detailed log of the installation.
`/l`	InstallShield argument that creates a log file that can be used to troubleshoot installation issues.
`Msiexec.exe` arguments	Specifies an installer action: For example: • `/i`: Install. • `/f`: Repair. • `/x`: Remove. **Note:** The `/i` argument is the default and does not need to be specified.
Windows Installer properties	Specifies an installer action.

Argument	Description
Features to install	Installs the specified Intelligent Capture features. For example, the following command line installs an Intelligent Capture Server: `setup.exe /s /v"/qn ADDLOCAL="ALL" SERVER_INSTANCES="1" IA_SERVICES_ RUNAS_LOCAL_SYSTEM="1" /promptrestart"`

5.8.2 Command Line Considerations

When installing Intelligent Capture from a command line, consider the following.

Escape characters

When creating the installation command line, some installer properties and characters must be escaped (by adding a backslash ("\") before the character) for the installation to succeed.

Properties containing spaces

Any property containing a space must have escaped double-quotes. For example:

```
INSTALLDIR=\"c:\Program Files\InputAccel\Client\"
```

or

```
IA_SERVICES_RUNAS_USER_ACCT=\" CORP\My Login\"
```

Ampersand symbol

Some characters require escaping by the Windows command prompt. The ampersand symbol (&) must be escaped using a caret character (^).

Maximum length

The maximum number of characters that can be entered on the command line is 1066. If more characters are entered, `setup.exe` launches and then quits.

5.8.3 Installing Intelligent Capture from a Command Line

Use the InstallShield and Windows Installer command line arguments to create instructions to install Intelligent Capture software.

To install Intelligent Capture from a command line:

1. From the **Command Prompt** or **Start** > **Run**, browse to `setup.exe` in the installation program directory, which includes the **Clients**, **Databases**, **Server**, and **WebComponents** directories.
2. Type a customized installation command in one line to add, modify, repair or remove Intelligent Capture features.

Example 5-1: Installing one Intelligent Capture Server type

```
setup.exe /s /v"/qn ADDLOCAL="ALL" SERVER_INSTANCES="1" IA_
SERVICES_RUNAS_LOCAL_SYSTEM="1" /promptrestart"
```

Caution

Use of non-code page Unicode characters in the setup program may cause data corruption and installation failure. Only specify characters from the code page of the machine running the setup program.

Note: You can automatically install Intelligent Capture features using a batch file that contains silent installation command line instructions.

5.8.4 Automating Unattended Installations

You can specify multiple installation command lines in a batch file to automate an unattended installation. The following example shows three commands contained within one batch file that generate a log file:

Example:

```
 1 //Begin contents of irr_sp1.bat batch file
 2 //Install Service Pack 1 and write log file
 3 setup.exe /s /v"/qn ADDLOCAL="ALL" IA_SERVICES_RUNAS_LOCAL_SYSTEM="1" /l*v
 4  "C:\logs\sp1_install.log""
 5
 6 //Remove COPY features and write a log file
 7 setup.exe /v"/qn REMOVE="COPY" /l*v "C:\logs\sp1_remove.log""
 8
 9 //Repair features and write log file
10 setup.exe /v"/qn /fvomus /l*v "C:\logs\sp1_repair.log""
11 //End contents of irr_sp1.bat batch file
```

- The first command line argument installs the entire Clients directory.
- The second command line argument removes selected features of the installation.
- The third command line argument repairs the features removed by the second command line argument.

5.8.5 Modifying Unattended Installations

From the directory location of the base Intelligent Capture *MSI* files, you can modify unattended installations by:

- **Adding features and modules**: To add a feature or a list of features, use the `ADDLOCAL` property. For examples, see Supported Intelligent Capture feature properties and names.
- **Removing features and modules**: Use the `REMOVE` property to remove a feature or a list of features. After removing features, repair the installation. The following example removes the COPY module and creates a log file of the procedure:

  ```
  setup.exe /v"/qn REMOVE="COPY" /l*v "C:\logs\remove.log""
  ```

Use the /x Install Shield switch to remove the **Clients**, **Databases**, **Server**, or **WebComponents** directories. For example, from a **Command Prompt** window, navigate to the `Clients` directory on the Intelligent Capture installation media. At the command prompt, type the following command line to remove the **Clients** directory and write a log to the specified directory:

```
setup.exe /v" REMOVE="ALL" /qn /l*v "C:\delete.log""
```

Note: Use the Intelligent Capture Administrator module to delete an Intelligent Capture Server or remove an Intelligent Capture Server from a ScaleServer group before removing the server. For more information, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

- **Repairing an Intelligent Capture installation**: Use the /f *MSI* switch to repair an installation. The following command line example repairs the removed features:

  ```
  setup.exe /v"/qn /fvomus /l*v "C:\logs\sp1_repair.log""
  ```

5.9 Manually Registering a Client Module to Run as a Service

By default, Intelligent Capture client modules that can run as services are installed as services. Users may want to manually register client modules to run as services in the following situations:

- The client module was installed as an application during the installation process.
- The modules were uninstalled as services to change the login parameters.

Not all modules can run as services. For a list of client modules that can run as services, see "Intelligent Capture Modules" on page 189.

To manually register a client module to run as a service:

1. Open a command window with **Run as administrator** privileges on the machine where the client module is installed.
2. In the command window, switch to the directory where the module executable files are installed. By default, this is `C:\Program Files\InputAccel\Client\binnt`. Alternatively, use full path names for each file name specified in the following commands.
3. Enter one of the following commands, according to the type of module you are configuring. This is the same command line that is entered to run the module, but with the `-install` argument appended:

   Note: Optional parameters are offset in [ ] brackets. Do not include the brackets when typing the parameters.

   - Modules that are listed as "New in 7.0 - 7.7, 16.5, 16.6, 20.2" in "Intelligent Capture Modules" on page 189:

```
<moduleexecutable>.exe
 -login:<username>,<password>@<servername>
 -install[:<serviceName>] -serviceAccount:<account>
 -servicePassword:<password>
```

- Modules that are listed as "New in 6.x" in "Intelligent Capture Modules" on page 189, except custom exporters:

```
quickmodulehost.exe -modulename:<moduleexecutable>
 -login:<username>,<password>@<servername>
 -install[:<serviceName>] -serviceAccount:<account>
 -servicePassword:<password>
```

- Export modules that are listed as "New in 6.x" in "Intelligent Capture Modules" on page 189 (including Documentum Advanced Export):

```
quickmodulehost.exe -modulename:<moduleexecutable>
 -login:<username>,<password>@<servername>
 -loginex[:<username>,<password>@<repository>]
 -install[:<serviceName>]
```

- Modules that are listed as "Available prior to 6.0" in "Intelligent Capture Modules" on page 189:

```
<moduleexecutable>.exe
 -login:<username>,<password>@<servername> -install
```

where:

- *<moduleexecutable>* is the full module name. In the case of modules that are "New in 6.x", *<moduleexecutable>* includes the namespace; for example, `Emc.InputAccel.Rescan`. Do not include the `.dll` extension of the module namespace. In the case of Documentum Advanced Export, the full *<moduleexecutable>* is `DocumentumAdvancedExport`. For other modules, *<moduleexecutable>* is the executable name of the module; for example, `iatimer` for the Timer module.

- `-login:`*<username>*`,`*<password>*`@`*<servername>* are the credentials to log into the Intelligent Capture Server. For security reasons, we recommend not specifying an actual user name and password in the command line because doing so also stores these items as unencrypted text in the registry. Instead, use the "run-as" account specified in the **Log On** tab of the Windows Service Control Manager window. To do this, specify * for the *<username>*,*<password>* argument; for example ...-login:*@*<servername>*... *<servername>* is the name of machine hosting the Intelligent Capture Server to which the module should connect when running as a service. The topic "Running Modules as Services" on page 19 provides more information on how to configure modules to run as services.

- *<account>* specifies the account that the service will run as. If the account is not specified, then the service is registered as **LocalSystem**. Allowed values are: `LocalSystem`, `LocalService`, `NetworkService`, and `domain\username`.

- -servicePassword:*<password>* where *<password>* specifies the password for the `serviceAccount`. The default value is **None** which is applicable only if the service account is a named user.
- *<serviceName>* is the name by which the service is registered and listed in the Service Control Manager. Omit this argument to register the service using its default module name. Specifying this parameter enables running multiple instances of the same module, each as a separate service. This is not supported for modules that are listed as "Available prior to 6.0" in "Intelligent Capture Modules" on page 189.
- `-loginex:`*<username>*`,`*<password>*`@`*<repository>* are the credentials used by a custom export module to log into a third-party repository.

Notes

- Registering a module as a service from the command line configures the module to run as a service; it does not install or run the module.
- Registering a module as a service when it is already registered overwrites its previously-registered properties with the new properties.
- Only modules listed as "New in 6.x" in "Intelligent Capture Modules" on page 189 support the *<serviceName>* attribute. When specified, this argument enables configuration of multiple instances of a single module to run as a service, each with a unique service name. When a module is registered as a service, parameters such as a user name or account name can be specified. If the service is reregistered, the newly specified parameters, or default parameters if none are specified, overwrite the existing ones. To register another instance of a client module as a service on the same machine, run the command with a unique *<serviceName>* to avoid overwriting the previously installed service.
- To configure a module registered as a service for high availability, configure the **Recovery** tab in the Windows Service Control Manager. The Intelligent Capture Client setup program does this automatically when it registers a module as a service; however, you must configure this option when manually registering a module as a service. To match the configuration used by the Intelligent Capture Client setup program configure the following settings:
  - **First failure** list: select **Restart the Service**
  - **Second failure** list: select **Restart the Service**
  - **Subsequent failures** list: select **Restart the Service**
  - **Reset fail count after** field: Enter `1` days
  - **Restart service after** field: Enter `1` minutes

Caution

When configuring a module to run as a service, do not enable **Allow service to interact with desktop**. When a module runs as a service, it suppresses its user interface and does not run properly when configured to interact with the desktop.

5.9.1 Unregistering Client Modules Registered as Services

Intelligent Capture client modules that are registered as services can be unregistered.

To unregister a client module registered as a service:

1. Open the command window on the machine where the client module is registered as a service.
2. In the command window, switch to the directory where the module executable files are installed. By default, this is `C:\Program Files\InputAccel\Client\binnt`. Alternatively, use full path names for each file name specified in the following commands.
3. Enter one of the following commands, according to the type of module you are configuring. This is the same command line entered to run the module, but with the `-uninstall` argument appended:

   - Modules that are listed as "New in 6.x" or "New in 7.0 - 7.7, 16.5, 16.6, 20.2" in "Intelligent Capture Modules" on page 189:

     `quickmodulehost.exe -modulename:<moduleexecutable> -uninstall[:<serviceName>]`

   - Modules that are listed as "Available prior to 6.0" in "Intelligent Capture Modules" on page 189:

     `<moduleexecutable>.exe -uninstall`

   where:

   - *<moduleexecutable>* is the full module name. In the case modules that are "New in 6.x", <*modulename*> includes the namespace; for example, `Emc.InputAccel.DocumentumAdvancedExport`. Do not include the `.dll` extension of the module namespace. In the case of traditional executable modules, <*modulename*> is the executable name of the module; for example, `iatimer` for the Timer module.
   - *<serviceName>* is the name by which the service was registered. Omit this argument if the service was registered under its default service name.

   After the module is unregistered as a service, it can continue to run as an application. (Exceptions: the Web Services subsystem, including Web Services

Coordinator, Web Services Hosting, and the Web Services Input and Web Services Output modules, can only run as services, not as applications.)

Chapter 6

Installing Intelligent Capture in a Development or Demonstration Environment

This section describes an installation where all Intelligent Capture or Intelligent Capture Real Time Services components are installed on a single machine.

Caution

A single machine deployment must only be used in a development, demonstration, and extremely low volume production environment.

Note: Intelligent Capture Real Time Services uses the same installer as Intelligent Capture.

"Development or Demonstration Installation" on page 127 summarizes the configuration for a single machine installation:

Table 6-1: Development or Demonstration Installation

Machine	Component to install	User Account
Machine 1	(Optional) Intelligent Capture Database hosted by SQL Server	N/A
	Intelligent Capture Server	User in the local **InputAccel_Server_admin_group** group
	Unattended Intelligent Capture client modules	**Network Service** or domain user
	Attended Intelligent Capture client modules	Domain user

To install Intelligent Capture on a single machine:

1. Make sure the machine meets the system requirements outlined in the *Release Notes*, available in My Support (https://support.opentext.com). For the best performance, always use the vendor's latest operating system (that Intelligent Capture supports) for all Intelligent Capture components. Furthermore, you should always make sure that you have applied the latest service packs and patches to your supported operating system for all Intelligent Capture components. In addition to meeting the other recommended system requirements, keeping your operating system up-to-date helps to ensure the best performance for your Intelligent Capture system.

2. Make sure the locale, globalization, and code page settings are specified as detailed in "Locale Considerations" on page 12.
3. (Optional) Perform the following steps:
   a. Install the Intelligent Capture Database components.
   b. Create a SQL Server user account with minimum permissions to access the Intelligent Capture Database.
4. Install the Intelligent Capture Server components.
5. Install the Intelligent Capture client components.
6. Activate the Intelligent Capture Server and install the Intelligent Capture licenses.
7. Set the UI language for Intelligent Capture components.

Chapter 7

Upgrading Intelligent Capture

This section explains how to upgrade an existing Intelligent Capture system.

7.1 Planning an Upgrade

Upgrading requires careful planning and execution. Upgrade planning includes the following activities:

- Understanding the valid "Upgrade Paths" on page 130.
- "Understanding Compatibility among Intelligent Capture Components, Web Client, and REST Services" on page 130.
- "Understanding Locale Considerations before Planning the Upgrade" on page 133.
- "Identifying Irreplaceable Files" on page 135 to archive.
- "Identifying New System Requirements" on page 138 and obtaining new equipment as needed.
- "Understanding the Upgrade Process" on page 140.
- Granting "Permissions and Roles" on page 139 so users can use the upgraded system.
- "Performing Pre-Production Testing and Acceptance" on page 139.
- "Scheduling Upgrade Phases" on page 140.

Note: Intelligent Capture Real Time Services, including Intelligent Capture Web Client and Intelligent Capture REST Service, cannot be upgraded from versions 16.5 or earlier. You must uninstall the existing Intelligent Capture Web Client and Intelligent Capture REST Service Web sites and then install 22.2. You can uninstall the previous installation and install 22.2 by using the **Install Web Components** > **Upgrade** dialog box; however, the previous installation's `web.config` settings are not preserved. For more information, see "Installing Intelligent Capture Web Client and Intelligent Capture REST Service" on page 94.

Make sure that your existing users' permissions conform to the permissions (new as of 7.7) requirements as described in "Setting Up Required Intelligent Capture Permissions for Intelligent Capture Web Client and REST Application Users" on page 103.

7.1.1 Upgrade Paths

Customers can upgrade to Intelligent Capture 22.2 from the following versions only:

- Intelligent Capture 22.1
- Intelligent Capture 21.4
- Intelligent Capture 20.2
- Intelligent Capture 16.6
- Intelligent Capture 16.5
- Intelligent Capture 7.7

To upgrade from any other version, first upgrade to the latest applicable supported version and then perform the upgrade. Alternatively, perform a new installation as explained in "Installing Intelligent Capture in a Production Environment" on page 47.

7.1.2 Understanding Compatibility among Intelligent Capture Components, Web Client, and REST Services

This section provides compatibility information related to the various components and can help plan an upgrade scenario for your specific environment.

Intelligent Capture supports rolling upgrades of client modules; that is, customers may upgrade client machines gradually (or not at all) while still being able to connect to Intelligent Capture Server 22.2 until you want to upgrade them. The specific versions that can connect to an Intelligent Capture Server 22.2 are shown in Client Upgrade Compatibility table. The Intelligent Capture Server refuses connections from clients of any other version. Version 22.2 client modules cannot connect to Intelligent Capture Servers from previous releases.

For more information about the locale, globalization, and code page settings to consider when planning an upgrade, see "Understanding Locale Considerations before Planning the Upgrade" on page 133.

The versions of the following components must be the same:

- The Intelligent Capture Database (if installed), Intelligent Capture Server, and all four components of the Intelligent Capture Web Services subsystem (WS Input, WS Output, WS Coordinator, and WS Hosting) must all be the same version; that is, you cannot mix versions of these core components. These components must be at the 22.2 version level before client modules are allowed to connect to the 22.2 server.
- All client modules that are installed on a single physical machine must be the same version. For example, Intelligent Capture 7.7 client and Intelligent Capture 22.2 client modules cannot run together on the same machine.

- Intelligent Capture Web Client must be the same version as the Intelligent Capture Server and the Intelligent Capture REST Services version released with that Intelligent Capture Server.

Table 7-1: Client Upgrade Compatibility with Intelligent Capture Server

Intelligent Capture Client version	Connects to upgraded Intelligent Capture Server version 22.2?	Connects to new Intelligent Capture Server version 22.2?	Can be upgraded to version 22.2?
6.0	No	No	No
6.0 SP1/SP2/SP3 6.5 6.5 SP1	No	No	No
6.5 SP2	No	No	No
7.0	No	No	No
7.1	No	No	No
7.5	No	No	No
7.6	No	No	No
7.7	Yes (1)	Yes (1)	Yes
16.5	Yes (1)	Yes (1)	Yes
16.6	Yes (1)	Yes (1)	Yes
20.2	Yes (1)	Yes (1)	Yes
21.4	Yes (1)	Yes (1)	Yes
22.1	Yes (1)	Yes (1)	Yes

Notes

- In-place upgrade is supported for 64-bit operating systems only because the Intelligent Capture 20.2, 21.4, 22.1, and 22.2 installers are a 64-bit application.
- The following notes correspond to the numbers in parentheses in the table:
  1. Versions 7.7, 16.5, 16.6, 20.2, 21.4, and 22.1 client modules can connect to a 22.2 server (upgraded or new installation) if the 22.1 database is an external or internal database as it was in the previous version (for example, if the 7.0 database was external, then the 22.2 database must also be external). Furthermore, the external or internal database can be either an upgraded or new installation.

Intelligent Capture REST Services

Intelligent Capture REST Services versions are as follows:

Note: If you upgrade to Intelligent Capture 22.2, then Intelligent Capture REST Services versions 1.0 (released with Intelligent Capture 7.1) and 2.0 (released with Intelligent Capture 7.5) must also be upgraded to version 2.1, 2.5, or 2.6.

- Intelligent Capture REST Services 2.1
  - Released with Intelligent Capture 7.6.
  - Includes the Intelligent Capture REST Service Web application that runs on Microsoft IIS.
  - Includes the Module Server Windows service.
  - Customer- and partner-developed clients that use Intelligent Capture REST Services 2.1 are completely compatible with both Intelligent Capture Servers 7.6, 7.7, 16.5, 16.6, and 20.2.
- Intelligent Capture REST Services 2.5
  - Released with Intelligent Capture 7.7, 16.5, and 16.6.
  - Includes the Intelligent Capture REST Service Web application that runs on Microsoft IIS.
  - Includes the Module Server Windows service.
  - Customer- and partner-developed clients that use Intelligent Capture REST Services 2.5 are completely compatible with both Intelligent Capture Servers 7.7, 16.5, 16.6, and 20.2.
- Intelligent Capture REST Services 2.6.0
  - Released with Intelligent Capture 21.4.
  - Includes the Intelligent Capture REST Service Web application that runs on Microsoft IIS.
  - Includes the Module Server Windows service.
  - Customer- and partner-developed clients that use Intelligent Capture REST Services 2.6.0 are completely compatible with both Intelligent Capture Servers 21.4, 22.1, and 22.2.

7.1.3 Understanding Locale Considerations before Planning the Upgrade

A pure Intelligent Capture version 22.2 system (all components and modules upgraded to version 22.2) can operate across multiple languages, multiple code pages, and multiple regional settings. Depending on decisions made during the system upgrade, certain language and code page restrictions may apply.

- To process multiple languages from different code pages in the same task or use different regional settings among client modules and Intelligent Capture Servers, upgrade the client modules to version 22.2.
- If using modules that were developed by your own software developers or OpenText Global Technical Services, be aware that they are most likely not designed for double-byte characters. Unless these modules are updated to handle double-byte characters, they can only process tasks that contain single-byte (non-East Asian) data values. Furthermore, because Intelligent Capture has changed the way in which it handles date and number formatting for multiple locales, if these custom modules read and write date and number values, data may become corrupted if the module connects to an Intelligent Capture Server that is using different locale formatting than the client. To successfully continue using custom modules, be sure that they connect to an Intelligent Capture Server that is using the same locale, globalization, and code page settings.
- Process Developer is code page-based; therefore you must obey the following restrictions when developing processes that support multiple languages and code pages:
  - Choose a single code page and use it as the system code page across all machines running Process Developer. If you choose not to heed this restriction, then you must use only *ASCII* characters for process names, step names, IA value names, variable names or Visual Basic code. This means, for example, that you cannot use non-ASCII characters in direct literal assignments or in local variable names. (Although Process Developer allows you to use non-ASCII characters for these items, the Intelligent Capture Server does not allow you to install a process containing non-ASCII characters if it detects that the process was compiled on a machine having a different code page.)

Caution

The Intelligent Capture Server cannot detect whether it is code page-compatible with pre-6.5 processes. Data corruption or server exceptions may occur if your processes were compiled on a pre-6.5 system that had a different code page setting than the Intelligent Capture Server. Therefore, you should recompile and reinstall all processes that are being used in a mixed code page environment.

These restrictions do not apply to department names or to the default values of IA values defined in *MDF*s using *UTF-8* encoding. In other words, Unicode

characters are supported in dynamic IA value names. Also, none of these restrictions apply if the Process Developer machine and the Intelligent Capture Server are using the same code page.

- Use a UTF-8 editor (for example, Windows Notepad) to define a custom data-only MDF to hold literal text values in multiple languages. MDFs may declare Unicode (UTF-8) values.
- In the custom data-only MDF, define variables for all literal text that use characters from languages that are not included in the specified system code page. The variable names themselves must use characters from the system code page only; however, the values may be in any language present in the system. For example, if the Process Developer system code page is 1252, the variable names must use characters from the Latin alphabet (English, French, Spanish, Portuguese, and others); however, the values may be any mixture of these or other languages, such as Korean, Chinese, French, and Russian.
- Use only characters from the Process Developer system code page for the following:
  - Process names
  - IA value names
  - Step names
  - Variable names
- If you plan to execute your processes on machines with a different code page than the machine on which the process was defined, do not use any literal strings that contain non-*ASCII* characters in your *VBA* code. (If your environment has only a single code page, VBA literal strings can be defined without this restriction.)

When processes are designed following these recommendations, batches from the resulting complied process can be run on Intelligent Capture Servers and client machines using any combination of code pages and regional settings (subject to the upgrade considerations described in this section).

To ensure seamless multiple language/multiple code page compatibility, use CaptureFlow Designer instead of Process Developer to create your process.

Note: For more information on the multiple language feature in Intelligent Capture, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

7.1.4 Identifying Irreplaceable Files

Certain files should be archived before performing any upgrade. Creating an archive is important when:

- Re-implementing custom index validation code after upgrading.
- Rolling back the system to the previous version.
- Preserving previously-customized processes in case you need to roll back the installation.
- Preserving special patches and module customizations in case you need to roll back your installation.

The upgrade process automatically backs up certain key files and settings on servers and client machines. However, making copies of the following files and data, and store them in a safe place is a recommended practice.

Table 7-2: Irreplaceable Files and Data

Data Type	Host location	Default File Location	Notes
Activation files	Intelligent Capture Servers	`C:\ias\activation\*.*`	Files used by software security key activation (*CAF*) files. Retain these files in case reactivation becomes necessary. Identify each activation file according to the server from which it was archived.

Module Definition Files	Process Developer machines	`C:\program files\inputaccel\client\src\ipp\*.mdf\`
		
		`program files\inputaccel\client\pcf\*.mdf`
		
		`inputAccel\client\src\ipp\dia`
			Your developers or OpenText Global Technical Services may have customized *MDF* files. Retain these files for future maintenance.

Data Type	Host location	Default File Location	Notes

Integrated ProcessFlow Project source files	Process Developer machines	`C:\program files\inputaccel\client\src\ipp\*.ipp`
		
		`client\src\ipp\dia`
			Your developers or OpenText Global Technical Services may have created or customized *IPP* files. Retain these files for future maintenance.

Intelligent Capture System files	Intelligent Capture Designer machines	`C:\Users\<<username>>\My Documents\Intelligent Capture <version>\Default`	This directory is the working directory for Intelligent Capture Designer. It includes configuration settings for Intelligent Capture Designer as well as files for Intelligent Capture systems such as Captureflows (XPPs), profiles, document types, and scripting.
`settings.ini`	Client machines	`C:\Users\<user>\AppData\Local\VirtualStore\ProgramData\EMC\InputAccel` **Note:** If the user has read/write permissions on `C:\ProgramData\EMC\InputAccel`, then `settings.ini` is created in it, instead.	Contains settings for tuning module behavior. May have been customized on a client-by-client basis; therefore, identify each `settings.ini` file according to the client machine from which it was archived. This file contains settings for modules that are listed as "New in 6.x" in "Intelligent Capture Modules" on page 189.

Data Type	Host location	Default File Location	Notes
Batches and stage files	Intelligent Capture Servers	`C:\ias\batches\*.*`	All in-process data (images, intermediate files, and other batch data). Each Intelligent Capture Server has a unique set of batches; therefore, identify each data set according to the server from which it was archived. Be aware that there may be a large amount of data.

Processes	Intelligent Capture Servers	`C:\ias\process\*.iap`
		
		`\Client\src\ipp\dia`
			Compiled versions of `.ipp` files that are used in daily production. They are typically based on customized source files. All Intelligent Capture Servers within a ScaleServer group should contain an identical set of processes; therefore, archiving a single server should be sufficient.

Supplemental module configuration files	Intelligent Capture Servers	`C:\ias\modules\*.*`	Some client modules store shared configuration files such as templates, reference images, or other data files in this location. Check each server to determine if multiple archives are necessary.
Registry parameters	Intelligent Capture Servers	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InputAccel\Parameters`	You or OpenText Global Technical Services may have modified server registry values to tune performance. Check each server to determine if multiple archives are necessary.

7.1.5 Automatic Backup during Upgrade

When upgrading the Intelligent Capture Server and client machines, the setup programs automatically create backup directories containing copies of key files so that you can restore the previous version. Maintain these backup directories until you are certain that the updated system is functioning as expected and that you will not need to return to the previous version.

Table 7-3: Automatic Backup Locations during an Upgrade

Location	Automatic backup directory	Contents
`C:\Program Files\InputAccel\Server`	`$InputAccelServer<version>$`	Files that were used in previous versions to restore a previous version of Intelligent Capture Server files.
`C:\Program Files\InputAccel\Client`	`$InputAccelClient<version>$`	Files that were used in previous versions to restore a previous version of Intelligent Capture client files.

7.1.6 Identifying New System Requirements

Many existing components have new system requirements and some new components have been added. In some cases, the hardware and software hosting your current system might not be suitable for the most recent Intelligent Capture version. Carefully check the information in the *Release Notes* to be sure you are upgrading on supported platforms. For the best performance, always use the vendor's latest operating system (that Intelligent Capture supports) for all Intelligent Capture components. Furthermore, you should always make sure that you have applied the latest service packs and patches to your supported operating system for all Intelligent Capture components. In addition to meeting the other recommended system requirements, keeping your operating system up-to-date helps to ensure the best performance for your Intelligent Capture system.

Caution

Upgrade customers may require higher performing hardware due to the new features. Test your environment to ensure you have adequate performance.

Note: As with any upgrade, go to ISIS Scanner Drivers (http://www.emc.com/microsites/scannerdrivers/index.htm) to ensure your scanner will still be supported in the new environment.

7.1.7 Permissions and Roles

Several system **Roles** with permissions become available after an upgrade. The Intelligent Capture **Administrator** can assign users and groups to these roles without creating them. The Intelligent Capture administrator may, if required, define additional user roles, possibly additional Administrator roles, and assign appropriate users to each of those roles. The minimum Intelligent Capture permissions needed to run a module in production mode include:

- Server.Login
- Server.Read.Module.Data
- Server.Write.Module.Data
- System.BatchRead
- System.BatchModify
- System.ProcessRead

Some modules require additional permissions to function, and certain specific tasks (other than processing batches) require special permissions. For information about permissions and user roles, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

7.1.8 Performing Pre-Production Testing and Acceptance

If possible, perform an upgrade in a test environment before upgrading in a production environment. Follow all appropriate upgrade steps, install new functionality and integrate replacement modules, and update processes, settings and custom behaviors. Then run acceptance tests using typical documents and also test for performance and throughput.

Proceed to upgrade your production environment only after you achieve the expected results from the test upgrade.

Migrating configurations and settings stored in the Intelligent Capture Database from a test environment to a production environment requires the use of the IAMigrate application. Information on using this tool is provided in the *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

7.1.9 Scheduling Upgrade Phases

After completing upgrade testing and acceptance, carefully schedule each phase of the production system upgrade. Consider the following recommendations:

- Determine which components you will upgrade in each phase.
- Locate all installation media for the current system prior to beginning the upgrade. You will need these items if unexpected upgrade issues require rolling back the upgrade to the previous version.
- Choose the best day of the week to upgrade, taking advantage of both production and non-production time.

  For example, if production normally operates five days per week, consider upgrading the night before the last production day of the week. You then will have a full day of production load followed by two days of non-production, allowing time to resolve any issues.
- If you encounter major issues during upgrade, contact OpenText Global Technical Services at My Support (https://support.opentext.com).

7.2 Understanding the Upgrade Process

When upgrading, install or upgrade the following components in this sequence:

Step	Component to install or upgrade	For information, see
1	Intelligent Capture Database hosted by SQL Server Required for users upgrading from 7.x customers that installed an external database.	"Intelligent Capture Database" on page 141)
2	Intelligent Capture Servers	"Intelligent Capture Servers" on page 141
3	Intelligent Capture Web Client and Intelligent Capture REST Services	"Intelligent Capture REST Services" on page 131
4	Upgraded Intelligent Capture client modules	"Existing Clients" on page 142
5	New Intelligent Capture client modules	"New Client Modules" on page 150
6	New security keys, licenses, and activation files, as needed	"Licenses, Activation Files, and Security Keys" on page 150

7.2.1 Intelligent Capture Database

Users upgrading from 7.5, 7.6, and 7.7 versions must upgrade their version of the Intelligent Capture Database (if installed). Except for development and demonstration systems, the Intelligent Capture Database should be installed on a dedicated server that meets or exceeds the performance criteria to keep the Intelligent Capture system at peak production capacity. System requirements and recommendations for the Intelligent Capture Database host system can be found in the *Release Notes*. For the best performance, always use the vendor's latest operating system (that Intelligent Capture supports) for all Intelligent Capture components. Furthermore, you should always make sure that you have applied the latest service packs and patches to your supported operating system for all Intelligent Capture components. In addition to meeting the other recommended system requirements, keeping your operating system up-to-date helps to ensure the best performance for your Intelligent Capture system.

7.2.2 Intelligent Capture Servers

Regardless of which version you are upgrading, Intelligent Capture Servers must be upgraded. Furthermore, upgrade customers must ensure that the Intelligent Capture Server machines meet or exceed the system requirements listed in the *Release Notes*. For the best performance, always use the vendor's latest operating system (that Intelligent Capture supports) for all Intelligent Capture components. Furthermore, you should always make sure that you have applied the latest service packs and patches to your supported operating system for all Intelligent Capture components. In addition to meeting the other recommended system requirements, keeping your operating system up-to-date helps to ensure the best performance for your Intelligent Capture system.

For more information about upgrading Intelligent Capture Servers in Microsoft Failover Clustering, see "Upgrading the Server in a Clustering Environment" on page 152.

Caution

For existing customers, be aware that hardware requirements have increased due to increased functionality. For more information related to server requirements for better performance, see "Intelligent Capture Server Considerations" on page 16.

For all upgrade scenarios, if you have configured multiple Intelligent Capture Servers as a ScaleServer group, the ScaleServer group is maintained during the upgrade procedure. Upgrade each Intelligent Capture Server in the ScaleServer group, and then confirm that it is configured as needed by using Intelligent Capture Administrator. For more information, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

Notes

- When upgrading a ScaleServer group, if the setup program detects that the Windows Management Instrumentation (WMI) service is running, it displays a message indicating that WMI will be stopped before proceeding. Allow the setup program to stop WMI to upgrade a ScaleServer group. After the upgrade completes, the setup program restarts the WMI service.
- The name of the Intelligent Capture Server host machine must not be longer than 15 bytes; otherwise, client machines will be unable to connect.
- The upgrade procedure automatically creates a least-privileged user account (LUA) group named **InputAccel_Server_admin_group** if none already exists and then adds the specified domain user account that is used to run the Intelligent Capture Server to this group, enabling the Intelligent Capture Server to operate with a LUA. Details of the LUA configuration can be found in "Running Intelligent Capture with Minimum Microsoft Windows Permissions" on page 31

Caution

When upgrading a ScaleServer group that has one or more Intelligent Capture Servers installed on the same machine as the SQL Server , stop all SQL Server instances and close all Service Control Manager windows before starting the upgrade.

7.2.3 Existing Clients

New client modules are provided as replacements for legacy modules. Also, some modules are no longer shipped.

"Client Module Upgrade Issues" on page 143 lists modules that require special upgrade considerations.

Notes

- The user Help files for legacy modules are removed after an upgrade.
- With any recognition engine upgrade, we cannot guarantee that the performance, accuracy, and behavior will match the previous version. We recommend that you test these changes thoroughly and optimize the settings for your environment before deploying.

Table 7-4: Client Module Upgrade Issues

Module	Upgrade issue
Intelligent Capture Designer	After upgrading, 7.5 or earlier XPP-based CaptureFlows, which were uploaded to the server using CaptureFlow Designer, might be in an incorrect status, **Not in server source**. Workaround: Convert CaptureFlows to the current format and redeploy them from the Intelligent Capture Designer **Deployment** tab (or with CaptureFlow Designer).
Classification Edit	Classification Edit must be at the same version level as its associated modules: • Classification • Extraction • Intelligent Capture Designer (and hence, Recognition Designer) In addition, the recognition project file (DPP) in the recognition project shared directory must have been saved and deployed by the same version of Intelligent Capture Designer/Recognition Designer. **Note:** If the aforementioned modules were upgraded to version 22.2, then the Classification Edit module must also be upgraded to the version 22.2 legacy Classification Edit module (that is, the legacy module installed by the Intelligent Capture 22.2 installer).
Documentum Advanced Export	As of 7.6, this module no longer supports PDF/Web as a content file type for export. Therefore, during setup mode (after upgrading), you must replace PDF/Web with the appropriate output file type for upgraded batches and processes. **Note:** Batches created in Intelligent Capture 7.5 and then upgraded without changing the PDF/Web output file type to a valid output file type fail upon execution in Intelligent Capture 7.6 (or later).

Module	Upgrade issue
East Euro / APAC OCR	As of 7.7, this module is no longer shipped and does not have a replacement. **Notes** • The East Euro / APAC OCR extraction engine that is used in Advanced Recognition is also no longer shipped. • If you are using this module in previous releases, then the East Euro / APAC OCR module (as well as corresponding Advanced Recognition engine) will be available in 22.2 after upgrade. • If you want to continue using this module and are upgrading from 7.5 or earlier, you must first upgrade to 7.6. • To use this module in Intelligent Capture Designer after the upgrade, see the *Release Notes* for the instructions on how to enable the East Euro / APAC OCR module in Intelligent Capture Designer.
Email Import	As of 7.7, this module is no longer shipped and is replaced with the Standard Import module.

FileNet Panagon IS/CS Export	Users no longer need the Panagon API and capture license. This module internally uses IBM IDM API.
	
	As of 7.1, the FileNet Panagon IS/CS Export MDF file contains new fields. Therefore, recompile pre-7.1 processes that use FileNet Panagon IS/CS Export with the 7.5 version of the MDF file, which is located in one of the following default paths:
	
	`C:\Program Files (x86)\InputAccel\src\ipp\iaxfnet2.mdf`
	
	`C:\Program Files\InputAccel\src\ipp\iaxfnet2.mdf`

Module	Upgrade issue

Export for IBM Content Manager	• Export for IBM Content Manager only
	As of 16.5, the Export for IBM Content Manager module has been upgraded to use the IBM Content Manager Java API. If you want to export to the IBM Content Manager Enterprise Edition v.8.5 (or greater), it is recommended to upgrade to the 20.2 module because IBM no longer supports their C++ API.
	• With the Legacy IBM CM C++ client libraries (for v.8.5 and below) option
	As of 16.5, you must install the Export for IBM Content Manager with the Legacy IBM CM C++ client libraries (for v.8.5 and below) option if you want to continue to use the pre-16.5 IBM CM Advanced Export module (which works with the IBM Data Server Client and IBM Content Manager Client for Windows v.8.4) to export to the IBM Content Manager Enterprise Edition v.8.4.
	Note: Although you could also export to the IBM Content Manager Enterprise Edition v.8.5, it is not recommended; install only the Export for IBM Content Manager module instead.
	If you do not want to uninstall the Legacy IBM CM C++ client libraries (for v.8.5 and below) option, you can enable or disable it using the following commands:
	– To enable:
	`regsvr32 exicm818.dll`
	– To disable:
	`regsvr32 /u exicm818.dll`

Module	Upgrade issue
Image Converter	If you no longer require the virtual printer for either Image Converter or the Module Server when upgrading from Intelligent Capture 7.7, 16.5, or 16.6 only to Intelligent Capture 20.2, then you must manually uninstall the virtual printer. That is, when upgrading from the aforementioned versions, clearing the Virtual Printer feature does not remove the existing virtual printer from Windows **Devices and Printers**. Furthermore, if you do not want the Module Server to use the virtual printer, then the virtual printer must be uninstalled. However, if you require the Virtual Printer feature for either Image Converter or the Module Server, then simply select the Virtual Printer feature for the upgrade.
Multi-Directory Watch	As of 7.7, this module is no longer shipped and is replaced with the Standard Import module.
NuanceOCR	• NuanceOCR no longer supports the following Output Format settings: **Excel 97, 2000**, **Microsoft Reader**, **Open eBook 1.0**, **RTF Word ExactWord**, **RTF Word 6.0/95**, **RTF Word 97**, **Word 97**, and **2000, XP** After an upgrade, processing a batch configured to use any of these settings will fail. You will need to reconfigure the batch or process to use supported settings. Review the *NuanceOCR Guide* for more information on the supported settings. • As announced in Intelligent Capture 7.0, the NuanceOCR module no longer supports Intelligent Character Recognition (ICR). After an upgrade, processing a batch configured to use the ICR engine will fail with a message stating that the Handprint Numerals (HNR) and Recognition Handprint (RER) engines are not supported in this version. You will need to reconfigure the batch or process to use a different recognition engine, such as Advanced Zonal OCR.

Module	Upgrade issue
Page Registration	As of 7.7, this module is no longer shipped and does not have a replacement. **Note:** If you were using Page Registration to improve zonal recognition with NuanceOCR, you can migrate to the Extraction module, which also provides zonal recognition. You do not need to purchase an Advanced Recognition license. If you have further questions, contact OpenText Global Technical Services at My Support (https://support.opentext.com).
Recognition Designer	Standard Handprint/General-Use ICR Engine is no longer supported in Recognition Designer. Existing projects that use this engine must be migrated to use the handprint engine included with Advanced Zonal OCR/ICR. The replaced engine does not ensure a feature by feature replacement. The following are some of the differences between Standard Handprint/General-Use ICR Engine and Advanced Zonal OCR/ICR Engine: • Character type **Alphabetic**, **All**, and **Customized** is not required by Advanced Zonal OCR/ICR and will be replaced with **Alphanumeric**. • Engine Mode is not needed and will be ignored. • Reader will be set to default value **Recostar**. • Advanced Zonal OCR/ICR requires a single selection of language.

Module	Upgrade issue
Pre-7.0 customers: Intelligent Capture Designer is installed when a client machine that has Process Developer or CaptureFlow Designer installed upgrades to version 20.2.	After the upgrade completes, both Intelligent Capture Designer and Process Developer reside on the machine. Start using Intelligent Capture Designer to create processes using the graphical-based CaptureFlow Designer, create various profiles, setup modules, and so on. For information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*. To modify pre-7.5 processes in Intelligent Capture Designer 20.2 (and later), you must upgrade them; furthermore, once you have upgraded them, you cannot modify them in earlier versions of Intelligent Capture Designer. **Note:** You are prompted to upgrade pre-7.5 processes when you open them in Intelligent Capture Designer 20.2 (and later). For migration guidance, see "Upgrading Process Developer Processes" on page 162 and "Migrating Process Developer Processes to Intelligent Capture Designer" on page 158 .
Pre-7.0 customers: Automatic Quality Assurance ECM Web Services Importer Configuration iManage WorkSite Server Export PrimeOCR Plus IBM CMIP-390 Export IBM CMIP-390 Index	These modules are no longer shipped and have no replacements.
Pre-7.0 customers: Dispatcher Statistics	As of 7.5, the Dispatcher Statistics database is no longer shipped. Configure Classification and Identification module steps to export statistics to an IA Value or XML file. You could use the Standard Export module's **ODBC** export option to export statistics to a database.

Module	Upgrade issue
Pre-7.0 customers: File System Export Image Export Index Export PDF Export Values to XML	As of 7.5, these modules are no longer shipped and are replaced with Standard Export. For migration guidance, see "Migrating to Use Standard Export" on page 171.
Pre-7.0 customers: Image Image Enhancement	As of 7.5, these modules are no longer shipped and are replaced with Image Processor. For migration guidance, see "Migrating from Image Enhancement to Image Processor" on page 170.
Pre-7.0 customers: Spawn	As of 7.5, this module is no longer shipped and has no replacement.
Pre-7.0 customers: Image Quality Assurance Index IndexPlus Dispatcher Validation	As of 7.5, these modules are no longer shipped and are replaced with Completion. For migration guidance, see "Migrating from Dispatcher Validation to the Completion Module" on page 167, "Migrating from Image Quality Assurance to the Completion Module" on page 164 and "Migrating from IndexPlus and Dispatcher Recognition to Completion and Extraction" on page 164.
Pre-7.0 customers: Dispatcher Recognition	As of 7.5, Dispatcher Recognition is no longer shipped and has been replaced by Extraction. For migration guidance, see "Migrating from IndexPlus and Dispatcher Recognition to Completion and Extraction" on page 164.
Custom modules in CaptureFlow Designer	If you used custom modules in a previous version of CaptureFlow Designer, they will need to be added manually for them to be available in the **Steps** panel. For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.

"Appendix—Intelligent Capture Client Modules" on page 189 identifies key characteristics of each module, including whether it runs in attended mode and unattended mode, whether it is ScaleServer compatible, whether it can run as a service, and whether it provides scripting capabilities.

7.2.4 New Client Modules

While upgrading existing client machines, you may want to install new client modules. These modules can be installed on existing client machines or on new machines.

Note: When installing new client modules, the Intelligent Capture Client setup program also updates all client components.

7.2.5 Licenses, Activation Files, and Security Keys

The licensing mechanism uses a software security key (CAF file). You will need to obtain new licenses for the new client modules.

7.3 Upgrade Procedures

This section includes the procedures to upgrade each component.

7.3.1 Upgrading the Intelligent Capture Server

Upgrading the Intelligent Capture Server involves replacing current versions of all Intelligent Capture Servers with the new version.

Caution

For all upgrade customers, be aware that hardware requirements have increased. For more information related to performance, see "Intelligent Capture Server Considerations" on page 16.

This procedure is required for all upgrade scenarios.

To upgrade the Intelligent Capture Server:

1. Make sure the server machine meets the Intelligent Capture Server requirements as outlined in the *Release Notes*. If the machine does not meet those requirements, then perform the necessary upgrades or select a different machine. Furthermore, if your current operating system is not supported (for example, 32-bit operating systems), then you will most likely need to install Intelligent Capture Server on a different operating system and then migrate your current Intelligent Capture Server configuration to the new Intelligent Capture Server. For more information about the operating system upgrade procedure, see Microsoft TechNet (http://technet.microsoft.com).

2. Record the version numbers of the Intelligent Capture Servers. The version number is displayed in the **Properties** window of the Intelligent Capture Server executable. The version number is required if you need to revert to a previously installed version of Intelligent Capture Server.

3. Disconnect all client modules. Use the Administrator module, the Administration Console, or Intelligent Capture Administrator to view the list of Intelligent Capture Server connections and then disconnect all client modules.
4. Stop the Intelligent Capture Servers. If the Intelligent Capture Server is running as a service, then stop the service.
5. Make a backup copy of the `\IAS` data directory tree to create a snapshot of the system state immediately before upgrade.

   Note: The installer also creates a backup of the current Intelligent Capture Server. For more information, see "Automatic Backup during Upgrade" on page 138.
6. For Intelligent Capture Server 7.x with the Intelligent Capture Database, install or upgrade the Intelligent Capture Database before upgrading the Intelligent Capture Server.
7. Run the setup program with an account that has Administrative privileges. From the **Installation Choices** list, select **Step 2 - Install the Intelligent Capture Server**.
8. Upgrade the Intelligent Capture Servers. See "Installing the Intelligent Capture Server" on page 54 for instructions.

   If you are installing a new Intelligent Capture Server on a different operating system, then copy the backup of the `\IAS` data directory tree to the new Intelligent Capture Server before starting the Intelligent Capture Server.

   Note: To preserve the security settings on the `\IAS` directory, use `xcopy`; you can also reset the proper security settings on the `\IAS` directory by running `C:\Program Files\InputAccel\Server\Server\binnt\ias64.exe -repair` (default path).

   You might also need to reactivate the Intelligent Capture Server and license keys. For more information, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

7.3.1.1 Reverting to a Previously Installed Version of the Intelligent Capture Server

In some situations, you may want to revert to a previously installed version of Intelligent Capture Server. This involves completely removing the Intelligent Capture Server and all previous versions from the system while leaving the Intelligent Capture files and data intact and then reinstalling the earlier version.

To revert to a previously installed version of the Intelligent Capture Server:

1. Remove the Intelligent Capture Server from any ScaleServer group, if applicable.
2. Ensure client modules are compatible with the earlier Intelligent Capture Server. If you have upgraded the client modules, then revert these client

modules to versions that are compatible with the earlier Intelligent Capture Server.

3. Stop the Intelligent Capture Server.
4. Uninstall the Intelligent Capture Server.
5. Reinstall the earlier Intelligent Capture Server version as well as any required patches and service packs.
6. Restart the Intelligent Capture Server.

7.3.2 Upgrading the Server in a Clustering Environment

To upgrade the cluster environment, you upgrade the Intelligent Capture Servers on both nodes and recreate **Named Resource** types for the Intelligent Capture Server applications/roles.

The upgrade does not affect the batches and processes stored on the Intelligent Capture Servers and you do not need to reactivate their licenses.

Note: If you have new module licenses, then install them only after you have completed the upgrade; also make sure that the Intelligent Capture Servers are online in the cluster.

The following are upgrade requirements:

- Make sure that your environment meets the requirements as specified in "Requirements for Intelligent Capture Server in Microsoft Failover Clustering" on page 83.
- Upgrade the Intelligent Capture Database before upgrading the Intelligent Capture Servers in the cluster.

7.3.2.1 Upgrading Intelligent Capture Server in a Microsoft Failover Clustering Environment

Note: Keep the Intelligent Capture Server principal folders as-is.

To upgrade the Server in a Microsoft Failover Clustering Environment:

1. In the Failover Cluster Manager, make the **Other Resources** resource (for example, **InputAccel** or **InputAccel2**) of both applications/roles offline.
2. Move both applications/roles to the same node (node 1 or node 2).
3. For each application/role, delete the **Other Resources** item, but keep the **Server Name** and **Disk Drives** resources as-is and online.
4. Delete the **Named Resource** types for each resource as follows:
   a. Right-click the cluster name in the left pane.

b. Go to **Properties** > **Resource Types** tab > **User defined resource types**, and then select each resource and click **Remove**.

5. Run the Intelligent Capture Server upgrade installer on the node hosting both applications/roles and perform these tasks:

a.

Automatically start the Intelligent Capture Server service when the system starts	Clear this option. The service startup mode for the Intelligent Capture Server services must be set to **Manual** when running it in a cluster.
Start the Intelligent Capture Server service when setup completes	Clear this option. The Intelligent Capture Server should not be started outside of the cluster control.

b. In the **Configure Intelligent Capture Service Accounts** window, select the same credentials for running the Intelligent Capture Server as the current version uses.

c. If required, restart Windows after the installation has completed.

6. Move both applications/roles to the second node.

7. Run the Intelligent Capture Server upgrade installer on the second node as in Step 5.

8. To register the Intelligent Capture Server cluster resource *DLL*s with the cluster, on one node, in a command prompt (running as Administrator), execute the following file for each Intelligent Capture Server:

```
C:\Program Files\InputAccel\Server\<Server#>\binnt\
CreateIAResType.bat
```

where <*Server#*> is the directory for each Intelligent Capture Server.

`InputAccel` resource type is created for the first Intelligent Capture Server and `InputAccel2` resource type is created for the second one.

Note: For more information about running `CreateIAResType.bat`, simply execute it.

9. To add the Intelligent Capture Servers to the cluster application/role, right-click the Intelligent Capture Server application/role and select **Add a resource > More resources… > Add InputAccel** and > **Add InputAccel2**.

Do not make these resources online.

Caution

If the following error message is displayed, then the Intelligent Capture Serversare not installed on both nodes:

```
1 The resource type Add InputAccel is not configured on all nodes.
2 Do you wish to continue and create the resource?
```

10. Edit the **Properties** of the **New InputAccel** resource as follows:

Tab	Action
General	Change the name of the first and second servers to **InputAccel** and **InputAccel2**, respectively.
Dependencies	Insert the following dependent resources for this Intelligent Capture Server: • **Cluster disk** • **Name**
Policies	Until the Intelligent Capture Server is fully licensed and operational, it is recommended that you change the setting of **Response to resource failure** to **If resource fails, do not restart**. **Note:** This setting can be reconfigured later as required. Select any other required settings.
Advanced Policies	Ensure that both nodes are enabled as possible owners.

11. Make the **InputAccel** resource online.

Note: You must make at least one attempt to bring the **InputAccel** resource online before you can edit the parameters in Intelligent Capture Administrator.

7.3.3 Upgrading Client Modules

This procedure applies to upgrading from Intelligent Capture 7.7, 16.5, or 16.6, 20.2, 21.4, and 22.1 to 22.2.

Notes

- If you installed Intelligent Capture Server 7.7, 16.5, 16.6, 20.2, 21.4, or 22.1 with the file-based, internal database, then you need to upgrade only the Intelligent Capture Server before upgrading the client modules.
- If you installed Intelligent Capture Server 7.7, 16.5, 16.6, 20.2, 21.4, or 22.1 with the Intelligent Capture Database, then you must upgrade both the Intelligent Capture Server and the Intelligent Capture Database before upgrading the client modules.

To upgrade client modules:

1. Log in to each client machine as a user with local administrative rights.
2. Stop all Intelligent Capture Server, client software, and client services running on the machine you are upgrading.

3. From the **Installation Choices** list, select **Step 4 - Install Client Components**.
4. A message appears, verifying that the client components installed on the machine must be upgraded to the latest version. Click **Yes** to upgrade.

   Note: At this time, you can also select new modules to install.

5. Adjust features for the selected setup type. Features that are not selected, are marked with a cross sign. Expand each available feature and choose whether you want only the feature installed or the feature and all of its sub-features. After completing the selection, click **Next**.
6. In the **Configure Service Accounts** window, you can define how the following service settings must be configured by installer during upgrade: startup mode and account to log in.

   The following options are available:

   - **Keep logon settings for services running under built-in credentials**: selected by default. If any services in the previously installed Intelligent Capture version use built-in accounts (`NT AUTHORITY/NetworkService`, `NT AUTHORITY/LocalService`, or `LocalSystem`), then after upgrade such services will run under the built-in credentials. For all newly installed services, select **Use the built-in Network Service account** or specify credentials for a user account.

     In case you do not need to keep logon settings for such services, clear the check box and then select **Use the built-in Network Service account** or specify credentials for a user account.
   - **Automatically start newly installed services when the system starts**: select it if you want the newly installed services to be started automatically when the system starts. When the **Reset all service settings to the default values** check box is selected, this option is applied to all services.
   - **Reset all service settings to the default values**: select it if you want all services to run with the default settings. This option does not reset service command line arguments. When selected, the **Keep logon settings for services running under built-in credentials** option is disabled.

   Command line properties provided for these options are specified in the "Client Components Installer Properties" on page 233 section.

7.3.3.1 Reverting to a Previous Client Release

Reverting to a previous client release removes the latest installation of the client modules and reverts to a previously installed release of the client modules.

To revert to a previously installed client release:

1. Stop and close all client modules that are running on the machine you are upgrading.
2. Back up client data.
3. Uninstall the client modules.
4. Reinstall earlier client software, patches, and service packs.

7.3.4 Upgrading Processes

The *<IATaskPriority>* IA value was added in 7.6 P01. Therefore, if you have processes from 7.6 (unpatched) or earlier, you must recompile those processes to use this IA value.

7.4 Sample Upgrade Scenarios

Upgrading to Intelligent Capture requires thoughtful planning and careful execution. This section provides upgrade scenarios for typical situations to help understand the considerations unique to your environment.

7.4.1 Sample Scenario: Upgrade from Intelligent Capture 7.7 to 22.2

This scenario is an upgrade from a release that the 22.2 upgrade software directly supports, Intelligent Capture 7.7. This scenario has the following characteristics:

- Existing 7.7 Intelligent Capture Database.
- One or more 7.7 Intelligent Capture Servers.
- No custom modules and no special customizations by the customer or OpenText Global Technical Services.

To upgrade this Intelligent Capture system:

1. Archive irreplaceable files such that you can roll back to version 7.7, if required.

   For more information, see "Identifying Irreplaceable Files" on page 135.
2. Disconnect all client modules and stop all Intelligent Capture Servers and client services.
3. To upgrade the Intelligent Capture Database, run the Intelligent Capture Database installer.

For more information, see "Installing the Intelligent Capture Database" on page 51.

Note: The system requirements for the Intelligent Capture Database have changed. Be sure your SQL Server installation meets or exceeds the new requirements listed in the *Release Notes*.

4. To upgrade each Intelligent Capture Server, run the Intelligent Capture Server installer on each machine.

   Make sure the Intelligent Capture Server Windows service can be started. For more information, see "Upgrading the Intelligent Capture Server" on page 150.

   Note: The system requirements for the Intelligent Capture Server have changed. Be sure your server machine meets or exceeds the new requirements listed in the *Release Notes*.

5. To install Intelligent Capture Administrator, run the Intelligent Capture Client installer.

   After the upgrade is complete, Intelligent Capture Administrator is installed. Use Intelligent Capture Administrator to install your license codes for new modules and activate the product, if required.

6. NuanceOCR no longer supports the following Output Format settings: **Excel 97, 2000**, **Microsoft Reader**, **Open eBook 1.0**, **RTF Word ExactWord**, **RTF Word 6.0/95**, **RTF Word 97**, **Word 97**, and **2000, XP**

   After an upgrade, processing a batch configured to use any of these settings will fail. You must reconfigure the batch or process to use supported settings. For more information, see *OpenText Intelligent Capture - NuanceOCR Guide (ECPCORE-CNU)*.

7. (Optional) To upgrade existing client modules (including Process Developer and the Web Services subsystem) or install new ones, run the Intelligent Capture Client installer.

   For more information, see "Upgrading Client Modules" on page 154.

Caution

When you upgrade File System Export, PDF Export, Values to XML, Index Export, and Image Export, the setup program uninstalls these modules and installs the Standard Export module. Make sure that you maintain a machine with these modules so that you can continue to use them until you are ready to upgrade your processes to use Standard Export.

Before using the Standard Export module, you must create export profiles in Intelligent Capture Designer, upgrade your processes, and set up each Standard Export step in every upgraded process.

Note: ClickOnce deployment is no longer shipped.

8. (Optional) Edit or create processes to use any new client functionality that you have added (for example, Completion, Standard Import, Identification, Image Processor, Image Converter), and then compile and install them on your Intelligent Capture Servers.

7.5 Migration Guidance

This section is intended to provide IT personnel and administrators with high-level guidance when planning the requirements and tasks involved when migrating to use the new modules and functionality in Intelligent Capture. This section is not a step-by-step set of instructions; it provides enough high level information to help users plan their migration effort. This section must be used as a planning tool and it includes the most common scenarios that users may encounter.

Prerequisites:

Before users plan on migrating, they must:

- Complete the upgrade.
- Read the updated and new documentation to learn about the new functionality.

7.5.1 Migrating Process Developer Processes to Intelligent Capture Designer

This section is targeted towards users that used Process Developer to design processes but now want to migrate to using CaptureFlow Designer for existing processes.

Note: Process Developer provided functionality to trigger module steps, assign values conditionally, assign departments, conditional routing, and basic error handling. All these features are available in the CaptureFlow Designer user interface. In addition, CaptureFlow Designer includes an integrated CaptureFlow Script Editor that enables adding custom code for advanced data manipulation such as iterating and calculating totals, string manipulations, and provides access to more advanced scripting functions. Other benefits of using CaptureFlow Designer to design processes include:

- Processes are more maintainable and easier to understand due to the graphical user interface
- Easier to update processes
- Deployment support
- Ability to configure process steps
- CaptureFlow Designer now compiles processes that require only the .NET runtime. In previous CaptureFlow Designer releases, processes still required

the VBA runtime. Because VBA is an old technology, moving to .NET promotes usability and ensures the ongoing viability of processes. Furthermore, you can now use CaptureFlow Designer to update a process (within certain restrictions) such that after you deploy the updated process, then all of that process's existing batches use the updated process.

The *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)* provides detailed instructions on using CaptureFlow Designer and CaptureFlow Script Editor. For more information on the *API*s used to create CaptureFlow scripts, see*OpenText Intelligent Capture - Scripting Guide (ECPCORE-PSC)*.

To redesign Process Developer processes in CaptureFlow Designer:

1. Start with a technical design of your *IPP*. This design must provide detail on control flows, levels at which the steps are triggered, and so on.
2. Gather dependencies, such as Dispatcher project files, 3rd party validation databases, and export configuration.
3. Verify the steps that you want replaced with newer modules. For example, you may want to replace the Image Enhancement step with the Image Processor step. Learn how value processing is impacted and the new module functionality. Read the specific module guide to learn about using the new module.
4. Port all the dependencies using Intelligent Capture Designer: import the existing *DPP* into the Recognition Designer, get familiar with automatically generated Document Types, create and deploy the Image Processor profiles, and so on. for more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.
5. Rewrite the DPP code for validation using Document Type expressions and field properties, and Document Type Scripting. Details on validation using Document Types are provided in the *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*. Document Type Scripting information and *API*s are provided in the*OpenText Intelligent Capture - Scripting Guide (ECPCORE-PSC)*.
6. Implement Index Families in a Recognition project. For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.
7. Redesign the process in CaptureFlow Designer, adding steps to the canvas, connecting them in the desired order, and specifying trigger levels for each step. For information on creating a process using CaptureFlow Designer, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.

   Note: Existing IPP Finish() code must be implemented in CaptureFlow Designer as a **Decision** block.

   Duplicate IPP value assignments using the **Assign Value** functionality in CaptureFlow Designer.
8. Port scripts written in Process Developer to the redesigned CaptureFlow:

- Port `Finish` and `Prepare` methods to the **CaptureFlow Script Editor**.
- For step error handling: CaptureFlow Designer provides the `ErrorCode` IA value. Use this value to check for errors in the `Finish` routine of the CaptureFlow Script Editor and then continue to the next step.
- For porting Common_Constants used in Process Developer, use the Custom Values functionality of CaptureFlow Designer.
- For Tree `PostNodeAdd` and `PostNodeMove` events: Use the CaptureFlow Designer provided `SubTreeModified` and `TreeNodeModified` nodal values in the `Finish` routine. After a task is finished, these values are populated and provide information on changes to the tree structure and where the change occurred.
- For triggering newly inserted nodes: Add the Completion module to the CaptureFlow. Triggering a node is handled automatically in this module.
- For Tree `PreNodeDelete` and `PreNodeMove` events: There is no direct replacement for these events. You can use the `NodeDeleted` event provided with Document Type Scripting.
- For setting the default values for newly inserted nodes: Use the `NodeMoved` and `NodeAdded` events provided with Document Type Scripting. For more information, see, *OpenText Intelligent Capture - Scripting Guide (ECPCORE-PSC)*.
- For the `StepNotify` event: This event is no longer supported. Users should migrate to using Completion, and modify their process so Completion is triggered at a higher level so the affected nodes are within the task.
- For the `Retrigger` event: CaptureFlow Designer automatically handles step re-triggers. Note that if a step is re-triggered, all the tasks are re-triggered.
- For the `Batch_Create` event: This event is no longer supported.
- For the `Install` event: This event provided the capability to assign initial values for the batch. Users can use the Custom Values functionality in CaptureFlow Designer.

9. Save the redesigned process. If the redesigned process uses the same module steps as the previous process, then save the *XPP* and make sure the name conforms to the *XPP* naming conventions.
10. Compile the CaptureFlow and then install it to the server.
11. Configure the process:
    - If the redesigned process uses the same module steps as the previous process, use Intelligent Capture Administrator to connect to the server where the old process is installed and copy the process settings to file. Then, paste the process settings to the newly designed process.
    - If the redesigned process uses some of the same module steps as the previous process and a few different module steps compared to the previous process, then save the *XPP*, and then configure the module steps that are

different using CaptureFow Designer. Next, use Intelligent Capture Administrator to connect to the server where the old process is installed and copy the module settings for steps that are same in both the old and new process. Then, paste the copied step settings to the newly designed process steps.

12. Upload .NET Code module assemblies and Document Type Script assemblies: Copy the assemblies to the `<solution directory>/bin` directory for deployment. Then in Intelligent Capture Designer, navigate to **System** > **System Configuration** > **Other Options** and enter the names of these assemblies and the `Custom.Uimscript.Dll` in the **DeploymentFiles** field in the **File Management** area.

7.5.2 Migrating CaptureFlow Designer Processes to Intelligent Capture Designer

As of 7.0, CaptureFlow Designer was no longer a standalone module but part of the integrated development tools provided with Intelligent Capture Designer. To continue using CaptureFlow Designer processes, do the following:

1. Rename the existing *XPP* to conform to the current *XPP* naming conventions.
2. Copy the *XPP* to the `\GlobalData\XPP` folder.
3. Open the *XPP* file from Intelligent Capture Designer and ensure that it opens correctly.

   When opening an *XPP* file with **Intelligent Capture Designer > CaptureFlow Designer**, the process flow is automatically updated to use the Synchronize module in place of some Multi module steps.

   If you used custom modules in a previous version of CaptureFlow Designer, they will need to be added manually for them to be available in the **Steps** panel. For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.
4. Connect to the server where the previously configured*XPP* is installed. Open an existing process and copy the step settings to the newly created *XPP* file on the local development system. Save the updated *XPP* file and then compile and install it on the required servers.

In 6.0 SP3, CaptureFlow Designer replaced certain automatically-inserted steps with equivalent steps of a different module. CaptureFlow Designer 1.0 automatically inserted steps that used the Multi module at several key points in the process flow:

- End of batch creation
- Beginning of each decision step
- End of each decision step

7.5.3 Upgrading Process Developer Processes

Your existing Process Developer processes should run as-is in Intelligent Capture 22.2.

If you want to add 22.2 modules and functionality to your existing Process Developer processes, then follow these steps:

To upgrade Process Developer processes:

1. In Process Developer, add module steps for the new client modules in 22.2.
2. Compile the process and reinstall the process to Intelligent Capture Servers.
3. This step is required only if the new client modules added to the process use profiles. Use Intelligent Capture Designer to create profiles and deploy the profiles to Intelligent Capture Servers.
4. Use Intelligent Capture Administrator to configure process steps.
5. Install .NET Code module assemblies, *DPP* project files, and client-side scripting assemblies.

7.5.4 Migrating from Multi-Directory Watch and Email Import to Standard Import

1. In Intelligent Capture Designer, in existing processes, replace legacy Multi-Directory Watch or Email Import module steps with the Standard Import module.
2. Create a corresponding **Import** profile of either the **Email Import** type or **File System** type.

   You can implement similar behavior in Standard Import as follows:

Feature	Procedure
To import email from multiple email servers	Create separate email connection profiles and select all of them in the **Incoming Email Connection** property.
To filter out email attachments that are missing the file extension	Select the **Ignore Attachments without Extension** property.
To prevent inline attachments, such as email signatures, from being imported. Attachments, such as documents, are still imported.	Select the **Ignore Inline Attachments** property.
To import encrypted emails	No configuration required; automatically performed.

Feature	Procedure
To keep emails on the email server in order for another email profile to process them	Specify a filter in the **Email Filter Rule** property and select the **Keep Emails Excluded by Filter** property.
To import encrypted zip files in the batch while at the same time unzipping unencrypted zip files	Select the **Unzip Files** (File System profile) or **Unzip Attachments** (Email profile) properties.
To specify an arbitrary string used to identify the email or file system source, for example, `HR` or `Finance`.	Select the **Custom Value** property (in both File System and Email profiles).

3. (Optional) If customized poll scheduling or tree restructuring is required, create a custom script and reference it in the profile.

4. Add the profile name to each Standard Import module instance by restarting each module instance with the appropriate command line parameters as follows:

   - **Email Import**

     ```
     -
     EmailProfileNames:<profileName>[,<profileName2>,<profileName3>
     ,...]
     ```

   - **File System**

     ```
     -
     FileProfileNames:<profileName>[,<profileName2>,<profileName3>,
     ...]
     ```

   - A profile name configuration file.

     Using a profile name configuration file is a convenient way to add multiple Email and File System profile names to each Standard Import module instance. In addition, using a profile name configuration file can overcome the maximum Windows command line length.

     ```
     -Profilesconfig:configFile
     ```

     To create a profile name configuration file:

     a. Click **Import** > **Import Profiles** > **Create Configuration File**.

     b. Select all of the profiles that you want to add and click **Create**.

   Make sure to also specify the names of any current profiles that you still want to use; otherwise, they would be removed from the Standard Import module instance.

   For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)* or *OpenText Intelligent Capture - Module Reference (ECPCORE-CMD)*.

7.5.5 Migrating from Image Quality Assurance to the Completion Module

This section is targeted towards users of Image Quality Assurance that now want to migrate to using Completion. For information on using the module, see *OpenText Intelligent Capture - Desktop Client Operator Guide: Identification and Completion (ECPCORE-UCV)*.

1. Replace the Image Quality Assurance step in the process with Completion.
2. Use the following settings when you configure Completion:
   - View mode: Image only
   - Trigger level: page
   - Show flags: true, and define the page flags
3. Adjust process routing to use the `DocumentStatus` flag.

7.5.6 Migrating from IndexPlus and Dispatcher Recognition to Completion and Extraction

This section is targeted towards users that used IndexPlus and Dispatcher Recognition but now want to migrate to using Completion and Extraction. For information on using and configuring these modules, see *OpenText Intelligent Capture - Desktop Client Operator Guide: Identification and Completion (ECPCORE-UCV)* and *OpenText Intelligent Capture - Extraction Guide (ECPCORE-CEX)*.

1. Create a Recognition Project in Intelligent Capture Designer.
2. (Optional) Define the *OCR* and field zones if the Extraction module functionality or *KFI* mode is required:
   - If the NuanceOCR engine was used for zonal recognition, then manually define each OCR zone in the newly created recognition project. If NuanceOCR was used for full-page OCR, then you do not have to redo any steps.
   - If a custom OCR module was used, then use the .NET Code module and configure it so that it reads each *OCR* zone and value. Manually assign each field value to document types using InUIMData.
   - If IndexPlus was used to define field zones, then each zone needs to be manually re-defined in the recognition project. OCR engines are not required to define zones if the Extraction module functionality is not required.
3. Remove IndexPlus steps from the process and replace with Completion. Note that IndexPlus and Completion cannot coexist in the same process. Configure module settings as required. Additional configuration includes:
   - Configure the module to use manually created Document Type scripts.

- If using existing exporters, select the option to **Flatten to IA values**. Then configure the exporters to make sure the values are mapped correctly.
- You may be required to map page flags to the RescanPlus step using the `MatchAny` function in CaptureFlow Script Editor.
- If required, add an Image Conversion step to burn annotations into the image.

4. Port client-side scripts (if any):

   - If using IndexPlus, then the Client-side scripts must be manually ported to Document Type scripts.
   - Adjust process routing to use the `DocumentStatus` flag.
   - Write Document Type scripts and configure expressions inIntelligent Capture Designer to handle any custom behaviors preferred, including validation and population functionality that was implemented with the Index module by using one of the validation *DLL* files.
   - Use any .NET IDE to write and compile Document Type scripts. Deploy the scripts to the server.

   Note: All scripting usage is documented in the *OpenText Intelligent Capture - Scripting Guide (ECPCORE-PSC)*.

5. Remove the Dispatcher Recognition step from the process and replace with Extraction if you are using *OCR* to extract zones. Configure it to use the newly created recognition project. In addition, update the existing process to remove NuanceOCR module from the *XPP* if it was used for zonal extraction.
6. Deploy document types and the recognition project using Intelligent Capture Designer.
7. Configure reporting:

   - Configure the Extraction and Completion modules to export statistics to the new reports.
   - Generate the **Operator Productivity**, **Page Extraction**, and **Field Extraction** reports. You could also use the `Template`, `Field`, and `DocType` tables to create custom reports; for more information, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.

Key differences between IndexPlus and Completion

1. Fields in Completion have a data type: string, date/time, number, or boolean.
2. Index values are not assigned by level.
3. The multi-line edit popup functionality is no longer supported in Completion but this functionality can be used with Document Type scripting.
4. Regular expressions functionality is handled using rules.

5. Fields and rules are always auto-validated.
6. Document types in IndexPlus are different from the Document Types created in Intelligent Capture Designer. Use a regular field to store previously defined Document Types.
7. Completion does not allow access beyond the task. Users must use flags so the process can take appropriate action.
8. Completion does not require re-validation.
9. Completion includes document-, page-, and field-level flags.

Key differences between IndexPlus client-side scripting and Document Type Scripting

Many IndexPlus client-side scripting events are replaced with the Document Type scripting events. Significant changes include:

1. In place of the `Initialize` event, users must initialize document data in the `DocumentLoad` event and user interface state in the `FormLoad` event.
2. In place of the `Changed` event, update document data or user interface state when the field loses focus and `ExitControl` executes.
3. In place of the `Populate` event, pre-fill document fields in `DocumentLoad` or update them in `ExitControl` if their values depend on other fields.
4. In place of the `Validate` event, use expressions, database lookups, or scripted validation rules.
5. In place of the task-level `PrepareTask` and `BeforeTaskFinished` events, use CaptureFlow scripting or add the .NET Code Module step and configure the step to modify document data at a task level.

Changes to migrate from using the Legacy Validation DLL:

1. In place of the `Date` method, configure the document type field to a date or use expressions to set its value.
2. In place of the *ODBC* method, configure the document type to use named queries for database validation and `DocumentLoad` or `ExitControl` scripts to populate the field using scripted database lookups.

7.5.7 Migrating from Dispatcher Validation to the Completion Module

This section is targeted towards users that used Dispatcher Validation but now want to migrate to using Completion. For information on using the module, see *OpenText Intelligent Capture - Desktop Client Operator Guide: Identification and Completion (ECPCORE-UCV)*.

1. Import an existing *DPP* file into **Intelligent Capture Designer** > **Recognition Designer**. The DPP is converted and a Recognition Project is automatically created after the import and includes Document Types that are generated from existing Index Families. Also, the defined zones (or free form templates) are available in the imported DPP file.

   Note: Depending on the size of the DPP file, the import operation may take significant time to complete, maybe about an hour.

2. Remove the Validation step from the process and replace with Completion. These modules cannot coexist in the same process.
3. Port Index family scripts to Document Type scripts.
4. Adjust process routing to use the `DocumentStatus` flag.
5. Deploy document types and the recognition project using Intelligent Capture Designer.
6. Configure reporting:

   - Configure Completion to export statistics to the new reports.
   - Generate the **Operator Productivity**, **Page Extraction**, and **Field Extraction** reports. You could also use the `Template`, `Field`, and `DocType` tables to create custom reports; for more information, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.
   - Remove the use of Dispatcher Statistics for the Validation module.

Key differences between Dispatcher Validation and the Completion module

1. Character mode functionality is replaced with character work level.
2. Completion has a new Boolean data type.
3. Partial value formatting is now done with Document Type scripting.

7.5.8 Migrating from Dispatcher Classification Edit to the Identification Module

This section is targeted towards users that used Dispatcher Classification Edit but now want to migrate to using Identification. For information on using the module, see *OpenText Intelligent Capture - Desktop Client Operator Guide: Identification and Completion (ECPCORE-UCV)*.

1. Import an existing *DPP* file into **Intelligent Capture Designer** > **Recognition Designer**. The DPP is converted and a Recognition Project is automatically created after the import and includes document types that are generated from existing index families. Also, the defined zones (or free form templates) are available in the imported DPP file.

   Note: Depending on the size of the DPP file, the import operation may take significant time to complete, maybe about an hour.

2. Remove the Classification Edit step from the process and replace it with Identification.
3. Remap the IA values to fit the new Identification step into the Capture Flow. At a minimum, map page-level IA values <*Image*> (input and output), <*InputPageDataXML*> (input), <*OutputPageDataXML*> (output), and <*OcrDataCahce*> (input and output). The description of each value can be found in the `CPIDENTF.MDF` file and in the *OpenText Intelligent Capture - Desktop Client Operator Guide: Identification and Completion (ECPCORE-UCV)*.
4. Port index family scripts to document type scripts. Use any .NET enabled environment to create and debug new scripting. Upload the compiled `DLL` files on the server using Intelligent Capture Designer.
5. Run setup on the new Identification step(s). The description of all available setup settings can be found in *OpenText Intelligent Capture - Desktop Client Operator Guide: Identification and Completion (ECPCORE-UCV)*. The following Classification Edit setup settings are configured differently or not supported:

Table 7-5: Classification Edit setup settings

Classification Edit setup settings	Identification
External IA Values	Not configurable in setup. You can do it Intelligent Capture Designer through <*UIMDataImportMode*> and <*UIMData_*> IA Values. For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.
Process backside images as pages	Identification setup: Select **Display Back Side of Images**.

Classification Edit setup settings	Identification
Error handling options	Not configurable in setup. The error handling scenario is specified for each CaptureFlow step in Intelligent Capture Designer. For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.
Reject folder if one of its documents is rejected	Identification setup: Supply only one flagging reason for documents and no flagging reasons for pages. At runtime the flag command will mark the selected document as flagged.
Display active folder thumbnails	Not configurable. Replaced by new design of the tree view.
Document-code oriented keying	Identification setup: Select **Identify pages by template code**.
Go to next field automatically	Not configurable in setup. Configured in a document type by setting the field property **Manual Confirmation** to "always confirm". For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.
Display next document automatically	Identification setup: Select settings **Auto Advance to Next Page** and **Auto Advance to Next Document**.
Confirm closing session after task completed	Identification setup: Select **Auto Advance to Next Task**.
Keyboard shortcuts	Not configurable in setup. Shortcuts are provided by default and can be customized in Intelligent Capture Designer. For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.
Color settings (for folders, fields to be confirmed)	Not configurable in setup. Default color settings are provided as system styles and can be customized in Intelligent Capture Designer. For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*. System styles do not include custom colors for even and odd pages in the Page List View.

6. Configure system styles in Intelligent Capture Designer. Upload the configuration file to the server. For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.

7. Deploy document types and the recognition project using Intelligent Capture Designer. For more information, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.

8. Configure Identification to collect statistics:

   - Set up the new Identification steps to export statistics.
   - Reference the `Template`, `Field`, and `DocType` tables from your reporting tool. For more information, see *OpenText Intelligent Capture - Administration Guide (ECPCORE-AON)*.
   - Remove the use ofDispatcher Statistics for the Classification Edit module.

Key differences between Dispatcher Classification Edit and the Identification module

1. Fields (names, labels, data types, behavior, formatting) are defined in a document type that exists out of the `DPP` project but related to it.
2. Index family scripting is replaced by .NET scripting created for a certain document type.
3. Identification reads User Interface color settings from global options (`config` file) uploaded on the server. All Identification and Completion modules that communicate with this server share the same system styles, including color settings.
4. Identification reads shortcuts from the `config` file uploaded on the server. All Identification and Completion modules that communicate with this server share the same shortcuts.
5. Error handling is configured for each step in the process settings rather that during step setup. Error handling can be enhanced with CaptureFlow scripting.

7.5.9 Migrating from Image Enhancement to Image Processor

This section is targeted towards users that used Image Enhancement, Auto Annotate, and Image modules but now want to migrate to using Image Processor module for all functionality. For information on creating Image Processing profiles, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*. To learn how to use the module, see *OpenText Intelligent Capture - Image Processor Guide (ECPCORE-CIP)*.

1. For each existing Image Enhancement step in the process, create an Image Processing profile in Intelligent Capture Designer. To learn more about available filters, see the Image Processor profile documentation in *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)*.
2. Deploy Image Processing profiles to the server.
3. Add the Image Processor step to the process, and:

- Configure module settings to use the appropriate Image Processing profile.
- Remove the Image Enhancement step. It cannot coexist with Image Processor in the same process.
- Update the process to return values such as barcodes.

4. Image Enhancement exposed many filter settings in IA values. If your process made extensive use of this functionality, then you may need to create a Document Type Script to read and dynamically adjust filter parameters.
5. Remove the Auto Annotate step from the process, and:

   - Replace with an Image Processor step or reuse an existing one.
   - Add equivalent annotations to the Image Processing profile. If text annotation use IA values, then use format expressions.
   - If Automatic Annotations used dynamic values in text, then replace the functionality using Document Type scripting.

6. Remove the Image step from the process, and:

   - Replace with an Image Processor step or reuse an existing one.
   - Add the **Rotate** filter to the profile to perform rotation.

   Notes

   - Image Processor module does not convert images to 16-bit or 32-bit multiples. This feature is not relevant for modern image files.
   - Image Processor automatically generates thumbnails.

Key differences between Image Enhancement and Image Processor

1. Image Processor includes many new filters.
2. Binary and color filters are now combined.
3. Barcode detection filters are merged into a single filter.

7.5.10 Migrating to Use Standard Export

This section is targeted towards users that used standard export modules such as File System Export, ApplicationXtender Export, Image Export, Index Export, PDF Export, or Values to XML in the previous versions and want to update to using the profile-based Standard Export 21.4. For information on creating export profiles, see *OpenText Intelligent Capture - Designer Guide (ECPCORE-CPD)* and *OpenText Intelligent Capture - Standard Export Guide (ECPCORE-CXB)* to learn how to use the module.

1. In Intelligent Capture Designer, add one or more export profiles to map to the previous export modules.

- For File System Export, create a **File** export profile command
- For Index Export, create a **CSV** or **Text** export profile command
- For Values to XML, create an **XML** export profile command
- For the Email Export module, create an **Email** export profile command

2. To replace Image Export and PDF Export functionality, create an Image Conversion profile to create an output file with the required settings. Add a **File** export profile command and see the output file.
3. Deploy your export profiles to the server.
4. Remove File System Export, ApplicationXtender Export, Image Export, Index Export, PDF Export, or Values to XML (as applicable) from the process. Replace with Standard Export. Configure the Standard Export module to use the appropriate profiles.

Chapter 8

Modifying, Repairing, and Removing Intelligent Capture

An Intelligent Capture installation can be modified, repaired, or uninstalled.

8.1 Modifying an Intelligent Capture Installation

The current installation of Intelligent Capture can be modified. Modifying the installation lets you install features that are not currently installed and remove features that were installed.

To modify an Intelligent Capture installation:

1. Stop the component you want to modify.
2. Run the setup program and select **Install Products**.
3. Select the component to modify and click **Next**. The **Program Maintenance** window displays.
4. Select the **Modify** option and then click **Next**. The **Custom Setup** window displays. The left pane of the window displays the features of the component. Expand the feature to view its sub-features.
5. Click the down arrow situated before the feature name and select from the options displayed to modify the installation of the selected feature.
6. Click **Next**, **Next**, and then **Install**.

   The installation is modified.

8.2 Repairing an Intelligent Capture Installation

The Intelligent Capture installation repair functionality is useful if you have removed a feature or if the program becomes corrupted.

To repair the Intelligent Capture Server after removing a feature, use the same `Intelligent Capture Server.msi` file used to install the original server. To repair a Client installation after removing selected modules or an entire service pack you must use the same `Intelligent Capture Client.msi` file used to install the original system.

To repair an Intelligent Capture installation:

1. Stop the component you want to repair.
2. Run the setup program and select **Install Products**.

3. Select the component to repair and then click **Next**. The **Program Maintenance** window displays.
4. Select the **Repair** option and then click **Next**. The **Ready to Repair the Program** window displays.
5. Click **Install**.

8.3 Removing Intelligent Capture Components

Installed Intelligent Capture components can be removed. When you remove a component, the entire component is removed from the machine. For instance, removing the client installation removes all the client modules installed on the machine.

To remove Intelligent Capture components:

1. Stop the service for the component you want to remove. For example, stop the Intelligent Capture Server service before removing the Intelligent Capture Server.
2. (When removing the Intelligent Capture Server) From the Intelligent Capture Administrator module, navigate to the **Servers** pane and delete the Intelligent Capture Server to remove.
3. Run the setup program on the machine where you want to remove the component and select **Install Products**.
4. Select the component to remove and click **Next**. The **Program Maintenance** window displays.
5. Select the **Remove** option and click **Next**. The **Remove the Program** window displays.
6. Click **Remove**. The component is removed completely from the machine.

Note: The **InputAccel_Server_admin_group** group created by the Intelligent Capture Server setup program is removed when the Intelligent Capture Server is removed. This group cannot be used after the server is removed.

Chapter 9

Troubleshooting

This section provides information to help you troubleshoot installation problems with Intelligent Capture and its components.

9.1 Installation Failures

When a component fails to install correctly, the setup program performs a rollback operation and returns the machine to the state it was in prior to starting the installation. Troubleshooting this type of installation issue requires examination of setup program log files. However, setup program log files are not generated by default. To generate a log file, you must enable logging when starting the setup program by including a command line parameter of `/l`.

Example 9-1: Enabling logging

Start the client setup program (or any of the other setup programs) by typing the following in a command prompt window:

```
setup.exe /v"/l*v <logfilename>"
```

where

`/v` passes the part of the command line enclosed in quotes to the Microsoft Installer package.

`/l*v` enables verbose logging.

`<logfilename>` is the path and file name to which to write the log data.

This command line starts the setup program and writes detailed information to the specified file. After the installation completes (or fails and rolls back), you can examine the log file to help determine the cause of the problem.

Note: Wait until the setup program closes before opening the log file to ensure that all log entries have been written to the file.

A log file created in this manner is a simple text file that can be opened with any text editor. The log file can become quite large (20 *MB* or more) depending on the particular setup program and the specified logging level.

Setup programs write entries to the log file as events occur. In some cases, one error might lead to another. It is important to find the first error in the chain to properly troubleshoot an issue.

Both errors and non-error information may be written to the log file. A return value of 3 indicates an error or failure entry in the log. You can save time by searching for the string “return value 3”. The following log entry is an example of a failure:

```
Action ended 14:04:40: InstallFinalize. Return value 3.
```

This message in this example is not an actual error, but an indication of where the error occurred. The preceding lines in the log file indicate the problem. Most installation errors are written to the log with a specific error code and, when available, an error message. These errors often provide enough information to enable you to resolve the issue. If not, a setup program log file will help your customer support representative quickly evaluate the problem.

9.1.1 Installation Errors

Errors discussed here occur during installation and do not cause the setup program to perform a rollback operation. Most can be corrected and then the installation completed. “Common Installation Problems” on page 176 lists the most common installation errors.

Table 9-1: Common Installation Problems

Problem	Possible cause / Workaround
While installing any component, the setup program indicates that you have supplied an invalid password when in fact the password is correct.	An authentication problem occurs when the user is logged into a machine without the necessary access rights to query the Windows domain. This happens when both of the following conditions are true: • The user is logged into a local user account while running the setup program. • The credentials causing the authentication failure are domain credentials.
When installing the `IAS` folder to a UNC path, an error is displayed stating that the user account rights for the server has not been set and it may prevent the server from running correctly.	Although supported, installing the `IAS` folder to a UNC path is not recommended. If you do install the `IAS` folder to a UNC path, ensure the following: 1. Run the server using a domain account. 2. Grant the UNC directory for `IAS` folder to have full Windows permissions for that domain account. 3. Ensure that every Intelligent Capture user that accesses and creates processes and batches are granted the Windows permission (use Windows tools) to access the `IAS` folder.

Problem	Possible cause / Workaround
When installing the server, an error message is displayed stating that **DCOM** permissions were not set.	When this error occurs, users can continue with the installation of the server. However, the outcome of this error is that the server is unable to execute scripts written using the CaptureFlow Script Editor. To fix this issue users must run `dcomcnfg` to grant the **InputAccel_Server_admin_group** permissions to activate and execute **DCOM** objects.

9.2 Command Line Installation Failures

Command line installation failures include syntax errors.

9.2.1 Syntax Errors

"Unattended Installations" on page 117 explains how to install Intelligent Capture from command line instructions. When using this method, the command line can become very long due to the number of features and options.

Many command line errors occur because the command line contains syntax errors or incomplete information.

Some properties require their values to be encapsulated in quotes (`" "`).

Example: `setup.exe /s /v"/qn ADDLOCAL="ALL""`

Note that every open quote character must have a matching close quote character. This example shows one quoted parameter correctly nested within another quoted parameter. A common error is to omit or misplace one or more quote marks.

The best way to troubleshoot command line installation issues is to examine the setup program log files, as explained in "Installation Failures" on page 175.

9.2.2 Common Command Line Installation Errors

"Common Installation Problems" on page 177 lists some of the more common errors that customers experience when running setup programs from the command line.

Table 9-2: Common Installation Problems

Problem	Possible cause
Installation does not occur silently—the user interface displays and waits for a response.	A space character was typed between `/v` and the first open quote symbol.

Problem	Possible cause
The message "`Please go to the Control Panel to install and configure system components`" is displayed.	The setup command was not executed from the directory containing the `setup.exe` program.
Windows restarts automatically after setup completes.	If the setup program determined that a restart was necessary to complete the installation, it performs an automatic restart. This behavior can be changed by including one of the following restart options: `/norestart`: Do not restart after setup completes. `/promptrestart`: Prompt the user to restart if necessary. `/forcerestart`: Always restart after setup completes, regardless of whether the setup program determines that a restart is necessary.
Client installation requires 1024 x 768 display resolution.	Regardless of whether you are running modules as applications or as services, and regardless of whether you are installing on a physical machine or in a VMware image, your client machine must have its screen resolution set to a minimum of 1024 x 768. If set to a lower resolution, the setup program will not allow you to proceed.
Installation does not occur.	The command line exceeds the maximum allowable length of 1066 characters. You can verify this problem by observing the Windows Task Manager and noting that the setup program starts and then exits before installation occurs.
Miscellaneous installation errors.	Syntax issues can cause various errors when attempting a command line installation. Note the following rules: • Properties containing spaces must be enclosed in quotation marks that have been escaped with a backslash character (\). Example: `1 INSTALLDIR=\"c:\Program Files \InputAccel\Client\" 2` • Properties containing the reserved characters \, &, |, >, <, and ^ must escape those characters with a caret character (^).

9.3 Third-Party Component Issues

Certain Intelligent Capture client modules rely on third-party components provided by the company that produces the application to which they connect. Two categories of modules have this issue:

- Modules that will not install without the required third-party components
  - ApplicationXtender Export
  - Export for IBM Content Manager

    Note: With the Legacy IBM CM C++ client libraries (for v.8.5 and earlier) (for export to IBM CM v.8.5 (and lower)) option selected.
- Modules that will install, but not run, without the required third-party components
  - Archive Export
  - Documentum Advanced Export
  - FileNet Content Manager Export
  - FileNet Panagon IS/CS Export
  - Global 360 Export
  - Export for IBM Content Manager

    Note: Without the Legacy IBM CM C++ client libraries (for v.8.5 and earlier) (for export to IBM CM v.8.5 (and lower)) option selected.
  - Export for SAP Archive and AP Connect
  - Export for OpenText Content Server

For a list of third-party software requirements for client modules, see the *Release Notes > Module-Specific Requirements*, available on My Support (https://support.opentext.com).

9.4 Post-Installation Issues

This section provides troubleshooting tips for issues that can occur after a successful installation.

9.4.1 Intelligent Capture Database Issues

The Intelligent Capture Database is an optional component that resides in an instance of Microsoft SQL Server. SQL Server must be configured to enable the Intelligent Capture system to connect and communicate with the Intelligent Capture Database. Following are some common problems that can occur.

Table 9-3: Common Intelligent Capture Database-Related Problems

Problem	Possible cause
Intelligent Capture Database setup program cannot create the Intelligent Capture Database.	• SQL Server is not running. On the SQL Server host machine, use the Windows Service Control Manager to locate the SQL Server service and make sure it is started. • Inadequate SQL Server permissions. During Intelligent Capture Database setup, the account specified to create the Intelligent Capture Database must be assigned the `dbcreator` Server Role. Typically, you would enable the `dbcreator` account login and assign it a password within SQL Server and then specify this account to install the Intelligent Capture Database.
Intelligent Capture components cannot connect to SQL Server.	• *TCP/IP* protocol is disabled within SQL Server. Consult the SQL Server documentation for instructions on enabling the TCP/IP protocol. Restart the SQL Server service after changing this setting. • The SQL Server is not listening on the expected port. (The default SQL Server port is 1433. These may have been changed during SQL Server configuration.) Specify the correct port in the connection information during setup.

Problem	Possible cause
Intelligent Capture components cannot log into SQL Server	• When enabling SQL Server Authentication mode, the **User must change password at next login** check box was selected. The first time an Intelligent Capture component attempts to connect to the Intelligent Capture Database, SQL Server attempts to prompt for a password change. Because the component has no user interface to support changing the password, it cannot connect. You must ensure that SQL Server does not prompt for a password change. • SQL Server is using a named instance. When specifying a connection string to the SQL Server, you must include the instance name as follows: <*hostname*>\<*instancename*>
Intelligent Capture components cannot access the Intelligent Capture Database.	• Insufficient access rights. The account specified during installation to connect to these databases must have the database role membership set to public and must have been granted the **Connect**, **Delete**, **Execute**, **Insert**, **Select**, and **Update** permissions. • The Intelligent Capture Database is renamed or the service was stopped. If the database is renamed, all components must be reconfigured to connect to the database using the new name. If the service was stopped, it must be restarted.
Batches from previous versions that contain Documentum Server Export steps cause batch errors when run by Documentum Advanced Export.	Login credentials are not retained when upgrading and must be specified again.

9.4.2 ScaleServer Issues

When Intelligent Capture Servers are configured as a ScaleServer group, client modules must connect to one of the Intelligent Capture Servers in the ScaleServer group by using the machine name of the machine hosting the Intelligent Capture Server. If an *IP* address or the name “localhost” is used in the **Server name** field of the connection string, the connection to the server will fail.

9.4.3 Help Issues

Problem

After configuring the Intelligent Capture system to use a Private Help Server (PHS), for example in situations where a site does not have Internet access, users cannot access Help files.

Solution

Check the Private Help Server URL in the configuration file.

1. To access the configuration file, navigate to `<InstallationDrive>\ProgramData\OpenText\Capture` where *<InstallationDrive>* represents the drive where Intelligent Capture is installed.
2. Using a text editor, open the configuration file.
3. Check the following:
   - The Private Help Server URL uses a root URL that includes the path segments to the actual API endpoint of the GHS/PHS server.
   - The URL specified for the Private Help Server in the configuration file is correct.
   - The transfer protocol is the same as your site's transfer protocol.

Note: For detailed information about the PHS, see *OpenText Help System - Private Help Server Administration Guide (OTHS-AGD)*.

9.4.4 Other Issues

This section explains some common issues that may occur during Intelligent Capture setup.

Table 9-4: Other Problems during Intelligent Capture Setup

Problem	Possible cause
Intelligent Capture Server fails to start	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.

Problem	Possible cause

	Example:
	• Create the *LUA* group using the default Intelligent Capture Server data directory and service instance name:
	`ias64.exe -repair -r C:\IAS -s InputAccel`
	• 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.

Intelligent Capture Server installer appears to stop unexpectedly or stop working when installing with an existing `IAS` folder.	When the Intelligent Capture Server installer is installed with an existing `IAS` folder, it may take a long time to install and the installer may appear to have stopped unexpectedly. This happens if the existing `IAS` folder has a large number of batches and stage files resulting in the installer requiring additional time to update security permissions on the folder.
Intelligent Capture client fails to connect to Intelligent Capture Server	• Intelligent Capture Server service is not running. On the Intelligent Capture Server host machine, use the Windows Service Control Manager to locate the Intelligent Capture Server service and make sure it is started. • Client cannot communicate with server. Verify that the client machines and the Intelligent Capture Server are all configured to communicate on the same port (10099, by default).

Problem	Possible cause
Intelligent Capture client fails to connect to Intelligent Capture Server (continued)	• Client cannot connect to server when running the module as a service using a local machine account, such as Network Service. To successfully connect, you must do one of the following: – Configure the Intelligent Capture Server machine to allow anonymous access. – Run the client module on the same machine as the Intelligent Capture Server. – Configure Intelligent Capture to use Kerberos and set an *SPN* for the Intelligent Capture Server, as explained in "Configuring Intelligent Capture to use Kerberos authentication" on page 21. • The machine name of the Intelligent Capture Server is longer than 15 bytes. Machine names longer than 15 bytes are truncated by NetBIOS software and result in an inability to connect to the Intelligent Capture Server. • Hostname resolution fails. If attempting to connect using a machine name rather than an *IP* address, make sure the name resolves to an IP address by using the command line `ping` or `nslookup` program. • A firewall is blocking access. Make sure the Intelligent Capture Server host machine's firewall is configured to pass incoming network traffic on the required port (10099, by default).
The error "Setup has detected that the SQL Server <*servername*> is not configured properly" occurs during Intelligent Capture Database setup	The SQL Server host machine was renamed after SQL Server was installed. The host name registered within SQL Server must match the host name of the machine. This is a common problem when using VMware to host Intelligent Capture Server. A Microsoft Knowledge Base article provides a *SQL* query that fixes this issue.
Web Services Input does not function	Be sure that the Web Services Hosting service and the Web Services Coordinator service have been started in the Windows Service Control Manager.

9.4.5 Verifying Differences in the Locale, Globalization, and Code Page Settings on the Intelligent Capture Server and Client Machines

1. On the machine where a client module is installed, open the `settings.ini` file.
2. In the [INPUTACCEL] section, add `IAClientDebug=1` to activate the client debug file.
3. Open the `iaclient.log` file (default location: `c:\`). This file contains a section `Begin client locale settings` with all client module settings. Search for the `diff` string. This section lists the server settings that are different from the client module settings.
4. If there are differences in the locale, globalization, and code page settings on the Intelligent Capture Server machine and the client module machine, change the regional settings so that these settings on the Intelligent Capture Server and client machines are identical.

Chapter 10

Appendix—Prerequisite Software Installed by the Intelligent Capture Setup Program

The Intelligent Capture setup program installs prerequisite software if the software is not already installed. The prerequisite software varies depending on the Intelligent Capture component that is installed. This section lists the prerequisite software installed for each Intelligent Capture component.

Note: Depending on the language of the operating system and the presence of *MUI* packs, multiple language versions of some of the prerequisite files are installed on the target machine.

10.1 Prerequisite Software Installed with the Intelligent Capture Server

The following prerequisite software is installed with the Intelligent Capture Server:

- Microsoft Visual Basic for Applications Core
- Microsoft Visual Basic for Applications Core - English
- Microsoft Visual Basic for Applications Security Update

10.2 IIS Roles Enabled with Intelligent Capture Web Components

The following IIS roles are enabled when Intelligent Capture REST Service and Intelligent Capture Web Client are installed:

- .NET Extensibility 4.5
- Application Development
- ASP.NET 4.5 (IIS 8.0 and 8.5 only)
- HTTP Redirection
- IIS Management Script and Tools
- ISAPI Extensions
- ISAPI Filters
- Static Content
- Windows Authentication

Note: If you cancel the installation, any prerequisite IIS roles that have been enabled are not rolled back.

10.3 Prerequisite Software Installed with the Intelligent Capture Client Modules

The following prerequisite software is installed with the client modules:

- Microsoft Visual C++ 2013 RTM Redistributable Package (x86)
- Microsoft Visual Basic for Applications Core
- Microsoft Visual Basic for Applications Core - English
- Microsoft Visual Basic for Applications Security Update
- Microsoft Visual C++ 2017 RTM Redistributable Package (x86)

Note: If you cancel the installation, any prerequisite software that has been installed is not rolled back.

Chapter 11

Appendix—Intelligent Capture Client Modules

"Intelligent Capture Modules" on page 189 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 could experience data loss. See this table for the list of modules that you can safely run as multiple application or service instances.

Table 11-1: 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`	N/A	N/A	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 - .NET Code Module Guide (ECPCORE-CNT)* 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

Chapter 12

Appendix—Client Module Features

This section lists the client modules that can be installed with each feature.

Note: For more information about modules and components that are no longer shipped and legacy modules, see the *Release Notes* (available in My Support (https://support.opentext.com)).

Table 12-1: Client Components Installation Features

Feature name	Installs
Administrator Tools	• Intelligent Capture Administrator • Intelligent Capture Designer, including the following: – New samples and Process Developer – **Extensions for Development Tools** (Advanced Recognition development tools and accessories) • Intelligent Capture Deployment • IA Migrate
Module Server	• Module Server **Note:** The Module Server also requires the following features: – Image Converter If you do not want the Module Server to use the Virtual Printer feature, then the Virtual Printer feature cannot be installed with the Module Server. – Image Processor – Extraction – Advanced OCR/ICR (Advanced Recognition) – General-Use OCR – Western OCR (Advanced Recognition) – Classification – Identification – NuanceOCR – Standard OCR

Feature name	Installs
Operator Tools	• Completion • Identification • ScanPlus • RescanPlus
Standard Unattended Modules	
Input/Output Modules	• Standard Import • ODBC Export • Standard Export • WS Input (Web Services) • WS Output (Web Services)
Utilities	• .NET Code Module • Copy • Multi • Timer
Image Handling Modules	• Image Converter – Virtual Printer: Installs a virtual printer named **InputAccel Virtual Printer**. • Image Processor
Recognition	• Extraction • NuanceOCR • Standard OCR
Enterprise Export Modules	• Archive Export • Documentum Advanced Export • Documentum ApplicationXtender Export • FileNet Content Manager Export • FileNet Panagon IS/CS Export • Global 360 Export • Export for SAP Archive and AP Connect • Export for IBM Content Manager – Legacy IBM CM C++ client libraries (for v.8.5 and below) option • Microsoft SharePoint Export • Export for OpenText Content Server

Feature name	Installs
Extraction Engines	• Advanced OCR/ICR (Advanced Recognition) The Intelligent Capture Asian Language Add-on is required to enable the following languages: – Chinese (Simplified) – Chinese (Traditional) – Chinese (Traditional, Hong Kong) – Japanese – Korean – Thai • Check Reading (Option) • General-Use OCR • Western OCR (Advanced Recognition)
Web Services Components	• WS Coordinator • WS Hosting
Advanced Recognition	• Classification • Collector • Production Auto-Learning Supervisor

Chapter 13

Appendix—Localized Languages

Intelligent Capture is localized into the following languages. These languages for Intelligent Capture are used to control the user interface (UI) language displayed to the user. The UI language that Intelligent Capture components use is independent of the languages that can be part of a batch, task, or page.

Table 13-1: Localized Languages Intelligent Capture

Language	Windows code page	Language code	Locale ID (LCID)
Chinese (Simplified)	936	zh-cn	2052
English (United States)	1252	en-us	1033
French (France)	1252	fr-fr	1036
German (Germany)	1252	de-de	1031
Italian (Italy)	1252	it-it	1040
Japanese	932	ja-jp	1041
Korean	949	ko-kr	1042
Portuguese (Brazil)	1252	pt-br	1046
Russian (Russian Federation)	1251	ru-ru	1049
Spanish (Spain)	1252	es-es	1034

Chapter 14

Appendix—Intelligent Capture Ports

"Ports Used by Intelligent Capture Components" on page 203 lists the ports used by the various components of the Intelligent Capture application.

Table 14-1: Ports Used by Intelligent Capture Components

Port number	Used for
1433	The SQL Server default port.
12007	The *TCP* port that enables Web Services Coordinator to receive connections from the WS Input module.
10099	The default TCP port that enables Intelligent Capture client modules to communicate with the Intelligent Capture Servers. This can be changed during installation and may be different for each Intelligent Capture Server in a side-by-side installation.
443/80	The default HTTPS/HTTP ports for Intelligent Capture REST Service and Intelligent Capture Web Client Web site.
50000	The TCP port that enables the Module Server (`CPMODSRV.exe`) to accept incoming requests.
50010 - 50999	The TCP ports that enables hosted modules (`Emc.Captiva.LccClientHost.exe`) to accept incoming requests.

Chapter 15

Appendix—Using the Database Manager Utility

By default, the database setup program creates an external, SQL Server-hosted Intelligent Capture Database. If customers choose not to install an Intelligent Capture Database, then running the Intelligent Capture Server setup program creates a file-based, internal database. You may be required to update the installed external or internal database or create the database for various reasons.

Use the Database Manager utility in the following circumstances:

- You disabled the default setting to create the Intelligent Capture Database when running the Intelligent Capture Database setup program.
- You have been directed by support personnel to update your Intelligent Capture Database with scripts provided to you.

15.1 Creating or Updating the External or Internal Database

1. From the **Start** menu, click **Programs** > **OpenText Intelligent Capture** > **Tools (Standard)** > **Database Manager.**

   You must run the Database Manager utility as an Administrator.

2. From the **Database type**, select **Microsoft SQL Server** to create a *SQL* Server-hosted database or **Internal Database** to create a file-based database.

3. Specify the following:

   - For **Internal Database**

     – **Data File Folder**: The location where the Database Manager utility creates predefined data files.

     – **Path to DB Scripts**: The location of the *XML* files, sub-folders and other scripts that contain the schema and data definitions. The folder selected must contain a sub-folder named `XML` which contains a file named `IADBFiles.xml`. This file is used by the Database Manager to determine the database schema and data objects to include in the database.

   - For **Microsoft SQL Server**:

     – **Database Server**: Type the name of the SQL Server on which you want to create the Intelligent Capture Database. If your SQL Server is using a named instance, append the instance name in this field, separated by a backslash (“\”).

- **Database Name**: Type the name of the database that you want to create.
- **User Account and User Password**: Type the login credentials for the SQL Server. The account specified must have the `dbcreator` role.
- **Install Mode**: Database + Schema + Data, Database only, Schema + Data
- In the **Path to DBScripts** field, type the root path to the `list.txt` file, which specifies all of the *SQL* scripts that need to be executed. Alternatively, click **Browse** to navigate to `list.txt`. The default installation scripts are installed in `C:\Program Files\InputAccel\Databases\DBScripts`. The top-level `lists.txt` file also can be found here.

4. Select the **Upgrade database** check box to update the Intelligent Capture Database for a patch or upgrade. If you are creating the database for the first time, clear the check box.

   Note: The internal database cannot be upgraded through the Database Manager utility; it can only be upgraded through an Intelligent Capture Server upgrade.

5. Click **OK** to save your settings, run the utility, and exit.

15.2 Running Database Manager in Silent Mode

The Database Manager utility can be used to silently create the external, *SQL* Server-hosted Intelligent Capture Database or the file-based, internal database. This utility is run from a command prompt window.

You must run the Database Manager utility as an Administrator.

Database Manager utility syntax to create a SQL Server-hosted database:

```
IADBManager -silent -mssql -all -dbserver <server> -dbname <database
name> -username <user name> -password <password> -dbscripts <path>
 -upgrade
```

Table 15-1: Explanation of Command Line Arguments used to Install the Intelligent Capture Database

Command line argument	Description
`IADBManager`	Runs the Database Manager utility.
`-silent`	Runs the Database Manager utility in silent mode.
`-mssql`	Create a SQL Server-hosted Intelligent Capture Database.

Command line argument	Description
One of the following: • `-all` • `-dbonly` • `-schema`	Installation mode: • `-all`: Creates the Intelligent Capture Database, the schema, and data • `-dbonly`: Creates the Intelligent Capture Database • `-schema`: Creates the schema and data
`-dbserver <server>`	Name of the SQL Database Server.
`-dbname <database name>`	Name of the database that you want to create and populate with database scripts.
`-username <user name>`	User name for the SQL Server login screen, the database account, and the scripts to be executed. The account specified must have the `dbcreator` role.
`-password <password>`	Password for the specified user name.
`dbscripts <path>`	Root path to database schema *XML* files.
`-upgrade`	Updates the Intelligent Capture Database for a patch or upgrade.

Database Manager utility syntax to create a file-based, internal database:

Run the following command on the machine that hosts the Intelligent Capture Server:

```
IADBManager -silent -nodb -nodbpath <path> -dbscripts <path>
```

Table 15-2: Explanation of Command Line Arguments used to Install the File-based Database

Command line argument	Description
`IADBManager`	Runs the Database Manager utility.
`-silent`	Runs the Database Manager utility in silent mode.
`-nodb`	Create a file-based, internal database on the Intelligent Capture Server machine.
`-nodbpath <path>`	Path to the internal database data files.
`-dbscripts <path>`	Root path to database schema *XML* files (`c:\Program Files\InputAccel\Databases\DBScripts` by default)

15.3 Database Manager Command Line Examples

Example 15-1:

The following is a sample command line that creates a *SQL* database "IADB". It specifies a user name of "dbcreator" and a password of "passwd". It installs the database, schema, and database data:

```
IADBManager -silent -all -mssql -username dbcreator -password
passwd -dbserver localhost -dbname IADB -dbscripts "C:\Program
Files\InputAccel\DBScripts"
```

Example 15-2:

The following is a sample command line that creates a file-based, internal database.

```
IADBManager -silent -nodb -nodbpath "C:\IAS" -dbscripts "
C:\Program Files\InputAccel\Server\Server\DBScripts"
```

15.4 Manually Creating the Information Extraction (IE) Database

Like the Intelligent Capture Database utility, a command line utility enables you to manually create the Information Extraction (IE) database (default name: `IEDB`). Use this utility if you installed the database files without creating the database or if you need to create a second IE database. This command can be run only after the Intelligent Capture Database (default name: `ICDB`) has already been created. You can create the `IEDB` only from the command line; a GUI option is not available.

The command utility, `ConfigureIEE.exe`, creates an IE database on the same server where the Intelligent Capture Database is installed. Running this command overwrites any previous `IEDB` configurations in the Intelligent Capture Database, but it will not modify the database that it is replacing, only the database configuration.

The utility takes two sets of connection values (server, user, and so on):

- One for creating the IE database
- One that Intelligent Capture clients will use to connect to the IE database

Note: The IEDB command line utility can be used only when the ICDB is an external SQL Server database, it cannot be used when Intelligent Capture uses an internal database.

To manually create the IE database:

1. Create the Intelligent Capture Database.
2. From the command prompt, run `ConfigureIEE.exe`.
3. Use the following command line arguments to configure the IE database:

Table 15-3: Command line arguments for the IE database

Argument	Definition
`-server:<server>`	The server name or IP address and instance used to create the IE database. For example, `db.example.com\<SQLINSTANCE>`.
`-user:<username>`	The user name for the connection used to create the IE database.
`-password:<password>`	The password for the connection used to create the IE database.
`-integratedSecurity:true`	Set this argument instead of using user name and password to connect as the currently logged-in user when creating the IE database.
`-icDbName:<db-name>`	The name of the Intelligent Capture Database, which must be located in the given server/instance.
`-ieeIntegratedSecurity:true`	Set this argument to configure clients to connect to the IE database using integrated security.
`-ieePassword:<string>`	The password that clients will use to connect to the IE database.
`-ieePort:<number>`	The port that clients will use to connect to the IE database. If omitted, 0 is used to indicate the SQL Server default port.
`-ieeServer:<name>`	The name or IP address of the database server that clients will use to connect to the IE database.
`-ieeUser:<name>`	The user name that clients will use to connect to the IE database.

15.5 Information Extraction Database Command Line Examples

Example 15-3:

This example creates the Information Extraction database (name: `IEDB`) using explicit credentials for both creating the database and accessing it in production:

```
ConfigureIEE -server:localhost -user:dbadmin
 -password:adminpasswd -icdbname:ICDB -ieedbname:IEDB
 -ieeServer:db.example.com -ieeUser:ieeuser
 -ieePassword:ieepasswd
```

Example 15-4:

This example creates the Information Extraction database (name: `IEDB`) using integrated security for both creating the database and accessing it in production:

```
ConfigureIEE -server:localhost -integratedSecurity:true
 -icdbname:ICDB -ieedbname:IEDB -ieeServer:db.example.com
 -ieeIntegratedSecurity:true
```

Example 15-5:

This example uses explicit credentials to create the Information Extraction database (name: `IEDB`) but integrated security for clients to connect to the Information Extraction database:

```
ConfigureIEE -server:localhost -user:dbadmin
 -password:adminpasswd -icdbname:ICDB -ieedbname:IEDB
 -ieeIntegratedSecurity:true
```

15.6 Installing Information Extraction from the Command Line

You can install Information Extraction from the command line instead of using the installation wizard. The installer is named `iee-cloud-setup.msi`.

To install Information Extraction from the command line:

1. Ensure that you are logged in as an administrator user.
2. Navigate to the **Clients** directory of the installation media.
3. Type

   ```
   msiexec.exe /i "iee-cloud-setup.msi" /QN
   ```

Chapter 16

Appendix—Command Line Arguments for Installing Intelligent Capture

Intelligent Capture supports a subset of the standard InstallShield and Windows Installer command line arguments. All command line examples must be typed on one command line which may wrap to multiple lines in a command prompt window. The Windows Installer switches and Intelligent Capture features and properties are case sensitive. Use the examples as they are shown.

16.1 Supported InstallShield Switches

Table 16-1: Supported InstallShield Switches

Switch	Description
`/v`	Passes the MSI parameter switches from the InstallShield setup command line to MSI.
`/x`	Removes a product.
`/clone_wait`	Prevents the setup process from ending before the installation is finished.

For more information on the supported InstallShield switches, search the Internet for "Setup.exe and Update.exe command line Parameters."

16.2 Supported MSI Switches

Intelligent Capture supports the Windows Installer version 4.5 command line parameters that enable you to install, display, restart, log information, update, and repair Intelligent Capture installations. `Msiexec.exe` is the Windows Installer executable program that interprets packages and installs products.

To view a list of supported MSI switch command line arguments:

1. Open a command prompt.
2. Type

   ```
   msiexec.exe /?
   ```

16.3 Supported Windows Installer Properties

The ADDLOCAL Installer property is the most commonly used property. It locally installs a list of features, that are delimited by commas.

Tip: For additional information regarding Installer properties, search the Internet for "MSDN Library Windows Installer Property Reference".

16.4 Intelligent Capture Installer Properties and Feature Names

To perform a silent installation, use InstallShield and MSI command line parameters in conjunction with the Intelligent Capture feature names and properties. You perform silent installations on the appropriate machines to create the Intelligent Capture Databases, Intelligent Capture Server, Web components, and Client Components.

16.4.1 Intelligent Capture Database Installer Properties

You can install the Intelligent Capture Database in unattended mode using command line arguments.

Example: `setup.exe /s /v"/qn <property=value> /promptrestart"`

where "property=value" is a list of installer properties to be passed into the setup program.

At a minimum you must specify the ADDLOCAL property. For example:

```
setup.exe /s /v"/qn ADDLOCAL="ALL" /promptrestart"
```

The Database installer runs silently only when the CREATE_DATABASE installer property is set to a value of 1. This is the default value. In addition, the following installer properties must be specified:

- SQL Server name
- SQL Server port
- SQL Server user name
- SQL Server password
- Database name

The Database Manager utility must not be run in interactive mode during an unattended (or silent) installation.

The SQL Server port has a default value of 1433. This means that if this installer property is not passed in, 1433 is used.

Note: You cannot validate SQL Server during a silent installation. You are responsible to pass the correct information to the installer.

"Supported Intelligent Capture Database and Information Extraction Database Installer Properties" on page 215 lists the installer properties that can be specified when installing or upgrading the Intelligent Capture Database and Information Extraction database:

Table 16-2: Supported Intelligent Capture Database and Information Extraction Database Installer Properties

Installer property	Value	Required for upgrade	Description
ADDLOCAL	*<Features to install>*	-	A comma-delimited list of the features to install. Since there is only one feature in this component to install, you should specify ALL.
CREATE_DATABASE	0/1/2	Yes	Specify one of the following values: • 0: Do not install the Intelligent Capture Database. Only the database scripts are installed. • 1: Install the Intelligent Capture Database. • 2: Upgrade the Intelligent Capture Database. If this property is not specified, a default value of 1 is used.
DB_SERVER	*<Hostname>*	Yes	Hostname of the SQL Server. You can use (local) or localhost if you want to use the locally installed SQL Server.
IE_DB_SERVER	*<Hostname>*	Yes	Hostname of the SQL Server to which Information Extraction customers will connect.

Installer property	Value	Required for upgrade	Description
DB_PORT	*<TCP port number>*	-	The *TCP* port on which the SQL Server listens for connections. The default value is 1433.
IE_DB_PORT	*<TCP port number>*	-	The TCP port on which the SQL Server listens for connections. The default value is 1433.
DB_NAME	*<Database name>*	-	The name of the *SQL* database. The database name has the following restrictions: • It can have a maximum of 122 characters. • It can contain only the characters 0–9, A–Z, an underscore, $, #, @ and must begin with a number, a letter, or an underscore. A default value "IADB" is used if this property is not specified.

Installer property	Value	Required for upgrade	Description
IE_DB_NAME	*<Database name>*	-	The name of the Information Extraction SQL database. The database name has the following restrictions: • It can have a maximum of 122 characters. • It can contain only the characters 0–9, A–Z, an underscore, $, #, @ and must begin with a number, a letter, or an underscore. A default value "IEDB" is used if this property is not specified.
DB_USER	*<SQL user name>*	Yes	The name of the SQL Server user name to connect to SQL Server.
IE_DB_USER	*<SQL user name>*	Yes	The name of the SQL Server user name that Information Extraction clients will use to connect to SQL Server.
DB_PASS	*<SQL password>*	Yes	The password for the SQL Server that the user specified in the DB_USER property.
IE_DB_PASS	*<SQL password>*	Yes	The password for the SQL Server that the user specified in the IE_DB_USER property.

Installer property	Value	Required for upgrade	Description
INSTALLDIR	*<Path>*	-	The destination directory for the database application files. A default value of `%ProgramFiles%\InputAccel\Database` is used when this property is not specified.
WINDOWS_AUTHENTICATION	Boolean	-	• 0: (Default) SQL Server authentication is used. DB_USER and DB_PASS are required. • 1: Windows authentication is used. DB_USER and DB_PASS are ignored.
IE_WINDOWS_AUTHENTICATION	Boolean	-	• 0: (Default) SQL Server authentication is used. IE_DB_USER and IE_DB_PASS are required. • 1: Windows authentication is used. IE_DB_USER and IE_DB_PASS are ignored.

16.4.1.1 Intelligent Capture Database Installer Command Line Examples

Example 16-1: Install files and database scripts into the default installation directory

This example installs the `Database Manager`, `CreateDbConsole.exe`, and the database scripts into the default installation directory. The `Database Manager` is executed to install the Intelligent Capture Database on the locally installed SQL Server which listens for connections on the default port of 1433. The default Intelligent Capture Database name is used.

```
setup.exe /s /v"/qn ADDLOCAL=ALL DB_SERVER="(local)" DB_
USER="dbcreator" DB_PASS="password" /promptrestart"
```

Example 16-2: Install files and database scripts into a specified directory

This example installs `Database Manager` and the database scripts into the directory specified by `INSTALLDIR`. `IADBManager.exe` is executed to install the Intelligent Capture Database to the remote SQL Server named "CORP-SQL" which listens for connections on the default port of 1433. The default Intelligent Capture Database name is used.

```
setup.exe /s /v"/qn ADDLOCAL=ALL INSTALLDIR=\"c:\Program Files\
InputAccel\Databases\" CREATE_DATABASE=1 DB_SERVER=CORP-SQL DB_
USER=dbcreator DB_PASS=password /promptrestart"
```

Example 16-3: Upgrade the Intelligent Capture Database using the minimum parameters

```
setup.exe /s /v" /qn CREATE_DATABASE=2 DB_SERVER= "(local)" DB_
USER="dbcreator" DB_PASS="password""
```

16.4.2 Intelligent Capture Server Components Installer Properties

You can install the Intelligent Capture Server in unattended mode using command line arguments.

Example: `setup.exe /s /v"/qn property=<value> /promptrestart"`

where "`property=<value>`" is a list of installer properties to be passed into the setup program.

At a minimum, you must specify the `ADDLOCAL` and `IA_SERVICES_RUNAS_LOCAL_SYSTEM` properties. For example:

```
setup.exe /s /v"/qn ADDLOCAL="ALL" IA_SERVICES_RUNAS_LOCAL_SYSTEM="1"
 /promptrestart"
```

Notes

- The root directories for each Intelligent Capture Server must be specified when more than one instance is being installed. Each root directory must be unique and should be on its own hard disk drive. The properties for these instances are `IAS1_ROOT_DIR`, `IAS2_ROOT_DIR`, `IAS3_ROOT_DIR`, and so forth.
- The character limit on setup command line length is 1066 characters.

"Supported Intelligent Capture Server Installer Properties" on page 220 lists the installer properties that can be specified when installing or upgrading the Intelligent Capture Server.

Table 16-3: Supported Intelligent Capture Server Installer Properties

Installer property	Value	Required for upgrade	Description
ADDLOCAL	*<Features to install>*	-	Features to install. The following features are available. They are mandatory. • IASERVER: Intelligent Capture Server • IA_COMMON: Installs common components.
INSTALLDIR	*<Path>*	-	The destination directory for the Server application files. A default value of %ProgramFiles%\InputAccel\Server is used when this property is not specified.
SERVER_INSTANCES	1-8	-	The number of Intelligent Capture Server instances to install. A default value of 1 is used when this property is not specified.
INSTALLATION_TYPE	Specify only if an Intelligent Capture Database is not and will not be installed	-	Available feature: • NODB: The Intelligent Capture Database is not installed. The Intelligent Capture Server installer will install a file-based, internal database.

Installer property	Value	Required for upgrade	Description
REGISTER_DATABASE	0/1	-	• 0: Do not perform DAL registration for the Intelligent Capture Database. • 1: Perform DAL registration for the Intelligent Capture Database. A default value of 1 is used when this property is not specified.
DB_SERVER	*<Hostname>*	Yes, if the previous installation included an external database	Hostname or machine name of the SQL Server. You can use (local) or localhost if you want to use the locally installed SQL Server.
DB_PORT	*<TCP port>*	-	The *TCP* port number to use to connect to the SQL Server. A default value of 1433 is used when this property is not specified.
DB_NAME	*<Database name>*	-	The name of the Intelligent Capture Database. A default value of "IADB" is used if this property is not specified.
DB_USER	*<SQL user name>*	Yes, if the previous installation included an external database	The name of the SQL Server user name required to connect to the SQL Server.
DB_PASS	*<SQL password>*	Yes, if the previous installation included an external database	The password of the SQL Server user specified in the DB_USER property.

Installer property	Value	Required for upgrade	Description
WINDOWS_AUTHENTICATION	Boolean	-	• 0 (Default) SQL Server authentication is used. DB_USER and DB_PASS are required. • 1 Windows authentication is used. DB_USER and DB_PASS are ignored.
AC_MACHINE_USER_NAME	*<Username>*	-	The user account specified as the "Run-as" user for Intelligent Capture Administrator. This property is only valid when the Intelligent Capture Server is installed on machines that are members of a Windows domain.
AC_MACHINE_DOMAIN_NAME	*<Domain name>*	-	The domain name of the user account specified as the "Run-as" user for Intelligent Capture Administrator. This property is only valid when the Intelligent Capture Server is installed on machines that are members of a Windows domain.

Installer property	Value	Required for upgrade	Description
CONFIGURE_WINDOWS_FIREWALL	0/1	-	This property is only valid when the Microsoft Windows Firewall is running and enabled. • 0: Do not make configuration changes to the Windows Firewall. • 1: Allow setup to configure the Windows Firewall. This is the default setting when the property is not passed in.
IA_SERVICES_AUTOSTART	0/1	-	Automatically starts the Intelligent Capture Server service for the first instance when Windows starts. • 0: Manual. Do not start automatically. • 1: Automatically start the Intelligent Capture Server service for the first instance when Windows starts. The default value is 1 unless otherwise specified.

Installer property	Value	Required for upgrade	Description
`IAS<#>_ROOT_DIR` where <#> is a number from 1 through 8. Example: IAS1_ROOT_DIR	*<Path>*	Yes, if upgrading more than one instance of the server on the same machine	The destination directory for the root directory used by the Intelligent Capture Server instance that is determined by `<#>`. You can have instances from 1 through 8. A default path of *<WINDRIVE>*\IAS is used when this property is not specified. For example, the path is `C:\IAS` when Windows is installed on the C: drive. **Caution** The path length must not be greater than 109 characters and cannot be the same as the root directory for any other Intelligent Capture Server instance.

Installer property	Value	Required for upgrade	Description
USE_IN_CLUSTER	0/1	-	If this property is defined, the Intelligent Capture Server will be configured for use in a cluster. Do not define this property if you do not want to use Intelligent Capture Server in a cluster. • 0: The Intelligent Capture Server will not be configured for use in a cluster. This is the default value when the property is not specified. • 1: The Intelligent Capture Server will be configured for use in a cluster. The *IP* address for each Intelligent Capture Server instance being installed must be specified when the value of this property is 1.
IAS<#>_IP_ADDR where <#> is a number from 1 through 8. Example: IAS1_IP_ADDR	*<IP address>*	-	The IP address that the specified instance (determined by <#>) of Intelligent Capture Server listens to for network connections. This parameter should only be used when the property USE_IN_CLUSTER is defined.

Installer property	Value	Required for upgrade	Description
IAS<#>_IP_ADDR_V6 where <#> is a number from 1 through 8. Example: IAS1_IP_ADDR	*<IP address>*	-	The *IP* address that the specified instance (determined by <#>) of Intelligent Capture Server listens to for network connections. This parameter should only be used when the property USE_IN_CLUSTER is defined.
IAS<#>_TCP_PORT where <#> is a number from 1 through 8. Example: IAS1_TCP_PORT	*<TCP port>*	-	The specified Intelligent Capture Server instance (determined by <#>) listens to the specified *TCP* port number. The default value is 10099 when this value is not specified.
IA_SERVICES_RUNAS_LOCAL_SYSTEM	1/2	Yes	• 1: The Intelligent Capture Server service runs using the **Local System** account. • 2: The Intelligent Capture Server service runs without using the **Local System** account. When this option is selected, you must specify a user name and password.

Installer property	Value	Required for upgrade	Description
IA_SERVICES_RUNAS_USER_ACCT	*<Domain\Username>*	-	The Intelligent Capture Server service uses this account when running. When specifying a local account, use a ".\" (without quotes) in front of the user name. When specifying a domain account, use `domain\username`. This option is only used when the installer property IA_SERVICES_RUNAS_LOCAL_SYSTEM is passed in with a value of 2 indicating that the installer uses a specific user account and not the built-in local system account.
IA_SERVICES_RUNAS_PSWD	*<Password>*	-	The Intelligent Capture Intelligent CaptureServer service uses this password with the user account specified for running this service. This option is only used when the installer property IA_SERVICES_RUNAS_LOCAL_SYSTEM is passed in with a value of 2 indicating that the installer uses a specific user account and not the built-in local system account.

16.4.2.1 Intelligent Capture Server Installer Command Line Examples

Example 16-4: Install one instance of the Intelligent Capture Server into the directory specified by INSTALLDIR

The service is installed and runs under the built-in Local System account. It does not configure the Windows Firewall (if it is installed and running). The installer performs DAL registration against the Intelligent Capture Database on the SQL Server installed on the same machine, which listens for connections on the default port of 1433. The system automatically restarts if a reboot is required. Because DB_NAME is not specified, the IADB database is used.

```
setup.exe /s /v"/qn ADDLOCAL="ALL" INSTALLDIR=\"c:\Program Files\
InputAccel\Server\" IA_SERVICES_RUNAS_LOCAL_SYSTEM=1 CONFIGURE_
WINDOWS_FIREWALL=0 DB_SERVER="(local)" DB_USER="dbcreator" DB_
PASS="password""
```

Example 16-5: Install one instance of the Intelligent Capture Server into the directory specified by INSTALLDIR

The service is installed and runs under the built-in Local System account. It does not configure the Windows Firewall (if it is installed and running). The installer installs a file-based, internal database.

```
setup.exe /s /v"/qn INSTALLATION_TYPE="NODB" ADDLOCAL="ALL"
INSTALLDIR=\"c:\Program Files\InputAccel\Server\" IA_SERVICES_
RUNAS_LOCAL_SYSTEM=1 CONFIGURE_WINDOWS_FIREWALL=0"
```

Example 16-6: Install eight instances of the Intelligent Capture Server into the directory specified by INSTALLDIR

All eight instances of the Intelligent Capture service use the local Administrator user account (which has a password of "password") as the "run-as" credentials. The root directory for each Intelligent Capture Server instance is specified by the properties `IAS<n>_ROOT_DIR`, where <*n*> is the number of the specific instance. The *TCP* port used by each Intelligent Capture Server instance is specified by the properties `IAS<n>_TCP_PORT`, where <*n*> is the number of the specific instance. The installer performs DAL registration against the Intelligent Capture Database on the SQL Server installed on a different machine ("CORP-SQL"), which listens for connections on the NON-default port of 3999. The NON-default Intelligent Capture Database name is "CORP_IADB". The system automatically restarts if a reboot is required.

```
setup.exe /s /v"/qn ADDLOCAL="ALL" INSTALLDIR=\"c:\Program Files\
InputAccel\Server\" SERVER_INSTANCES=8 IAS1_ROOT_DIR=
\"C:\IADataFiles\" IAS2_ROOT_DIR=\"E:\IADataFiles\" IAS3_ROOT_
DIR=\"F:\IADataFiles\" IAS4_ROOT_DIR=\"G:\IADataFiles\" IAS5_
ROOT_DIR=\"H:\IADataFiles\" IAS6_ROOT_DIR=\"I:\IADataFiles\"
```

```
IAS7_ROOT_DIR=\"J:\IADataFiles\" IAS8_ROOT_DIR=\"K:\IADataFiles\"
IAS1_TCP_PORT=10099 IAS2_TCP_PORT=10100 IAS3_TCP_PORT=10101 IAS4_
TCP_PORT=10102 IAS5_TCP_PORT=10103 IAS6_TCP_PORT=10104 IAS7_TCP_
PORT=10105 IAS8_TCP_PORT=10106 IA_SERVICES_RUNAS_LOCAL_SYSTEM=2
IA_SERVICES_RUNAS_USER_ACCT=".\Administrator" IA_SERVICES_RUNAS_
PSWD="password" DB_SERVER="CORP-SQL" DB_PORT=3999 DB_NAME="CORP_
IADB" DB_USER="dbcreator" DB_PASS="password""
```

Example 16-7: Upgrade the Intelligent Capture Server using the minimum required parameters

```
setup.exe /s /v"/qn IA_SERVICES_RUNAS_LOCAL_SYSTEM=1 DB_SERVER=
"(local)" DB_USER="dbcreator" DB_PASS="password" "
```

16.4.3 Intelligent Capture Web Components Installer Properties

You can install Intelligent Capture Web components in unattended mode using command line arguments.

Example: `setup.exe /s /v"/qn property=<value> /promptrestart"`

where "`property=<value>`" is a list of installer properties to be passed into the setup program.

"Supported Intelligent Capture Web Component Installer Properties" on page 230 lists the installer properties that can be specified when installing or upgrading the Intelligent Capture web components:

Table 16-4: Supported Intelligent Capture Web Component Installer Properties

Installer property	Value	Required for upgrade	Description
ADDLOCAL	*<Features to install>*	-	This is a comma-delimited list of the features to install. The following features are available for installation: • COMMON: Installs common components. • CWC_SITE: As of Intelligent Capture 7.7, installs both Intelligent Capture Web Client and Intelligent Capture REST Service on the same machine. • CRS_DCA_JOINT : For Intelligent Capture 7.6 and earlier, installs both Intelligent Capture Web Client and Intelligent Capture REST Service on the same machine. **Note:** After performing a command line installation of the Intelligent Capture REST Service or Intelligent Capture Web Client, you must configure their settings. For more information, see "Installing Intelligent Capture Web

Installer property	Value	Required for upgrade	Description
			Client and Intelligent Capture REST Service" on page 94.
CAPWEBFILESDIR	*<Path>*	-	Sets the path for either the Intelligent Capture REST Service only or both the Intelligent Capture REST Service and Intelligent Capture Web Client on the same machine. The default value is: `C:\inetpub\captiva`
CRSDCA_WEB_SITE_DESCRIPTION	*<Website description>*	-	The name of both the Intelligent Capture REST Service and Intelligent Capture Web Client Web site. The default value is: `Intelligent Capture Capture Web Client (CWC) and REST Service`
CRSDCA_WEB_SITE_IP_ADDRESS	*<IP address>*	-	The IP address of both the Intelligent Capture REST Service and Intelligent Capture Web Client. The default value is: `*` `*` (asterisk) means `All Unassigned`.

Installer property	Value	Required for upgrade	Description
CRSDCA_WEB_SITE_STARTUP_STATE	0/1	-	Valid values are: • 0: (Default) Do not make the Intelligent Capture REST Service and Intelligent Capture Web Client online after installation. • 1: Make the Intelligent Capture REST Service and Intelligent Capture Web Client online after installation.
CRSDCA_WEB_SITE_TCP_PORT	*<TCP port number>*	-	The listening*TCP* port of both the Intelligent Capture REST Service and Intelligent Capture Web Client Web site. The default is 80.
MODULE_SERVER_DATA_FOLDER	*<Path>*	-	This folder contains temporary image capture files and other state information as well as a shared configuration file. See **Capture Web Client shared data folder**.

Installer property	Value	Required for upgrade	Description
SAASPUBLICURL	*<URL>*	-	This value sets Intelligent Capture and REST Service's **Application Settings** > **SaaSPublicUrl**. Specify the URL for users to use to call Capture Web Client in the following format: `[http|https]://` *`<servername>`*`:`*`<port>`* where • *<servername>* is the server name or its IP address • *<port>* is the port number For more information, see Capture Web Client Public URL.

16.4.3.1 Intelligent Capture Web Components Installer Command Line Example

Example 16-8: Install Intelligent Capture Web Client and Intelligent Capture REST Service

```
1 setup.exe /s /v"/qn ADDLOCAL=COMMON,CWC_SITE
2 CAPWEBFILESDIR=c:\inetpub\captiva\test
3 CRSDCA_WEB_SITE_TCP_PORT=86 CRSDCA_WEB_SITE_STARTUP_STATE=1
4 CRSDCA_WEB_SITE_DESCRIPTION=testing"
```

16.4.4 Client Components Installer Properties

You can install the client components in unattended mode using command line arguments.

Example 16-9: Unattended mode installation

```
setup.exe /s /v"/qn property=value /promptrestart"
```

where *<property=value>* is a list of installer properties to be passed into the setup program.

At a minimum, you must specify the ADDLOCAL=ALL and IA_SERVICES_RUNAS_NAMED_ACCT property. For example:

```
1 setup.exe /s /v"/qn ADDLOCAL="ALL"
2 IA_SERVICES_RUNAS_NAMED_ACCT=0 /promptrestart"
```

Note: Installing Documentum Advanced Export in unattended or silent mode does not check that the required Documentum software has been installed.

"Supported Client Components Installer Properties" on page 234 lists the installer properties that can be specified when installing the Intelligent Capture client components:

Table 16-5: Supported Client Components Installer Properties

Installer property	Value	Description
ABBYY_DROP	0/1	• 0: Keep the East Euro / APAC OCR module. • 1: Uninstall the East Euro / APAC OCR module.
ADDLOCAL	*<Features to install>*	This is a comma-delimited list of the features to install. See features and components for a list of features.
CONFIGURE_WINDOWS_FIREWALL	0/1	This property is only valid when the Microsoft Windows Firewall is running and enabled. • 0: Do not make configuration changes to the Windows Firewall. • 1: Allow setup to configure the Windows Firewall. This is the default setting when the property is not passed in.

Installer property	Value	Description
IASERVERNAME	*<Hostname or IP address>*	The host name or *IP* address of the Intelligent Capture Server that the Intelligent Capture client services connect to. **Note:** Some Intelligent Capture client modules will not start if this property is not specified during the silent installation.
IASERVERPORT	*<TCP port number>*	The *TCP* port number of the Intelligent Capture Server that the Intelligent Capture client services connect to. The default value is 10099 unless otherwise specified. This value must be a number from 1 to 65535.
IA_SERVICES_AUTOSTART	0/1	• 0: Intelligent Capture client services will not be set to start when Windows start. • 1: All Intelligent Capture client services will be set to start when Windows start. A default value of 0 is used when this property is not specified.

Installer property	Value	Description
IA_SERVICES_RUNAS_NAMED_ACCT	0/1	• 0: All Intelligent Capture client services run using the **Network Service** account. • 1: All Intelligent Capture client services not run using the **Network Service** account. When this option is selected, you must specify a user name and password. The properties IA_SERVICES_RUNAS_USER_ACCT and IA_SERVICES_RUNAS_PSWD must be specified when the value 1 is passed in. A default value of 1 is used when this property is not specified.
IA_SERVICES_RUNAS_PSWD	*<Password>*	All Intelligent Capture client services use this password with the user account specified for running the services. This option is only used when the services are set to "run as" the user account and not the **Network Service** account.
IA_SERVICES_RUNAS_USER_ACCT	*<Domain\Username>*	All Intelligent Capture client services use this account to run the services. When specifying a local account, use a ".\" (without quotes) in front of the user name. When specifying a domain account, use domain\username. This option is only used when the services are set to "run as" the user account and not the **Network Service** account.

Installer property	Value	Description
IA_SVCS_CONFIG_RESET	"" (Empty string) / Non-empty value	This property is valid during an upgrade only. An empty string (the default value for this property) does not reset settings of the previously installed services. A non-empty value resets all the settings (excluding command line arguments) of the previously installed services to the default values.
IA_SVCS_RUNAS_USER_KEEP	"" (Empty string) / Non-empty value	This property is valid during an upgrade only. A non-empty value (the default value for this property) specifies that the previously installed services which use built-in accounts (NT AUTHORITY/NetworkService, NT AUTHORITY/LocalService, or LocalSystem) will keep using built-in credentials after upgrade. If an empty string is set, then such services will use credentials specified in the properties: IA_SERVICES_RUNAS_NAMED_ACCT, IA_SERVICES_RUNAS_PSWD, and IA_SERVICES_RUNAS_USER_ACCT.
INSTALLDIR	*<Path>*	The destination directory for the Client application files. A default value of %ProgramFiles%\InputAccel\Client is used when this property is not specified.

16.4.4.1 Client Components Installation Features

Each feature listed in this table can be used to install its component during a silent installation by specifying its name as the ADDLOCAL property. You can specify more than one feature to install by separating the feature names with commas.

The following are supported feature names that can be specified when installing the Intelligent Capture client:

Table 16-6: Supported Client Components Installation Features

Feature name	Installs
CAPTIVA_ADMINISTRATOR	Intelligent Capture Administrator
CAPTIVA_DEPLOYMENT	Intelligent Capture Deployment
IA_MIGRATE	IA Migrate
PDEV	Intelligent Capture Designer, new samples, and Process Developer
MODULE_SERVER	Module Server Windows service. The Module Server also requires the following features: • IMAGE_CONVERTER • IMAGE_PROCESSOR • EXTRACTION • ENGINE_ADVANCED_OCR • ENGINE_GENERALUSE_OCR • ENGINE_WESTERN_OCR • DIA_CLASSIFICATION • IDENTIFICATION • NUANCE_OCR • STANDARD_OCR
Operator Tools	
CAPTIVA_DESKTOP	The Intelligent Capture Completion module.
SCAN_APPLICATION	The ScanPlus module.
RESCAN_APPLICATION	The RescanPlus module.
Input/Output Modules	
STANDARD_IMPORT	The Standard Import module.
STANDARD_EXPORT	The Standard Export module.
ODBC_EXPORT	The ODBC Export module.
WEB_SERVICES_INPUT	The Web Services Input module.

Feature name	Installs
WEB_SERVICES_OUTPUT	The Web Services Output module.
Web Services Components	
WEB_SERVICES_COORDINATOR	The Web Services Coordinator component.
WEB_SERVICES_HOSTING	The Web Services Hosting component.
Image Handling	
IMAGE_CONVERTER	The Image Converter module.
VIRTUAL_PRINTER	The Virtual Printer feature.  **Note:** Image Converter is required.
IMAGE_PROCESSOR	The Image Processor module.
Recognition	
NUANCE_OCR	The NuanceOCR module.
EXTRACTION	The Extraction module.
STANDARD_OCR	The Standard OCR module.
Enterprise Export Modules	
SAPAL_EXPORT	The Archive Export module.
DCTM_ADVANCED_EXPORT	The Documentum Advanced Export module.
AX_EXPORT	The Documentum ApplicationXtender Export module.
FNCM_EXPORT	The FileNet Content Manager Export module.
FILENET_EXPORT	The FileNet Panagon IS/CS Export module.
WANGNT_EXPORT	The Global 360 Export module.
CMNSTORE_EXPORT	The Export for SAP Archive and AP Connect module.
IBM_CM_EXPORT	The Export for IBM Content Manager module (with the Java API)
ICM_EXPORT	The Export for IBM Content Manager module (with the Java API) and with the Legacy IBM CM C++ client libraries (for v.8.5 and below) option (with the C++ API)
SHRPNT2_EXPORT	The Microsoft SharePoint Export module.
LL2_EXPORT	The Export for OpenText Content Server module.
Utilities	
DOTNETCODE_MODULE	The .NET Code Module.

Feature name	Installs
COPY	The Copy module.
MULTI	The Multi module.
TIMER	The Timer module.
Extraction Engines	
ENGINE_GENERALUSE_OCR	The General-Use OCR engine.
ENGINE_CHECK_READING	The Check Reading engine.
ENGINE_ADVANCED_OCR	The Advanced OCR/ICR engine.
ENGINE_WESTERN_OCR	The Western OCR engine.
Advanced Recognition[a]	
DIA_CLASSIFICATION	The Classification module.
IDENTIFICATION	The Identification module.
DIA_PAL_COLLECTOR	The Collector module.
DIA_PAL_SUPERVISOR	The Production Auto-Learning Supervisor service.
DIA_DEV_KIT	Advanced Recognition development tools and accessories.

[a] Although not listed in the installer, the Dispatcher Manager is also installed.

16.4.4.2 Client Components Installer Command Line Examples

Example 16-10: Install all client components into the default installation directory

The module services are installed and use a specific Windows user account as the "run-as" user account. The installed client services connect to the Intelligent Capture Server "PROD-IASERVER" when started. The services start automatically when Windows starts. The system does not restart after installation even if a reboot is required.

```
setup.exe /s /v"/qn ADDLOCAL="ALL" IA_SERVICES_AUTOSTART=1 IA_
SERVICES_RUNAS_NAMED_ACCT=1 IASERVERNAME="PROD-IASERVER" IA_
SERVICES_RUNAS_USER_ACCT=".\Administrator" IA_SERVICES_RUNAS_
PSWD="password" /norestart"
```

Glossary

ACL

Access Control List

API

Application Programming Interface

ASCII

American Standard Code for Information Interchange

CAF

Captiva Activation File

COM

Component Object Model

CPU

Central processing unit

DEP

Data Execution Prevention

DLL

Dynamic Link Library

DPP

Dispatcher project file extension

FIPS

Federal Information Processing Standard

GB

Gigabyte

HTTP

Hypertext Transfer Protocol

IP

Internet Protocol

IPP

Integrated ProcessFlow Project

ISIS

Image and Scanner Interface Specification

IT

Information Technology

KFI

Key from Image

LUA

least privileged user account

MB

megabyte

MDF

Module Definition File

MSI

Microsoft Windows Installer

MUI

Multilingual User Interface

NAS

Network Attached Storage

NTFS

Microsoft Windows NT File System

NTLM

NT LAN Manager authentication protocol

OCR

Optical Character Recognition

ODBC

Open Database Connectivity

PDF

Portable Document Format

RAID

Redundant Array of Inexpensive Disks

RAM

Random Access Memory

SAN

Storage Area Network

SID

system identifier

SLD

SAP System Landscape Directory

SPN

Service Principal Name

SQL

Structured Query Language

TCP/IP

Transmission Control Protocol/Internet Protocol

TCP

Transmission Control Protocol

UI

User Interface

UNC

Universal Naming Convention

UTF-8

Unicode Transformation Format 8–bit

VBA

Microsoft Visual Basic for Applications

XML

Extensible Markup Language