

EMC[®] Captiva[®] Capture

Version 7.5

Installation Guide

EMC Corporation
Corporate Headquarters
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Legal Notice

Copyright © 1994-2016 EMC Corporation. All Rights Reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com. Adobe and Adobe PDF Library are trademarks or registered trademarks of Adobe Systems Inc. in the U.S. and other countries. All other trademarks used herein are the property of their respective owners.

Documentation Feedback

Your opinion matters. We want to hear from you regarding our product documentation. If you have feedback about how we can make our documentation better or easier to use, please send us your feedback directly at ECD.Documentation.Feedback@emc.com

Table of Contents

Revision History	9
Chapter 1 Captiva Capture Overview	11
Chapter 2 Installation Planning	13
General Considerations	13
Locale Considerations	14
Performance and Throughput	14
Database Server Considerations	15
InputAccel Server Considerations	17
ClickOnce Host System Considerations	18
Web Services Subsystem Considerations	19
Client Machine Considerations	19
Running Modules as Services	20
Scalability	23
InputAccel Server Scalability	23
Client Scalability	24
Security	25
Running Captiva Capture in a Hardened Environment	28
Running Captiva Capture with Minimum Windows Permissions	28
Installing Captiva Capture across Multiple Domains	32
Installing Captiva Capture in a Workgroup	32
High Availability and Failover	33
High Availability Best Practices	33
Disaster Planning	34
Creating a Captiva Capture Disaster Continuation Plan	35
Disaster Recovery Considerations	35
Implementing a Disaster Continuation System	36
Licensing and Activation	36
ScaleServer Licensing	37
Licensing for Use in a Microsoft Cluster	38
Licensing for Disaster Recovery	38
Sample Production Installation Configurations	38
Chapter 3 Installing Captiva Capture	41
Installing Captiva Capture in a Production Environment	41
Installing the InputAccel Database	45
Creating a SQL Server User Account with Minimum Permissions to Access the InputAccel Database	47
Installing the InputAccel Server	47
Installing the Captiva Capture Client Components	50
Additional Installation and Configuration Requirements for Image Converter	53
Installing Multiple Instances of Image Converter	53
Additional Requirements to Run Image Converter as a Service	54
Specifying the Temporary Folder for Storing Intermediate Processed Files	56

Additional Configuration Steps for Processing Files using the Image Converter Module	57
Processing HTML Files using Internet Explorer 10 and 11	57
Processing PDF and Microsoft Office Documents with Security Restrictions	58
Printing Background Colors for MS Word Documents	58
Processing Macro-enabled MS Excel Files.....	58
Downloading ISIS Scanner Drivers	59
Registering the SLDRegistration Executable	59
Activating and Licensing Captiva Capture	59
Licensing the Check Reading Engine:.....	60
Setting the UI Language of Captiva Capture Components	61
Specifying Default UI Language Settings.....	61
Summary of Options for Overriding the Default UI Language.....	62
Procedures to Override the UI Language.....	63
Additional Installation and Configuration Options	65
Installing Multiple Instances of InputAccel Servers	65
Configuring Multiple InputAccel Servers as a ScaleServer Group	67
Installing the InputAccel Server in a Microsoft Failover Clustering Environment	69
Requirements for InputAccel Server in Microsoft Failover Clustering	69
Installing InputAccel Servers into Microsoft Failover Clustering.....	70
Installing Captiva Capture Web Client and Captiva REST Service	78
Localizing and Rebranding the Captiva Capture Web Client User Interface.....	83
Creating Resource Files.....	84
Configuring Pass-Through Login in Captiva Capture Web Client.....	85
Configuring the Jasig Central Authentication Service	85
Installing the Module Server	87
Deploying Modules with the ClickOnce Deployment Utility	89
Unattended Installations	94
Understanding Installation Command Line Arguments	94
Command Line Considerations	96
Installing Captiva Capture from a Command Line	96
Automating Unattended Installations	97
Modifying Unattended Installations	97
Manually Registering a Client Module to Run as a Service	98
Unregistering Client Modules that are Registered as Services	100
Installing Captiva Capture in a Development or Demonstration Environment	101
Chapter 4 Upgrading Captiva Capture	103
Upgrade Planning	103
Upgrade Paths.....	104
Understanding Compatibility among Captiva Capture Components.....	104
Captiva REST Services	106
Custom Modules	106
Understanding Locale Considerations before Planning the Upgrade	108
Identifying Irreplaceable Files	109
Automatic Backup during Upgrade	112
Identifying New System Requirements	113
Understanding the Upgrade Process	113
InputAccel Database.....	113
InputAccel Servers.....	114
Captiva Administrator	115
Licenses, Activation Files, and Security Keys	115
Captiva REST Services	115

Existing Clients	116
New Client Modules.....	121
Permissions.....	121
Performing Pre-Production Testing and Acceptance.....	122
Scheduling Upgrade Phases	122
Upgrading from 6.0 SP3 and 6.5.x to 7.5	123
Upgrade Procedures.....	124
Upgrading the InputAccel Database	125
Upgrading the InputAccel Server	126
Reverting Back to a Previously Installed Version of the InputAccel Server.....	127
Upgrading InputAccel Server in a Microsoft Failover Clustering Environment	127
Requirements.....	128
Upgrading InputAccel Server in a Microsoft Failover Clustering Environment	128
Upgrading Captiva REST Services	129
Upgrading Client Modules.....	130
Reverting to a Previous Client Release	130
Upgrading ClickOnce-Deployed Applications	131
Upgrading Existing CaptureFlow Designer XPP Processes	131
Upgrading Existing Scripts.....	132
Upgrading Documentum Advanced Export Client-Side Scripting.....	132
Sample Upgrade Scenarios	133
Sample Scenario: Upgrade from InputAccel 6.0	133
Sample Scenario: Upgrade from InputAccel 6.5 to 7.5	135
Migration Guidance.....	137
Migrating Processes.....	137
Migrating CaptureFlow-developed Processes to Only Use the .NET Runtime	137
Migrating Process Developer Processes to Captiva Designer.....	138
Migrating CaptureFlow Designer Processes to Captiva Designer	140
Upgrading Process Developer Processes	141
Migrating from Multi-Directory Watch and Email Import to Standard Import.....	141
Migrating from Image Quality Assurance to the Completion Module	142
Migrating from IndexPlus and Dispatcher Recognition to Completion and Extraction.....	142
Migrating from Dispatcher Validation to the Completion Module.....	144
Migrating from Dispatcher Classification Edit to the Identification Module	145
Migrating from Image Enhancement to Image Processor.....	147
Migrating to Use Updated Image Converter.....	148
Migrating to Use Standard Export	148
Chapter 5 Modifying, Repairing, and Removing Captiva Capture	151
Modifying a Captiva Capture Installation.....	151
Repairing a Captiva Capture Installation.....	152
Removing Captiva Capture Components	152
Chapter 6 Troubleshooting	155
Installation Failures	155
Installation Errors.....	156
Command-line Installation Failures	157
Syntax Errors	157
Common Command-Line Installation Errors	157

	Third-party Component Issues	159
	Post-installation Issues	159
	InputAccel Database Issues	160
	ScaleServer Issues	161
	Other Issues	162
Appendix A	Prerequisite Software Installed by the Captiva Capture Setup Program	167
Appendix B	Captiva Capture Client Modules	169
Appendix C	Client Module Features	173
Appendix D	New and Legacy Modules	177
Appendix E	Modules and Components No Longer Shipped	179
Appendix F	Localized Languages	181
Appendix G	Ports Used	183
Appendix H	Running the Database Manager Utility	185
	Running Database Manager in Silent Mode	186
	Database Manager Command-line Examples	187
Appendix I	Command-line Arguments for Installing Captiva Capture	189
	Supported InstallShield Switches	189
	Supported MSI Switches	190
	Supported Windows Installer Properties	190
	Captiva Capture Installer Properties and Feature Names	190
	InputAccel Database Installer Properties	191
	InputAccel Database Installer Command-line Examples	193
	InputAccel Server Components Installer Properties	193
	InputAccel Server Installation Features	200
	InputAccel Server Installer Command-line Examples	200
	Captiva Capture Web Components Installer Properties	202
	Captiva Capture Web Components Installer Command-line Examples	206
	Client Components Installer Properties	206
	Client Components Installation Features	209
	Client Components Installer Command-line Examples	211

List of Tables

Table 1.	Planning Considerations	13
Table 2.	Security Considerations for a Captiva Capture Installation	25
Table 3.	High Availability and Failover Technologies Used in Captiva Capture	33
Table 4.	Production Installation Configurations of a Captiva Capture System	39
Table 5.	Production Installation of a Captiva Capture System.....	41
Table 6.	Globalization and UI Language Settings for Captiva Capture Components	62
Table 7.	Captiva Capture Installation Command Line Arguments	94
Table 8.	Development or Demonstration Installation	102
Table 9.	Client Upgrade Compatibility with InputAccel Server	105
Table 10.	Running Custom Modules with an Earlier SDK	106
Table 11.	Irreplaceable Files and Data	110
Table 12.	Automatic Backup Locations during an Upgrade.....	112
Table 13.	Client Module Upgrade Issues	116
Table 14.	146
Table 15.	Common Installation Problems	156
Table 16.	Common Installation Problems	158
Table 17.	Common InputAccel Database-Related Problems	160
Table 18.	Other Problems during InputAccel Setup.....	162
Table 19.	Captiva Capture Modules	170
Table 20.	Client Components Installation Features	173
Table 21.	Localized Languages Captiva Capture	181
Table 22.	Ports Used	183
Table 23.	Explanation of Command-line Arguments used to Install the InputAccel Database	186
Table 24.	Explanation of Command-line Arguments used to Install the File-based Database	187
Table 25.	Supported InstallShield Switches.....	189
Table 26.	Supported InputAccel Database Installer Properties.....	191
Table 27.	Supported InputAccel Server Installer Properties.....	195
Table 28.	Supported InputAccel Server Installation Features.....	200
Table 29.	Supported Captiva Capture Web Component Installer Properties	202
Table 30.	Supported Client Components Installer Properties	207
Table 31.	Supported Client Components Installation Features	209

Revision History

Revision Date	Description
June 2016	In Running Captiva Capture with Minimum Windows Permissions , page 28, added minimum permission requirements for the Captiva REST Services.
March 2016	Added Configuring Pass-Through Login in Captiva Capture Web Client , page 85.
December 2015	Clarified that modules that are no longer shipped are removed and that 6.0 SP3, 6.5, 6.5 SP1, or 6.5 SP2 client modules that are currently installed work as-is and do not need to be upgraded. See Upgrading from 6.0 SP3 and 6.5.x to 7.5 , page 123.
June 2015	Updated Third-party Component Issues , page 159: updated list of modules that will not run until third-party components are installed.
May 2015	Initial Revision

Captiva Capture Overview

Captiva 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. Captiva 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.

Captiva 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. Benefits of Captiva 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.

Captiva Capture is modular and scalable; therefore, installation complexity depends on the business requirements of each organization. Various system configuration examples are provided in [Sample Production Installation Configurations, page 38](#). Different components have different hardware and software requirements, as explained in detail in the *Release Notes*.

This guide explains how to install, configure, and upgrade Captiva Capture.

Related Topics —

[Chapter 2, Installation Planning](#)

[Chapter 4, Upgrading Captiva Capture](#)

Installation Planning

A successful Captiva Capture installation depends on having a good installation plan. There are several considerations to understand before beginning with the installation. Topics in this section include:

- [General Considerations, page 13](#)
- [Sample Production Installation Configurations, page 38](#)

General Considerations

Carefully planning the installation requires attention to many aspects, including: hardware, software, locale, networking, security, system availability, backup, recovery, and more. The following table summarizes many of these issues and directs you to more information.

Table 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. (Locale Considerations, page 14)
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. (Performance and Throughput, page 14)
Scalability	Decide whether to install the entire system at once or start with a small system and then expand. Captiva Capture supports both server and client scalability. (Scalability, page 23)
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 InputAccel Database (if installed).
Network configuration	Determine how Captiva Capture fits into your network topology. Captiva Capture can be deployed to a single domain, multiple domains, or to a single, standalone machine. (Installing Captiva Capture across Multiple Domains, page 32)

Item	Planning activity
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 InputAccel 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. (High Availability and Failover, page 33)
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. (Disaster Planning, page 34)
Licensing and activation	EMC offers many different licensing plans to meet the needs of different types of customers. Obtain license codes for each InputAccel Server and use a software activation file issued by EMC. (Licensing and Activation, page 36)

Locale Considerations

Captiva 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. Refer to the [Administration Guide](#) to understand the multiple language feature.

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 InputAccel Server, the language specified by the locale setting must be supported by the code page selected on that machine.

Performance and Throughput

Maximizing performance and throughput are key objectives when designing a Captiva 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 Captiva Capture modularity.

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

To maximize the performance and throughput at all points in the system, consider each of the following components individually:

- [Database Server Considerations, page 15](#)
- [InputAccel Server Considerations, page 17](#)
- [ClickOnce Host System Considerations, page 18](#)
- [Web Services Subsystem Considerations, page 19](#)
- [Client Machine Considerations, page 19](#)

Database Server Considerations

The SQL Server hosted InputAccel Database is an optional component. The database is required only if your environment has any of the following requirements:

- Reporting functionality is required
- ScaleServer capability is required
- Web Services must be supported
- Microsoft Failover Clustering support is required
- Side-by-side InputAccel Servers are required
- You are upgrading from a Captiva 7.0 or 7.1 environment that included the InputAccel Database
- You are upgrading from Captiva 6.x

The machine that hosts the InputAccel 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 InputAccel 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 very 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 InputAccel Server and the InputAccel Database must have high bandwidth (about 1 GB per second) and low latency. For the InputAccel 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. Connect the drives to disk controllers that provide hardware-level support for RAID 0+1 or RAID 1+0. (RAID 0+1 and RAID 1+0 are recommended, RAID 0 is also acceptable, and the minimum requirement is for RAID 5. Note the RAID 5 is not recommended for high volume deployments.) In addition, the 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. Disk controllers that are integrated into motherboards typically do not provide the features, performance, or reliability that an enterprise platform demands.

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

Additional considerations when setting up the InputAccel Database:

- For all but low volume deployments, Captiva Capture requires a dedicated computer for the SQL Server that hosts the InputAccel Database. This computer must meet the recommended hardware requirements specified in the *Release Notes*. High volume deployments may require larger than the recommended hardware.
- Make sure that the SQL Server that hosts the InputAccel Database has sufficient connections available to accommodate your Captiva Capture system. Each InputAccel Server and web service instance consumes one connection.
- 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 InputAccel Database. You cannot increase performance by adding more instances of the InputAccel Database.
- If SQL Server has the necessary performance, then multiple InputAccel Databases (each with a different name) can be installed on a single instance of SQL Server. However, each InputAccel Server requires only one InputAccel Database. If you have multiple, independent InputAccel Servers, then they can share the same InputAccel Database, or they can have independent InputAccel Databases.
- The machine hosting the InputAccel Database should have the highest-speed network connection with low latency available to ensure maximum throughput.
- A ScaleServer group must have a single InputAccel Database. All InputAccel Servers within the ScaleServer group must access the same InputAccel Database. Within a Captiva Capture deployment, independent InputAccel Servers not configured as a ScaleServer group may access the same InputAccel Database or separate InputAccel Databases based on business requirements.
- Multiple Captiva Capture deployments that are completely separate and should be kept separate, require separate InputAccel Databases.
- A test InputAccel Database and a production InputAccel Database can be installed on the same SQL Server. However, EMC recommends 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.
- The amount of data written to the InputAccel Database is related to the logging and reporting configuration. Enabling Audit Logging and Reporting writes significant amounts of data to the InputAccel Database.
- By default, SQL Server Express does not accept connections over the TCP/IP protocol. Enable TCP/IP connections before installing the InputAccel 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:
 - 10 GB limit in SQL Server 2012 Express: When the database reaches this size, you must manually purge batches and other data before you can continue to use Captiva Capture.
 - SQL Server Express does not support configuration for failover or high availability.

- SQL Server Express supports the use of one GB of RAM, and utilizes 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.

Related Topics —

[Chapter 2, Installation Planning](#)

[Installing the InputAccel Database, page 45](#)

[InputAccel Database Issues, page 160](#)

InputAccel Server Considerations

The InputAccel 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, there are some important factors to consider related to the InputAccel Server.

- For all but low volume deployments, Captiva Capture requires a dedicated computer for the InputAccel Server. This computer must meet the recommended hardware requirements specified in the *Release Notes* (available from the **Start** menu of your desktop at **All Programs > EMC Captiva Capture > Documentation**). High volume deployments may require larger than the recommended hardware.
- Use the same performance considerations as for the InputAccel Database (described in [Database Server Considerations, page 15](#)) for selecting a network connection and a disk system for the InputAccel Server data directory (C:\IAS by default). Also, do not locate the InputAccel Server data directory and the Windows paging file on the same physical disk drive.
-



Caution: Do not run antivirus software on the InputAccel Server data directory. Running antivirus software on the InputAccel Server data directory and its subfolders will drastically degrade InputAccel 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 InputAccel Server operation. In all cases, you should exclude the following directories and their subdirectories from antivirus scanning:

InputAccel Server data directory (by default, C:\IAS)

InputAccel 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> is 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 InputAccel 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 Captiva system to crash. The files in the directories for Captiva use are transitory; that is, they exist only as long as the batch is in Captiva.

Note: You might consider an audit by security professionals who are familiar with Captiva 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-Captiva) systems could be one such optimal point in the chain of custody. Another alternative is to schedule a full virus scan of the InputAccel Server data folder to occur during off-production hours when the InputAccel Server service can be paused or stopped.

- Another option for improving performance is to install multiple InputAccel Server instances as described in [Installing Multiple Instances of InputAccel Servers, page 65](#). Each InputAccel Server instance should have 4 GB RAM and should have its data directory on a separate disk drive.
- The InputAccel 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 InputAccel 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. Note that while NAS is supported, it is not recommended as typically it reduces the server throughput.
- Be aware that even though the InputAccel Server will run under a VMware ESX Server, doing so will degrade the InputAccel Server performance by approximately 20% or more.

Related Topics —

[Installing the InputAccel Server, page 47](#)

[Upgrading the InputAccel Server, page 126](#)

[ScaleServer Issues, page 161](#)

ClickOnce Host System Considerations

ScanPlus and RescanPlus client modules can be distributed by using Microsoft ClickOnce deployment technology. ClickOnce can be accomplished either by deploying applications from a file share or from a web server. In either case, installations are relatively infrequent and have minimal performance impact. Unless the system that hosts ClickOnce is being shared with other Captiva Capture components that have special needs, no special performance or throughput considerations are required for this machine.

Before deploying modules using ClickOnce, ClickOnce publishing skills or a minimal understanding of ClickOnce technology is recommended. Be sure to read the articles about ClickOnce technology available on the Microsoft MSDN website.

Note:

- Command-line parameters (such as `-department`) cannot be specified when a module is deployed by ClickOnce from a file share, because the shortcut icon does not reference an actual module that can accept command-line arguments. If operators must specify departments or other command-line arguments when starting modules, deploy the modules from an IIS web server.
- Due to the way ClickOnce-deployed modules are registered, they are unable to write complete module information to the Windows Event Log. Therefore, message descriptions in the Windows Event Log will not exactly match messages displayed in Captiva Administrator.

Related Topics —

[Chapter 2, Installation Planning](#)

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 InputAccel Database, and should therefore be installed on a secure server with a high-speed network connection to the InputAccel 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 very little processing. Typically the only reason to install multiple instances is to separate internal from external request/response traffic. In any case, a Captiva 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.

Related Topics —

[Chapter 2, Installation Planning](#)

Client Machine Considerations

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

It is recommended that the network connection between the InputAccel 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 InputAccel Servers. Unattended modules are server-grade applications that should be installed on IT-managed servers and, if supported, run as Windows services. (Refer to [Table 19, page 170](#) for a list of modules that run in unattended mode and that run as services.) 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.

Note: 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. [Table 19, page 170](#) provides 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. [Manually Registering a Client Module to Run as a Service, page 98](#) explains how to configure modules that have already been installed to run as services.

For modules that support multiple service instances (as listed in [Appendix B, Captiva Capture Client Modules](#)), 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.

Related Topics —

[Running Modules as Services, page 20](#)
[Appendix B, Captiva Capture Client Modules](#)

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 InputAccel Server](#)
3. [Captiva Capture permissions](#)

Note: For a list of client modules that can be run in unattended mode and as services, refer to [Table 19, page 170](#).

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 InputAccel 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:** Captiva Capture supports the use of the Network Service account in cases where customers cannot use a user account to run modules as services. There are multiple ways to configure a module running under Network Service to authenticate with the InputAccel Server machine. We recommend that you enable and configure Kerberos authentication, as explained in [Configuring Captiva Capture to use Kerberos authentication](#), page 22.

Note:

- 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 Captiva 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 InputAccel 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 Captiva Administrator.

Enabling the “run-as” account to log into the InputAccel Server

Regardless of whether a module runs under a user account or Network Service, that account must have the ability to log into the InputAccel Server machine. This ability is automatically configured when using a domain user account—members of the `Domain\Users` group are added to the InputAccel 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 InputAccel Server (unless the module is running on the same machine as the InputAccel 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 InputAccel Server machine.

Configuring Captiva Capture Permissions

Use Captiva 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 Captiva 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 Captiva Capture modules running as services under Network Service.

The *Using Captiva Administrator* section in the [Administration Guide](#) provides more information about adding users and groups to permission roles.

Configuring Captiva Capture to use Kerberos authentication

To configure authentication using Kerberos in your Captiva 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 InputAccel Server.

Note:

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

To configure Captiva 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 InputAccel 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 InputAccel 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 InputAccel Server and the connection fails.

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

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

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

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

where:

- *ServiceClass*: Must be **IAServer**.
- *Host*: Fully qualified host name of the InputAccel 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 InputAccel Server is listening on (default: 10099).
- *MachineName*: The Windows account used to run the InputAccel Server service. When the InputAccel Server runs under Local System account, the *MachineName* is the machine name of the InputAccel Server. When the InputAccel Server runs under a domain user account, the *MachineName* is the user account name.

Examples —

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

Note:

- 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 InputAccel Server.

Related Topics —

[Appendix B, Captiva Capture Client Modules](#)

[Installing the Captiva Capture Client Components, page 50](#)

Scalability

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

Topics in this section include:

- [InputAccel Server Scalability, page 23](#)
- [Client Scalability, page 24](#)

InputAccel Server Scalability

When the document capture workload exceeds the capabilities of a single InputAccel Server, scale up the system by adding more InputAccel Servers and creating a ScaleServer group. A ScaleServer group combines multiple InputAccel 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 InputAccel 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 InputAccel 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 InputAccel Servers in the group simultaneously. Modules that are not ScaleServer compatible can connect to any one InputAccel Server in the ScaleServer group at a time. (No module can connect to multiple arbitrary InputAccel Servers - only to multiple servers that have been configured as a ScaleServer group.)

[Appendix B, Captiva Capture Client Modules](#) provides a table of client modules that indicates which modules are ScaleServer compatible.

Additional InputAccel Servers can be added to a ScaleServer group when the Captiva Capture system is initially configured or at any later time. For more information on managing and licensing ScaleServer groups, refer to the *Using Captiva Administrator* section in the [Administration Guide](#). For instructions on installing a ScaleServer group, refer to [Configuring Multiple InputAccel Servers as a ScaleServer Group](#), page 67.

Note: 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.

Note: ScaleServer technology does not provide batch data sharing.

The InputAccel 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 InputAccel 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 InputAccel Server to be installed in an Active/Active Microsoft Failover Clustering, as explained in [High Availability and Failover](#), page 33.

Related Topics —

[Installing the InputAccel Server](#), page 47

[Upgrading the InputAccel Server](#), page 126

[ScaleServer Issues](#), page 161

Client Scalability

Captiva Capture client modules process tasks sent to them from InputAccel Servers. Captiva 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. There are several factors to consider when planning the number of each module required:

- The volume of incoming paper that must be processed. For example, 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. Captiva Capture enables installing as many ScanPlus (and RescanPlus) machines as required to handle high workloads.
- The amount of processing power the module needs. For example, 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. Captiva Capture enables adding as many OCR modules as necessary to keep up with the system workload.

- The amount of time an operator requires to process a task. For example, 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. Captiva 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 B, Captiva Capture Client Modules](#) 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, page 98](#) explains how to install modules as services using the *serviceName* command-line argument.

Related Topics —

[Appendix B, Captiva Capture Client Modules](#)

Security

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

The following table explains major security considerations.

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

Table 2. Security Considerations for a Captiva Capture Installation

Element	Security considerations
SQL Server	<p>Captiva Capture supports only SQL Authentication. Therefore, SQL Server and Windows Authentication mode must be enabled in the SQL Server and a valid SQL Server login ID is required to connect to the SQL Server that hosts the InputAccel Database.</p> <p>A login ID having a SQL Server <code>dbcreator</code> role must be specified to create the InputAccel Database during the InputAccel Database installation.</p>

Element	Security considerations
InputAccel Database	<p>The InputAccel Database must have the database role membership set to Public. Captiva Capture does not use user-based authentication or authorization for database access; therefore, there is no need to create database users and groups. Choose any of the following options for database access:</p> <ul style="list-style-type: none"> • Create a SQL Server user account with SQL Authentication enabled. Grant the following permissions to the account: Connect, Delete, Execute, Insert, Select, and Update. Use this account to access the InputAccel 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.
InputAccel Server	<ul style="list-style-type: none"> • The InputAccel 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 InputAccel Server is done automatically by the InputAccel 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, page 162. • The Federal Information Processing Standard (FIPS) provides best practices for implementing cryptographic software. The InputAccel Server is designed to operate with Microsoft operating systems that use FIPS-compliant algorithms for encryption, hashing, and signing.
Authentication	<p>Captiva 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.</p> <p>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.</p>
Client privileges	<p>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.</p> <p>Access to client modules can be controlled by using Captiva Capture user roles and further refined by employing ACLs. User roles and ACLs are managed in Captiva Administrator. In addition, Captiva Capture licensing globally restricts which components can run and how many components can connect to an InputAccel Server at one time.</p>

Element	Security considerations
Web components	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – ClickOnce deployment – Captiva REST Service – Captiva 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 (ACLs), licensing, and Captiva Administrator-assigned user roles.
User accounts	<p>Consider using matching Windows user groups and Captiva roles for users to simplify permissions control.</p> <p>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 Captiva Administrator and all client modules. This default administrator user must create and configure the roles and permissions needed in Captiva Administrator, and then add users to these roles. This step is necessary to do before users can run client modules in production mode.</p> <p>Consider creating a “Captiva Capture Supervisors” role with members having specific Captiva Administrator permissions and full permissions to run client modules, and a “Captiva 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 and/or members.</p> <p>Captiva Capture requires that user accounts have passwords. Blank passwords are not supported in any scenario, even on a single-machine installation.</p> <p>Note: Default version of these roles with associated permissions are predefined in Captiva Administrator. Examine these default roles and change the permissions and then add new roles as required.</p> <p>Passwords must not contain “@” symbols because this symbol is used as a delimiter in command line arguments.</p> <p>Servers and client modules running as services can be configured to run under a specific user account or a built-in machine account.</p> <p>As with most software applications, the user installing Captiva Capture components must be a member of the machine’s local Administrators group.</p> <p>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 Captiva Administrator.</p>

Element	Security considerations
Firewalls	<p>Users are responsible for configuring firewall software in a compatible manner, as follows:</p> <ul style="list-style-type: none"> Ensuring that InputAccel Servers can communicate with the InputAccel Database (if installed). Firewalls in the path of the SQL Server that hosts the InputAccel Database must be configured to pass network traffic on the TCP port 1433.
Firewalls (continued)	<p>Note: When installing an InputAccel 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 Captiva Administrator.</p>

Other security considerations include:

- [Running Captiva Capture in a Hardened Environment, page 28](#)
- [Running Captiva Capture with Minimum Windows Permissions, page 28](#)

Running Captiva 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.

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

Related Topics —

[Chapter 1, Captiva Capture Overview](#)
[Chapter 2, Installation Planning](#)

Running Captiva Capture with Minimum Windows Permissions

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

- **InputAccel Database (if installed):**
 - **User:** A SQL Server user account with SQL Authentication enabled and these permissions enabled: **Connect**, **Delete**, **Execute**, **Insert**, **Select**, and **Update**.
- **InputAccel Servers:**
 - **User:** Must be a member of the **InputAccel_Server_admin_group** group on the server machine. This group is created by the InputAccel Server setup program and is granted the

following privileges and permissions, which are the only rights required for the InputAccel Server to function:

- Impersonate a client after authentication
- Load and unload device drivers
- Create global objects
- Full permissions on the InputAccel 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: On Windows 8, Windows 8.1, Windows Server 2012 and Windows Server 2012 R2, 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:**

- InputAccel 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 Captiva Capture objects.
- Captiva Capture Performance Counters (iaspmd1164.dll) uses shared memory with explicit permissions to read and write for authenticated accounts.
- Captiva REST Services (which includes Captiva REST Service, Module Server, Captiva Capture Web Client)
 - Shared data folder: If you are running multiple instances of Captiva 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.
 - For each Captiva 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 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

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

- Add the identity to the Captiva **Administrators** role so that it has the necessary permissions on the InputAccel Server.
- For Captiva REST Service and Captiva Capture Web Client, configure the SSL certificate and HTTPS binding by adding these bindings in **IIS Management Console** in **Actions > Bindings**.
- **All modules:** (By default, the Captiva Capture installer grants the required access to the specified folders and directories.)

- **User:** All users must have Read access to the InputAccel Server (IAS) data directory (c:\IAS by default) on each of the InputAccel Servers.

In addition, modules that create batches (for example: ScanPlus, Standard Import, WS Input) need Write access to the same folder.

- **Directories:**
 - **All supported operating systems:** Users must have Read/Write access to c:\ProgramData\EMC\InputAccel\settings.ini
 - 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 [Table 19, page 170](#) 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 do not require access to the logging library.
- **All modules listed as “New in 6.x” and “New in 7.x” in [Table 19, page 170](#):**
 - **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 Windows directories such as `c:\Windows\System32`.
- **All ClickOnce modules:**
 - **User:** Client machines must be part of the local **Users** group. To install ClickOnce prerequisites, the user must be a member of the **Administrators** group.
- **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 Captiva Capture installation directory to reserve these ports.
- **ClickOnce Deployment Utility (CODU):**
 - **User:** To write deployment packages to a web host, the user must be a member of the **Administrators** group on the target web server machine.
 - **Directories:** The user who is create deployment packages must have Write permissions for the directory where the deployment packages are written.

Related Topics —

[Chapter 1, Captiva Capture Overview](#)

[Chapter 2, Installation Planning](#)

Installing Captiva Capture across Multiple Domains

The Captiva 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 guide.

Any user who logs into an InputAccel Server must have the “Windows Login” privilege on the machine hosting the InputAccel Server.

To assign users or groups from other domains to Captiva Capture security roles, Captiva 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 Captiva Capture system is running.

Related Topics —

[Running Captiva Capture with Minimum Windows Permissions, page 28](#)

[Installing Captiva Capture in a Workgroup, page 32](#)

Installing Captiva Capture in a Workgroup

Installing Captiva 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, Captiva Capture still requires users to log in with a valid Microsoft Windows user name and password. Blank passwords are not allowed. Refer to [Installing Captiva Capture in a Development or Demonstration Environment, page 101](#) for detailed instructions.

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

Related Topics —

[Running Captiva Capture with Minimum Windows Permissions, page 28](#)

[Installing Captiva Capture across Multiple Domains, page 32](#)

High Availability and Failover

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

Table 3. High Availability and Failover Technologies Used in Captiva Capture

Technology	Description
ScaleServer groups	<p>If an InputAccel Server becomes unavailable due to a planned or unplanned interruption, other InputAccel 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.</p> <p>Refer to Configuring Multiple InputAccel Servers as a ScaleServer Group, page 67 for instructions on installing and configuring ScaleServer groups.</p>
General considerations	<p>Part of high availability includes choosing components and best practices designed to deal with faults. Examples include:</p> <ul style="list-style-type: none"> • 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 in the event of a power outage. • Remote monitoring and tuning software.
General considerations (continued)	<ul style="list-style-type: none"> • VMware VMotion in lieu of clustering, enabling movement of virtual machines from one host to another in the event of a system failure. • Offsite storage for short term, rotating backup of paper that has been scanned in addition to media containing backups of irreplaceable files.
Modular clients	<p>Client modules can be brought online to supplement or replace existing client modules without disrupting production. Refer to Installing the Captiva Capture Client Components, page 50 for client installation instructions.</p>

High Availability Best Practices

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

- At a minimum, connect the InputAccel Server machine and the InputAccel Database machine to an uninterruptible power supply.
- Configure the SQL Server for high availability by setting up database mirroring and/or clustering. Refer to Microsoft recommendations for advice and instructions.
- Configure the InputAccel Servers for high availability by using ScaleServer groups and configuring them in an Active/Passive or Active/Active Microsoft Failover Clustering cluster. Refer to [Configuring Multiple InputAccel Servers as a ScaleServer Group, page 67](#) and [Installing the InputAccel Server in a Microsoft Failover Clustering Environment, page 69](#) for instructions.
- Run unattended client modules as services and configure those services for high availability by enabling automatic restart on failure. Refer to [Manually Registering a Client Module to Run as a Service, page 98](#) for the necessary settings.

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. 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 in the event of a disaster.
- 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 in the event of a disaster.

EMC offers disaster recovery pricing that provides licensing and activation for periodic testing and one-time use of a disaster continuation system.

Topics in this section include:

- [Creating a Captiva Capture Disaster Continuation Plan, page 35](#)
- [Disaster Recovery Considerations, page 35](#)
- [Implementing a Disaster Continuation System, page 36](#)

Creating a Captiva Capture Disaster Continuation Plan

Disaster recovery planning should include a written plan describing exactly how to restore Captiva Capture production after a disastrous event. When writing the plan, consider the following questions:

- Who are the key personnel responsible for rebuilding the Captiva 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?

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 InputAccel Server IAS directories
- InputAccel Database from SQL Server
- Scanner drivers
- License files
- Patches
- Custom server and client software (from your developers or EMC Consulting)
- Custom client desktop shortcuts
- Client side script source code
- Client `win.ini` and `settings.ini` files

[Table 11, page 110](#) provides a detailed list of files that should be backed up together with their default locations on server and client machines.

Related Topics —

[Disaster Planning, page 34](#)

[Implementing a Disaster Continuation System, page 36](#)

[Installing the InputAccel Server in a Microsoft Failover Clustering Environment, page 69](#)

Implementing a Disaster Continuation System

Implementing a robust Disaster Recovery system is complicated, detailed and specific to each customer's environment. Contact EMC Consulting Services for help in planning, implementing, and testing a Disaster Recovery environment.

Related Topics —

[Disaster Planning, page 34](#)

[Disaster Recovery Considerations, page 35](#)

[Installing the InputAccel Server in a Microsoft Failover Clustering Environment, page 69](#)

Licensing and Activation

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

License codes are uniquely keyed to the Server ID that the InputAccel 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 InputAccel 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 InputAccel Server uses an activation file, which controls the licensing of the Captiva Capture system. Be aware that each InputAccel Server requires a one-time Internet activation step. Perform the activation step in the **Server Activations** pane of Captiva Administrator, where you can link directly to the EMC Captiva Activation Portal. You can also access the Activation Portal from <http://activation.captivasoftware.com>.

In the Activation Portal, 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 InputAccel Server to a different machine.
- Request conversion from using a hardware security key to a software activation file.

Note: Use activation file (software) security keys with side-by-side InputAccel Server installations. For more information on side-by-side installations, refer to [Installing Multiple Instances of InputAccel Servers, page 65](#).

To install and manage license codes, and to activate InputAccel Servers using activation files, use Captiva Administrator. You will typically receive a file from EMC containing all of your license codes, which you can import to your InputAccel Server in a single step. You can also manually type license codes one at a time. For more information on licensing and activation, refer to the *Using Captiva Administrator* section in the [Administration Guide](#).

Captiva REST Service client (including Captiva Capture Web Client) and Module Server licensing is managed through the Captiva REST Services Licensing tool.

For more information about the Captiva REST Services Licensing tool, see the [Administration Guide](#).

Topics on licensing and activation include:

- [ScaleServer Licensing, page 37](#)
- [Licensing for Use in a Microsoft Cluster, page 38](#)
- [Licensing for Disaster Recovery, page 38](#)

ScaleServer Licensing

Captiva Capture licensing for ScaleServer enables multiple InputAccel Servers to be configured so that all modules can connect to them. ScaleServer groups are defined and managed in Captiva Administrator. Each InputAccel 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 InputAccel 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 Captiva Capture licensing and is an available option in other license levels. Contact your account manager if unsure about the features included with your license.

Example —

- 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 Captiva Capture system in that day.

This is a simple example, but the logic applies to more complex scenarios, where you may have eight InputAccel Servers in a ScaleServer group, all having different remaining daily page counts.

For instructions on setting up ScaleServer groups and managing licenses, refer to the *Using Captiva Administrator* section in the [Administration Guide](#).

Related Topics —

- [Licensing for Use in a Microsoft Cluster, page 38](#)
- [Licensing for Disaster Recovery, page 38](#)

Licensing for Use in a Microsoft Cluster

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

For detailed information on configuring multiple InputAccel Server instances in an Microsoft Failover Clustering cluster, refer to [Installing the InputAccel Server in a Microsoft Failover Clustering Environment, page 69](#). For instructions on installing and managing licenses, refer to the *Using Captiva Administrator* section in the [Administration Guide](#).

Related Topics —

[Licensing for Disaster Recovery, page 38](#)

Licensing for Disaster Recovery

Certain levels of Captiva 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 your account manager. For information on setting up a disaster recovery system, refer to [Disaster Planning, page 34](#). For instructions on installing and managing licenses, refer to the *Using Captiva Administrator* section in the [Administration Guide](#).

Related Topics —

[ScaleServer Licensing, page 37](#)

[Licensing for Use in a Microsoft Cluster, page 38](#)

Sample Production Installation Configurations

The following table shows the Captiva 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 Captiva Capture in a Production Environment, page 41](#).

Table 4. Production Installation Configurations of a Captiva Capture System

Server/Machine	Small Volume	High Volume	High Availability
SQL Server Machine 1	(Optional) InputAccel Database hosted by SQL Server	(Optional) InputAccel Database hosted by SQL Server	(Required) InputAccel Database hosted by SQL Server installed in a Microsoft cluster
SQL Server Machine 2	-	-	(Required) InputAccel Database hosted by SQL Server installed in a Microsoft cluster
InputAccel Server Machine 1	InputAccel Server	InputAccel Server	InputAccel Server installed side-by-side and configured in a Microsoft Failover Clustering ServerActive/Active cluster
InputAccel Server Machine 2	-	-	InputAccel Server installed side-by-side and configured in a Microsoft Failover Clustering Active/Active cluster
Client Module Machine 1 (a)	<ul style="list-style-type: none"> • Captiva Designer • Captiva Administrator 	<ul style="list-style-type: none"> • Captiva Designer • Captiva Administrator 	Captiva Designer
Client Module Machine 1 (b)	-	-	Captiva Administrator
Client Module Machine 2	ScanPlus	ScanPlus	ScanPlus
	Completion		
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 Captiva REST Service Web machines can work with the same IA ScaleServer group.	<ul style="list-style-type: none"> • Captiva REST Service • Your custom Captiva REST Service authentication plugin • Captiva Capture Web Client 	<ul style="list-style-type: none"> • Captiva REST Service • Your custom Captiva REST Service authentication plugin • Captiva Capture Web Client 	<ul style="list-style-type: none"> • Captiva REST Service • Your custom Captiva REST Service authentication plugin • Captiva Capture Web Client
Machine 6 (Storage Device)	Captiva REST Service and Module Server shared data storage	Captiva REST Service and Module Server shared data storage	Captiva 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 Captiva Capture Web Client	Browser access to Captiva Capture Web Client	Browser access to Captiva 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 Captiva Mobile SDK, which is packaged separately from Captiva Capture.	Your custom mobile capture application	Your custom mobile capture application

Installing Captiva Capture

This section explains how to install Captiva Capture for the first time.

Topics on installing Captiva Capture include:

- [Installing Captiva Capture in a Production Environment, page 41](#)
- [Additional Installation and Configuration Options, page 65](#)
- [Installing Captiva Capture in a Development or Demonstration Environment, page 101](#)

Installing Captiva Capture in a Production Environment

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

Table 5. Production Installation of a Captiva Capture System

Server/Machine	Component to install	User Account	Runs as
Server 1	(Optional in general, but required for Web Services) InputAccel Database hosted by SQL Server. Configuring SQL Server in a clustered environment for high availability is recommended.	N/A	N/A
Server 2a	InputAccel Server	User in the local InputAccel_Server_admin_group group	Service
Server 2b	InputAccel Server	User in the local InputAccel_Server_admin_group group	Service

Server/Machine	Component to install	User Account	Runs as
Server 4	<ul style="list-style-type: none"> • (Optional) ClickOnce packages • ClickOnce Deployment Utility 	Domain user in the local Administrators group	N/A
Machine 5	Captiva Designer	Domain user	Application
Machine 6	Captiva Administrator	Domain user	Application
Machine 5	ScanPlus	Domain user	Application
Machine 6	RescanPlus	Domain user	Application
Machine 7	Completion	Domain user	Application
Machine 8	Identification	Domain user	Application
Machine 8 (multiple) Note: Web Services Coordinator can only be installed on a single machine in the Captiva Capture system.	(Optional and requires the InputAccel Database) <ul style="list-style-type: none"> • Web Services Coordinator • Web Services Hosting • Web Services Input • Web Services Output 	Domain user	Service only
Machine 9 (multiple) Note: Multiple Captiva REST Service Web machines can work with the same IA ScaleServer group.	(Optional) <ul style="list-style-type: none"> • Captiva REST Service • Your custom Captiva REST Service authentication plugin • Captiva Capture Web Client 	Domain user	Web application
Machine 10 (Storage Device)	(Optional) Captiva REST Service and Module Server shared data storage	N/A	N/A
Machine 11	Module Server	Network Service	Service
Machine 12	Image Processor	Network Service	Service
Machine 13	NuanceOCR	Network Service	Service

Server/Machine	Component to install	User Account	Runs as
Machine 14	Documentum Advanced Export	Network Service	Service
Machine 15	<ul style="list-style-type: none"> Multi Image Converter 	Network Service	Service
Machine 16	Standard Import	Network Service	Service
Machine 17	Standard Export	Network Service	Service
Machine 18 (multiple)	Other unattended client modules	Network Service	Service
Machine 19 (multiple)	Browser access to Captiva Capture Web Client	Domain user	Browser application
Mobile Devices (multiple)	Your custom mobile capture application Note: Custom mobile capture applications are developed using the Captiva Mobile SDK, which is packaged separately from Captiva Capture.	Customer-defined	Customer-defined

To install Captiva Capture in a typical production environment:

1. Make sure the servers and machines meet the system requirements outlined in the *Release Notes*. This document is available from the **Start** menu of your desktop at **All Programs > EMC Captiva Capture > Documentation**. For the best performance, always use the vendor's latest operating system (that EMC supports) for all Captiva 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 Captiva 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 Captiva Capture system.
2. (Optional) Install InputAccel Database on Server 1. Refer to [Installing the InputAccel Database, page 45](#) for instructions on installing the InputAccel Database.
3. Install the InputAccel Server. You have the following options:
 - Install the InputAccel Server on a single machine, Server 2. Refer to [Installing the InputAccel Server, page 47](#) for instructions.
 - Install multiple instances of the InputAccel Server on a single machine, Server 2. Refer to [Installing multiple instances of the InputAccel Server](#) for instructions.
 - Install the InputAccel Server on multiple machines, Server 2a and Server 2b, and optionally [configure them as a ScaleServer group](#).
 - Install the InputAccel Servers in a clustered environment and then configure them as a ScaleServer group. Refer to [Installing the InputAccel Server in a Microsoft Failover Clustering](#)

[Environment, page 69](#) for instructions on installing InputAccel Servers in an Active/Passive or Active/Active clustered environment.

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

4. Install development tools, Captiva Administrator, attended client modules, Completion, ScanPlus, RescanPlus, and Identification as applications on each machine designated for these modules according to the installation plan. Refer to [Installing the Captiva Capture Client Components, page 50](#) for instructions.

Note: ScanPlus and RescanPlus modules may optionally be deployed using the ClickOnce Deployment Utility. Users can then download these modules through a web server or network file share. Refer to step 6 for instructions.

5. (Optional. This step is required only if ScanPlus and RescanPlus are deployed using the ClickOnce Deployment Utility). Install ScanPlus ClickOnce Package and RescanPlus ClickOnce Package. Follow the same steps involved in installing client modules. Also, [deploy the ClickOnce packages on a web server or network file share by running the ClickOnce Deployment Utility](#) on the same machine.
6. (Optional) Install Web Services Coordinator, Web Services Hosting, Web Services Input, and Web Services Output client modules on a separate machine.
7. (Optional) Install the Captiva REST Service (stand-alone) and any custom applications that use it as follows:
 - a. Install and configure the Captiva REST Service and your custom Captiva REST Service authentication plugin on a separate machine.
 - b. Create an appropriate location for Captiva REST Service shared data storage and specify it in the Captiva REST Service configuration tool.
 - c. Deploy your custom applications that use the Captiva REST Service.
8. (Optional) Install the Captiva Capture Web Client and Captiva REST Service as follows:
 - a. Install and configure Captiva Capture Web Client, Captiva REST Service, and your custom Captiva REST Service authentication plugin.

A custom Captiva REST Service authentication plugin provides more flexibility for authenticating users of the Captiva REST Service. For more information, see the *Captiva Scripting Guide*.
 - b. Create an appropriate location for Captiva REST Service shared data storage and specify it in the Captiva REST Service configuration tool.
 - c. Deploy the Captiva Cloud Capture Toolkit to the machines from which users are to access Captiva Capture Web Client.
 - d. Deploy your custom applications that use the Captiva REST Service.
9. (Required for Captiva Capture Web Client; optional, otherwise) Install the Module Server on a separate machine.
10. 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, refer to [Table 19, page 170](#).

11. (Optional) [Set the UI language for the different Captiva Capture components.](#)
12. Run Captiva Administrator. Configure the Web Services Coordinator and Web Services Hosting components. Refer to the *Using Captiva Administrator* section in the [Administration Guide](#) for details.

Installing the InputAccel Database

The InputAccel Database is an optional component. See [Database Server Considerations](#), page 15 to understand the scenarios under which you will need to install the InputAccel Database.

Before installing the InputAccel 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 InputAccel Database.
- Enable **SQL Server and Windows Authentication** mode in SQL Server Management Studio, and then restart the SQL Server service.



Caution: EMC recommends disabling antivirus software and Data Execution Prevention (DEP), and to close any open programs before installing the InputAccel Database.

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

The *Release Notes* provides more information about supported versions of SQL Server. This document is available from the **Start** menu of your desktop at **All Programs > EMC Captiva Capture > Documentation**.

Note: Due to limitations built into SQL Server Express, it should only be used in low page volume deployments with minimal logging.

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 the InputAccel Database:

1. Start the Captiva 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 InputAccel 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 InputAccel Database** window, select the **Create InputAccel Database** option, specify the SQL Server administrative login credentials for the SQL Server, and then click **Next**.



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:

- Captiva Capture supports only SQL Authentication; therefore, specify a SQL Server login ID to connect to the SQL Server. Furthermore, the account specified when installing the InputAccel Database must have the dbcreator role.
 - If the **Create the InputAccel Database** checkbox is selected, the local **Database Server**, **SQL Server Port**, and Database name must be specified. The **Database name** can only have 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 InputAccel Database installation.)
 - If using a named instance for the SQL Server, be sure to specify the **Database Server** in the format, **[machine_name]\[instance_name]**. For SQL Server Express, the default instance name is **SQLExpress**.
 - If the **Copy Script Only** option is selected, the Database executable and scripts are copied to the target machine but the InputAccel Database is not created. The IADBManager executable must be manually run to create the database. [Appendix H, Running the Database Manager Utility](#) provides instructions for manually creating the InputAccel Database.
7. Click **Install** and then click **Finish**.

Note: The InputAccel Database cannot be installed onto a compressed drive.

8. To verify a successful installation of the InputAccel Database, run SQL Server Management Studio, and expand the **Databases** folder in the **Object Explorer** pane. The InputAccel Database (default name: IADB) should appear in the list of databases.
9. Create a new user account for SQL Server and set permissions for this user account to run the InputAccel Database. [Creating a SQL Server User Account with Minimum Permissions to Access the InputAccel Database, page 47](#) provides the appropriate settings.

Note: You may need to change SQL Server credentials after installing the InputAccel 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. Details of using this utility are in the [Administration Guide](#).

Related Topics —

[Database Server Considerations, page 15](#)

[Chapter 2, Installation Planning](#)

[InputAccel Database Issues, page 160](#)

Creating a SQL Server User Account with Minimum Permissions to Access the InputAccel Database

If the InputAccel 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 InputAccel Server and Client Components installation. 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 user account must use **SQL Server authentication**.
- The **Default database** must be set to the InputAccel Database.
- The user account must be mapped to the InputAccel Database and the database role membership must be set to **Public**.
- Grant the following permissions to the InputAccel Database:
 - **Connect**
 - **Delete**
 - **Execute**
 - **Insert**
 - **Select**
 - **Update**

Related Topics —

[Database Server Considerations, page 15](#)

[Chapter 2, Installation Planning](#)

[Installing the InputAccel Database, page 45](#)

[InputAccel Database Issues, page 160](#)

Installing the InputAccel Server

The InputAccel 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 InputAccel Server must not be longer than 15 bytes; otherwise, client machines will be unable to connect.
- EMC recommends disabling antivirus software and Data Execution Prevention (DEP), and to close any open programs before installing the InputAccel Server.

This procedure installs a single InputAccel Server and documentation.

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.
- Captiva Capture does not install any versions of Microsoft .NET Framework.

To install the InputAccel Server:

1. Start the Captiva 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 InputAccel 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 InputAccel 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 InputAccel 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 InputAccel Database is installed. Information on installing the server in a clustered environment is provided in [To install InputAccel Server on the first cluster node](#); page 72. 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.

**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, refer to the UNC path recommendations in [Installation Errors](#), page 156.
 - If the IAS folder is placed on a network shared drive, then the InputAccel Server must always run under the Local System or an Administrator account.
7. In the **Configure InputAccel 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 InputAccel Server to operate with a least-privileged user account. Details of the LUA configuration can be found in [Running Captiva Capture with Minimum Windows Permissions](#), page 28.



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 “EMC Captiva InputAccel Server” service when the system starts** if you want the InputAccel 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. This is the SQL Server user account created that provides permissions to access the InputAccel Database. Click **Next**.

Note: If the machine where the InputAccel Server is installed also has SQL Server installed, then by default **Register the Data Access Layer with the InputAccel database** is selected and the local database server, default SQL Server port 1433, and Database name are specified.
 9. In the **Configure Captiva Administrator User** window, specify the credentials of a user you want added to the Captiva Capture **Administrator** role. This user does not have to be a Windows Administrator on the server machine, or any other machine. When the InputAccel Server starts, this user is added to the Captiva Capture **Administrator** role and is granted all the permissions to start and use all features of any Captiva Capture component, including Captiva Administrator and all client modules.
 10. By default, **Start the EMC Captiva InputAccel Server service when setup completes** is selected. Clear the checkbox if you want to start the InputAccel 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. If there are any errors during installation, users must check this log file, which is written to the `Server\binnt\iasetenv<timestamp>.log`.

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



Caution:

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

Increasing the Shutdown Period for the InputAccel Server Service

Typically, the InputAccel 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 InputAccel Server service adequate time to shut down. Note that if the InputAccel Server service does not shut down gracefully, it may result in unsynchronized batches and loss of data. This section provides information on increasing the InputAccel Server service shutdown period for supported operating systems.

To understand the issues of shutting down the InputAccel Server in a clustered environment, refer to [InputAccel Server Shutdown in a Clustered Environment](#) in the *Installation Guide*.

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

To increase the InputAccel Server service shutdown time:

1. Login to the InputAccel Server machine as a member of the Windows **Administrators** group.
2. Stop all instances of the InputAccel Server service.
3. Open a command prompt window on the InputAccel 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 InputAccel Server (default: InputAccel). This is the true name of the InputAccel Server service and not its display name.
- **timeout** is a numeric value, representing the maximum time allowed, in minutes, for the InputAccel Server service to shutdown.

Example: **ias64 -repair -s InputAccel -t 25**

5. Start the InputAccel Server service.

Installing the Captiva Capture Client Components

This procedure installs Captiva Capture client modules and the following additional features:

- Captiva Designer and Process Developer
- Captiva Administrator
- Advanced Recognition development tools
- Extraction Engines
- Legacy modules
- Captiva Capture Scripting Libraries
- Web services modules and components

**Caution:**

- EMC recommends disabling antivirus software and Data Execution Prevention (DEP), and closing any open programs before installing the Client Components.
- Make sure that there are no pending Windows updates before you start the Captiva Capture client installer. If there are pending Windows updates, please install them first before starting the Captiva Capture client installer. Additionally, ensure that the machine does not require to be restarted before you begin the client installation.

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.
- Captiva Capture does not install any versions of Microsoft .NET Framework.
- Because of the limited number of printer ports, do not install Captiva Capture client modules and the Module Server on the same machine.

To install Captiva Capture Client Components:

1. Start the Captiva 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 4 - Install Client Components** 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 client modules](#) is installed. Click **Next**.
4. Accept the license agreement and then click **Continue**.
5. Select one of the following setup types, and then click **Next**:
 - **Developer**: Developer features
 - **Production User**: Operator client modules
 - **Unattended Module Server**: Unattended client modules
 - **Custom**: Custom selection of features to install
6. 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**.
Available features are listed in [Appendix C, Client Module Features](#).

Note: Before installing the Image Converter module, the **Print Spooler** service must be running in order to install the **InputAccel Virtual Printer**.

7. The **Required Third-party Software** window displays if third-party software that is required to run the client modules is not already installed. Click **Next** to continue. The specified client modules are installed, but will not run until the required third-party software is installed.
8. Click **Next** to install to the default destination directory or click **Change** to select a new location.
9. Select one of the following to specify a user account to use when logging in to the module:
 - **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 Captiva Capture components are installed on a single system or the InputAccel Server has been configured to allow anonymous access, you must configure the Captiva Capture system to use Kerberos authentication, as explained in [Configuring Captiva Capture to use Kerberos authentication, page 22](#)

- **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.

10. Select **Automatically start all services when the system starts** if you want the Captiva Capture client modules to be started as a service automatically when the system starts, and then click **Next**.



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.

11. In the **InputAccel Server Connection Information** window, specify the **Server name** and **Server port** of the InputAccel Server to connect to. Add a semi-colon (;) after the Server name to connect to a ScaleServer group. By default, **Try to contact the server during this installation** is selected. This option enables the setup program to attempt to establish a connection with the InputAccel Server. Click **Next**.



Caution: If the InputAccel 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 **InputAccel Server Connection Information** window. The non-code page characters may cause installation errors. Instead, proceed as follows:

- Return to the **InputAccel Server Connection Information** window and for the **Server Name** specify the InputAccel Server machine's IP address.
- Proceed with the client installation. The first time you run each client module, specify the correct InputAccel 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, page 98](#).

12. If the connection succeeds, click **Next**. If the attempt fails, verify that the InputAccel Server service is started.

Note: You may proceed with the installation of the client modules even if the server connection does not succeed. Restarting the server is not mandatory.

13. Click **Install** and then **Finish**.

14. If prompted to restart Windows, click **Yes**.

15. Verify that the InputAccel Server service is started on the machine where the InputAccel Server is installed.

16. (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 Captiva Administrator to work properly.

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

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

17. Ensure that the default administrator user logs in to Captiva Administrator, and then assigns appropriate permissions to users and adds users to Captiva 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. Refer to the *Using Captiva Administrator* section of the [Administration Guide](#) for additional information.

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 Captiva Capture component, including Captiva Administrator and all client modules.

18. Verify that the client modules have been installed successfully. Start a client module by clicking **Start > Programs > EMC Captiva Capture**, selecting the module type, and then the module. The module login window displays. Type your InputAccel Server login credentials, and click **OK**.

Related Topics —

[Client Machine Considerations, page 19](#)

[Client Scalability, page 24](#)

[Upgrading Client Modules, page 130](#)

Additional Installation and Configuration Requirements for Image Converter

This section includes the following topics:

- [Installing Multiple Instances of Image Converter, page 53](#)
- [Additional Requirements to Run Image Converter as a Service, page 54](#)
- [Specifying the Temporary Folder for Storing Intermediate Processed Files, page 56](#)
- [Additional Configuration Steps for Processing Files using the Image Converter Module, page 57](#)

Installing Multiple Instances of Image Converter

When Image Converter is installed, the Captiva Capture Virtual Printer is also installed to enable processing of all supported non-image files, except for PDF files. 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 Captiva Capture 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 Captiva Capture Virtual Printer when processing non-image files. This will cause an error and file processing cannot be performed. To use multiple instances of Image Converter simultaneously, manually install additional instances of the Image Converter module as a service. Each service instance is installed with its own virtual printer, and the name of the printer includes the name of the service instance

for easier identification. Thereby, several service instances of the Image Converter module can run independently at the same time.

Note:

- The number of Image Converter instances that can be installed is limited by the number of ports available for their connection.
- Multiple Image Converter instances cannot be configured to use the same port due to port conflicts.

By default, virtual printers connect to Line Printer Terminal (LPT) ports. If all available LPT ports are already used by other devices, the installation of the Image Converter instance is not performed, and you will see the corresponding error message.

Besides the LPT ports, you can use other available ports to connect virtual printers. Using the command line, you can define the required port (for example, one of COM ports) to connect the corresponding virtual printer. To do this, use the **-printerport** command-line parameter when installing Image Converter instance as a service:

-printerport:<PortName>

For example, provide the following command-line when installing Image Converter as a service:

imgconv -install:Image Converter -login:DOM\Administrator,PASS@XX.XX.XX.XX .XXX -printerport:COM1

where

- *imgconv* is the name of the Image Converter .exe file;
- *Image Converter* is the name of the service;
- *DOM\Administrator,PASS@XX.XX.XX.XX* is the string that defines the domain name\login, and password, accordingly, and the IP address of the server you want to log in;
- *COM1* is the name of a port.

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.

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

Note: If the client machine has Microsoft Office 2013 installed, using an administrative user account is a strict requirement.

Note: On Windows 8, Windows 8.1, Windows Server 2012 and Windows Server 2012 R2, 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 folder exists on the client machine:
 - In the 32-bit environment: %SYSTEMROOT%\System32\config\systemprofile\Desktop
 - In the 64-bit environment: %SYSTEMROOT%\SysWOW64\config\systemprofile\Desktop and the %SYSTEMROOT%\System32\config\systemprofile\Desktop

Make sure that the Desktop folder is assigned the **Write** permission for "Everyone".
2. Run the Component Services utility:
 - On 32-bit operating systems: navigate to **Start > Run**. Type **DCOMCNFG** and click **OK**.
 - On 64-bit operating systems: 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 on **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 on 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.

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, 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.

Additional Configuration Steps for Processing Files using the Image Converter Module

These configuration settings are needed in addition to the steps documented in .

This section includes the following topics:

- [Processing HTML Files using Internet Explorer 10 and 11, page 57](#)
- [Processing PDF and Microsoft Office Documents with Security Restrictions, page 58](#)
- [Printing Background Colors for MS Word Documents, page 58](#)
- [Processing Macro-enabled MS Excel Files, page 58](#)

Processing HTML Files using Internet Explorer 10 and 11

1. Disable Internet Explorer 10 and 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, page 56](#).
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}`.

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.

Printing Background Colors for MS Word Documents

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

To enable printing background colors for MS Word Documents:

1. Open the `QuickModuleHost.exe.config` file from `Program Files\InputAccel\Client\binnt` (or `Program Files (x86)` for 64-bit systems) using Notepad.
2. Add the following line between the **appSettings** tags:
`<add key="WordPrintBackgrounds" value="true"/>`

Processing Macro-enabled MS 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 printing background colors for MS Word Documents:

1. Open the `IMGCONV.exe.config` file from `Program Files\InputAccel\Client\binnt` (or `Program Files (x86)` for 64-bit systems) using Notepad.
2. Add the following line between the **appSettings** tags:
`<add key="ExcelMacrosEnabled" value="true"/>`

Note: Enabling macros can result in serious security vulnerability.

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.

Note: Your scanner device may include many advanced features. Captiva Capture may not support every advanced scanner feature that is available with your scanner device.

Note: EMC supports and recommends the ISIS scanner driver standard to seamlessly interface our scanning software with document scanners. Every ISIS driver must pass thousands of rigorous tests to fully validate its performance, compatibility and reliability in order 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. For more information on ISIS-certified devices, see www.scannerdrivers.com.

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.

Activating and Licensing Captiva Capture

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

Refer to the [Administration Guide](#) for details on the server and client licenses required for specific features. Refer to the *Using Captiva Administrator* section of the *Administration Guide* for instructions on security keys and licenses and activating InputAccel Servers. You can proceed to start using it for a limited time while waiting for a response to the activation request.

Related Topics —

[ScaleServer Licensing, page 37](#)

[Licensing for Use in a Microsoft Cluster, page 38](#)

[Licensing for Disaster Recovery, page 38](#)

Licensing the Check Reading Engine:

To license the Check Reading engine:

1. Run the SoftLockViewer utility, `SoftlockViewer2.exe`, (default location: `%QSDIR%\D11\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. Email the saved file to **EMC Activation** 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.

Setting the UI Language of Captiva Capture Components

After successful installation of Captiva 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.

Refer to [Appendix F, Localized Languages](#) for a list of supported UI languages, their language codes, and locale IDs.

Note:

- Performance counters are installed on the InputAccel Server machine and are available in the language of the operating system where they are installed or English.
- Windows Event Log typically displays event logs in the language of the operating system where they are viewed.

Topics in this section include:

- [Specifying Default UI Language Settings, page 61](#)
- [Summary of Options for Overriding the Default UI Language, page 62](#)
- [Procedures to Override the UI Language, page 63](#)

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 to 7.x.

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

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

1. Run the Control Panel on the machine running the InputAccel Server or any client module available prior to InputAccel 6.0. (Modules listed as "Available Prior to 6.0" in [Table 19, page 170](#))
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 F, Localized Languages](#) in Captiva capture. This sets the code page that the InputAccel 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.

- On the **Advanced** tab, select the **Default user account settings** checkbox. This ensures that the changed settings apply for all accounts that are used to run the InputAccel Server or client modules as a service.

To specify the default UI language for client modules new in InputAccel 6.x to 7.x versions:

- Client modules new in 6.x to 7.x versions (modules listed as “New in 6.0 ” and “New in 7.0 - 7.x” in [Table 19, page 170](#)) 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 InputAccel Server and client modules can be overridden. Refer to [Summary of Options for Overriding the Default UI Language, page 62](#) for details.

Summary of Options for Overriding the Default UI Language

The default UI language for the InputAccel 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, page 63](#).

Table 6. Globalization and UI Language Settings for Captiva Capture Components

Captiva Capture component	Globalization settings (for example, date, number, currency formatting) determined by	Default UI language determined by	Default UI language overridden by
InputAccel Server	User’s regional settings	User’s regional settings	Specifying the UI language in the: <ul style="list-style-type: none"> Win.ini file Setscan.ini file
Client modules that were available prior to 6.0 (Modules listed as “Available Prior to 6.0” in Table 19, page 170)	User’s regional settings	User’s regional settings	Specifying the UI language in the: <ul style="list-style-type: none"> Win.ini file Setscan.ini file

Captiva 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 to 7.x	Regional settings of the operating system	Language of the operating system Note: For Captiva 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: <ul style="list-style-type: none"> • Command line argument • settings.ini file • Setscan.ini file • Multilingual User Interface (MUI) Pack

Procedures to Override the UI Language

This section details the steps involved in overriding the default UI language of the InputAccel 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:

1. On the client machine where a module new in version 6.x to 7.x 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 Captiva Capture](#).

Examples (where the ScanPlus module is installed at the default location):

- `"C:\Program Files\InputAccel\Client\binnt\QuickModuleHost.exe" -module:Emc.InputAccel.Scan -language:en-us` (Starts the ScanPlus module with the UI language set to English-United States)
- `"C:\Program Files\InputAccel\Client\binnt\QuickModuleHost.exe" -module:Emc.InputAccel.Scan -language:pt-br` (Starts the ScanPlus module with the UI language set to Portuguese-Brazil)
- `"C:\Program Files\InputAccel\Client\binnt\QuickModuleHost.exe" -module:Emc.InputAccel.Scan -login:honor\johndoe,password99@Baltimore1;bermuda -language:pt` (Starts the ScanPlus module for production connecting to InputAccel Servers "Baltimore1" and "bermuda" with the domain name "honor", the user name "johndoe", the password "password99", and the UI language set to Portuguese).

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 to 7.x 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 Captiva Capture](#).

Examples:

- `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:

1. On the machine where the InputAccel Server or any Captiva Capture client module is installed, open the `setscan.ini` file. The default location is `c:\windows`.
2. 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 Captiva Capture](#).

Examples:

- `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 InputAccel Server or a client module available prior to the InputAccel 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 Captiva Capture](#).

Examples:

- **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. Refer to 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 to 7.x.
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.

Related Topics —

[Appendix F, Localized Languages](#)
[Table 19, page 170](#)

Additional Installation and Configuration Options

This section discusses additional installation and configuration options for the Captiva Capture system. Topics in this section include:

- [Installing Multiple Instances of InputAccel Servers, page 65](#)
- [Configuring Multiple InputAccel Servers as a ScaleServer Group, page 67](#)
- [Installing the InputAccel Server in a Microsoft Failover Clustering Environment, page 69](#)
- [Installing Captiva Capture Web Client and Captiva REST Service, page 78](#)
- [Installing the Module Server, page 87](#)
- [Deploying Modules with the ClickOnce Deployment Utility, page 89](#)
- [Unattended Installations, page 94](#)
- [Manually Registering a Client Module to Run as a Service, page 98](#)

Installing Multiple Instances of InputAccel Servers

Multiple instances of the InputAccel Server can be installed on a single machine (also called a side-by-side installation). A maximum of eight instances of InputAccel Server can be installed;

although in typical installations, one InputAccel 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 InputAccel Server.

Performance benefits of side-by-side installation include:

- Each InputAccel 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 InputAccel Server process. Furthermore, the VBA runtime is loaded only when processes require it.
- Enables Captiva Capture to be installed in an Active/Active clustered environment.

Note:

- Side-by-side installation requires that an InputAccel Database is installed.
- Side-by-side installation is required when installing the InputAccel Server in an Active/Active clustered environment.
- ScaleServer groups normally provide some degree of business continuation in the event of a server failure. 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 the intent is 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 InputAccel Servers:

1. From the **Installation Choices** list, select **Step 2 - Install the InputAccel 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 InputAccel Server on the first cluster node;](#), page 72
3. Choose a custom installation and click **Next**.
4. Select the number of InputAccel Server instances to install, and then click **Next**.
5. For each instance, click **Change** to specify a unique location for data files for each InputAccel Server, and then click **Next**.

Note: Each instance of the InputAccel Server must have its own principal folder. Each instance is installed on its own directory. EMC recommends 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, EMC recommends using the default port for all server instances.
7. The **Configure InputAccel 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 InputAccel 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 InputAccel Database. Click **Next**.

Note: If the machine where the InputAccel Server is installed also has SQL Server installed, then by default **Register the Data Access Layer with the InputAccel 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.

Note:

- If you choose to start the InputAccel Server as a service automatically when the system starts, the setup program configures only the first InputAccel Server instance to automatically start. All other instances of the InputAccel 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 InputAccel 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 InputAccel Servers 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 InputAccel Servers.
 11. To verify that multiple instances of the InputAccel Server are installed correctly:
 - a. Start any module in production mode.
 - b. When logging on, specify one of the InputAccel Servers and make sure the module connects.
 - c. Repeat these steps for each InputAccel Server instance.

Related Topics —

[InputAccel Server Considerations, page 17](#)
[InputAccel Server Scalability, page 23](#)
[Upgrading the InputAccel Server, page 126](#)

Configuring Multiple InputAccel Servers as a ScaleServer Group

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

ScaleServer technology uses a combination of licensing, server configuration parameters, and technology in the InputAccel Servers themselves. To configure a ScaleServer group, obtain a server

license that enables the ScaleServer technology. Refer to the [Administration Guide](#) to learn more about the licensing feature codes for ScaleServer groups.

Note:

- Client modules cannot connect to multiple independent InputAccel 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, refer to [Table 19, page 170](#).
- All InputAccel Servers within a ScaleServer group must access the same InputAccel Database.

To configure a ScaleServer group:

1. Install the required hardware and software on each InputAccel Server machine. Refer to the *Release Notes* for details. This document is available from the **Start** menu of your desktop at **All Programs > EMC Captiva Capture > Documentation**.
2. Install the InputAccel Database software.
3. Install the InputAccel Server software on each server machine.
4. Install Captiva Administrator from the client components setup program.
5. Run the Captiva Administrator module and do the following to configure the ScaleServer group:
 - a. For each installed InputAccel Server, be sure to install and activate the Activation File (CAF file).
 - b. Install valid ScaleServer licenses/feature codes on each InputAccel Server that is to be part of the ScaleServer group.

Note: Feature codes are established when the InputAccel Server license codes are installed. For details on server feature codes, refer to the [Administration Guide](#).

- c. Specify a ScaleServer group name and add a list of InputAccel Servers in the group.
- d. Make sure the same users are in the **InputAccel_Server_admin_group** group on all InputAccel Servers in the ScaleServer group.

Refer to the *Using Captiva Administrator* section in the [Administration Guide](#) for information on activating InputAccel Servers, installing license codes, adding users and groups, and specifying a ScaleServer group.

Note: When users running client modules connect to a ScaleServer group, they must specify the InputAccel 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. Refer to [Table 19, page 170](#) for a list of modules that are ScaleServer-compatible.
 - b. When logging on, select the **Connect to server group** checkbox.
 - c. Run Captiva Administrator and verify that the client module is logged into all servers in the ScaleServer group. Refer to the *Using Captiva Administrator* section in the [Administration Guide](#) for details.

Related Topics —

[InputAccel Server Considerations, page 17](#)

[InputAccel Server Scalability, page 23](#)

[High Availability and Failover, page 33](#)
[Upgrading the InputAccel Server, page 126](#)
[ScaleServer Issues, page 161](#)

Installing the InputAccel Server in a Microsoft Failover Clustering Environment

This section explains how to install InputAccel within Microsoft Failover Clustering.

Note:

- For a list of supported Microsoft Failover Clustering environments, see the *EMC Captiva Release Notes*.
- Captiva Capture has been tested on a Microsoft Failover Clustering cluster of two nodes. Other configurations may work, but are not officially supported.
- Captiva Capture supports one InputAccel Server running in an Active/Passive mode, or two servers running in an Active/Active mode. When two InputAccel Servers are used, they can be configured as a ScaleServer group or they can be used independently.
- For more information about Microsoft Failover Clustering, see technet.microsoft.com.
- Administrators must run the Failover Cluster Manager for all cluster configuration tasks, including defining each virtual server and its failover/failback rules. For more information about the Failover Cluster Manager, see the Microsoft documentation.
- Make sure that the InputAccel Servers have enough time to shut down in a cluster. For more information, see [Step 2](#).

Topics in this section include:

- [Installing InputAccel Servers into Microsoft Failover Clustering, page 70](#)

Requirements for InputAccel Server in Microsoft Failover Clustering

The Microsoft Failover Clustering and InputAccel 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. 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 InputAccel Database is installed on a server other than the InputAccel 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 in order to register the InputAccel Server cluster resource DLLs with the cluster:
 - **Failover Cluster Automation Server**
 - **Failover Cluster Command Interface**

InputAccel Server requirements

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

- Cluster disk for the \IAS data directory.
- Static IP address that clients use to access the InputAccel Server as a clustered application.
 - Windows Server 2008 R2, 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.
- InputAccel 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 InputAccel Server is not supported in the Microsoft Failover Clustering environment.
- A cluster CAF file for each InputAccel Server to be installed into the cluster; for example, for two servers in an Active/Active installation, you must have two CAF files.

Installing InputAccel Servers into Microsoft Failover Clustering

Although these instructions apply to the installation of two InputAccel Servers into an Active/Active cluster, you can still use them for the installation of a single InputAccel Server into an Active/Passive cluster. To use these instructions for installing a single InputAccel 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 InputAccel Servers into Microsoft Failover Clustering:

1. [Set up the cluster environment according to Microsoft and InputAccel Server requirements.](#)
2. [Define the cluster resources.](#)
3. [Verify that both InputAccel Server cluster drives are accessible from the first cluster node.](#)
4. [Install InputAccel Server on the cluster nodes.](#)
5. [Register the InputAccel Server cluster resource DLLs with the cluster.](#)
6. [Move both cluster disks to the second node and install the InputAccel Server on the second cluster node.](#)
7. [Complete the InputAccel Server cluster application configuration.](#)

8. [Complete additional configuration of server parameters in Captiva Administrator.](#)
9. [Activate and license the InputAccel Server in an Active/Active cluster.](#)

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 InputAccel Server installed in the cluster.
As a best practice, create these application resource groups with a single disk resource allocated, then install the InputAccel Server on both cluster nodes, and finally complete the remainder of the configuration by adding the remaining resources of IP address, DNS name, and InputAccel 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 InputAccel Server to be installed. For example, Active/Active requires two dedicated cluster disks.
5. Perform one of the following actions:
 - On Windows Server 2008 R2, right-click **Services and applications**, then select **More Actions > Create Empty Service or Application**. A new application named **New Service or Application** is created.
 - 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 InputAccel Server.
This name is used only for display purposes in the cluster administration user interface.
7. Repeat [Step 5](#) and [Step 6](#) to create a second application (for Active/Active cluster) and rename it to indicate it is the second InputAccel Server.
8. Edit the **Properties** of these new applications/roles to define the preferred owners on each application/role. Typically, the first InputAccel Server should have a preferred owner of node 1, and the second InputAccel 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 **Services and applications** (on Windows Server 2008 R2) or **Roles** (on Windows Server 2012 and 2012 R2), select the application/role, right-click and select **Add Storage**, and select the checkbox for the first InputAccel Server cluster disk (for example, drive R). Repeat the process for the second InputAccel Server application/role if creating an Active/Active cluster (for example, add drive S as the storage on the second InputAccel 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, there is only one application/role and it should be owned by first node.

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

1. Start Windows Explorer.

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

To install InputAccel Server on the first cluster node:

1. On the first node, start the Captiva 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 InputAccel Server** and follow the instructions.
3. In addition to the usual options, select the following options for configuring InputAccel 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 .
Number of InputAccel Server instances	<ul style="list-style-type: none"> • For an Active/Active cluster: 2 • For an Active/Passive cluster: 1
Choose Install Folder	Select a local drive; that is, do not install InputAccel Server application files onto the cluster disk.
Choose Data Files Install Folder	For each InputAccel Server's \IAS data directories, select its associated cluster disk (do not select a local drive).
Configure Cluster Settings	<ul style="list-style-type: none"> • For an Active/Active configuration, enter the following: <ul style="list-style-type: none"> — Two IPv4 addresses and port numbers. For the port numbers, use the same value for both of your InputAccel Servers. — (Optional) Two IPv6 addresses and same port numbers as for the IPv4 addresses. • For an Active/Passive configuration, enter the following: <ul style="list-style-type: none"> — The IPv4 address and port number. — (Optional) The IPv6 address and same port number as for the IPv4 address. <p>Note:</p> <ul style="list-style-type: none"> • The IPv4 addresses that you enter are static addresses, which are dedicated for use

Option	Action
	<p>only by each InputAccel Server application. These addresses are not the same ones that are used by the cluster nodes themselves.</p> <ul style="list-style-type: none"> 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 InputAccel Service Accounts	You can specify the user account under which the InputAccel 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.
Automatically start the EMC Captiva InputAccel Server service when the system starts	Deselect this option. The service startup mode for the InputAccel Server services must be set to Manual when running it in a cluster.
Start the EMC Captiva InputAccel Server service when setup completes	Deselect this option. The InputAccel Server should not be started outside of the cluster control.

To register the InputAccel Server cluster resource DLLs with the cluster:

- On one node, in a command prompt (running as Administrator), execute the following file for each InputAccel Server:

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

where <Server#> is the directory for each InputAccel Server.

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

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

- To ensure that the InputAccel 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, InputAccel 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 InputAccel Server on the second cluster node:

1. In **Failover Cluster Manager**, under **Services and applications** (on Windows Server 2008 R2) or **Roles** (on Windows Server 2012 and 2012 R2), move the InputAccel Server applications to the second node.
All InputAccel Server applications in the cluster must be owned by the second node.
Note: There is only one application/resource group for Active/Passive cluster.
2. On the first node, stop the Failover Cluster Manager application.
3. To install InputAccel Server on the second node, repeat the [To install InputAccel Server on the first cluster node](#);, page 72 procedure.

To complete the InputAccel 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 InputAccel Server's IP address and Network Name.
 - For Windows Server 2008 R2, under the console tree in the left pane, under **Services and applications**, right-click the InputAccel Server application and select **Add a resource > Client Access Point**.
 - For Windows Server 2012 and 2012 R2, under the console tree in the left pane, select **Roles**, and then right-click each InputAccel Server role and select **Add a resource > Client Access Point**.

Enter the following information:

- **Name:** The Network Name (hostname) by which this InputAccel Server is accessed over the network by client modules and Captiva Administrator.
- **Address:** Enter the static IPv4 address that is used to access this InputAccel Server. This is the same address which you entered during InputAccel 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 on the **Name** resource and select **Properties**.
- Under the **Dependencies** tab, if there are 2 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 InputAccel Server, write down the address. It can be manually entered through the Captiva Administrator module at a later time.
- Repeat these steps for the second InputAccel Server if installing Active/Active.

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

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



Caution: A message The resource type Add InputAccel is not configured on all nodes. Do you wish to continue and create the resource? indicates the InputAccel Servers are 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 InputAccel Server: <ul style="list-style-type: none"> • Cluster disk • Name
Policies	Until the InputAccel Server is fully licensed and operational, EMC recommends changing 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 InputAccel resource online.

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

6. For an Active/Active cluster installation, repeat all these steps to configure the second InputAccel Server, but use a different name and static IP address, and select the resource type as **InputAccel2**.
7. Verify that you can move each InputAccel 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 InputAccel 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 Captiva Administrator:

1. Install Captiva Administrator on a separate machine.
2. Make both InputAccel Servers online simultaneously on different nodes. In the case of Active/Passive cluster, bring the InputAccel Server online on either node.
3. Log in to any of the InputAccel Servers using the Captiva Administrator module.
4. Navigate to the **Systems** pane and click on **View Servers**. You should see the two InputAccel Servers (or in the case of Active/Passive cluster, just one InputAccel 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 on each of the InputAccel 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 InputAccel 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 InputAccel 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 InputAccel 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 InputAccel Servers. If no changes were made, you do not need to restart the InputAccel Servers.

To activate and license the InputAccel Servers on both cluster nodes:

To activate and license the InputAccel Server in a cluster, you must activate each InputAccel Server twice, once for each node in the cluster using the Activation IDs received from EMC.

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

1. Run Captiva 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 InputAccel 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 InputAccel Servers display an activation state of **Initial Grace Period**.

Note:

- You cannot use the same CAF file for both servers in an Active/Active cluster environment.
 - To activate the InputAccel Server in an Active/Passive cluster environment, you require a single activation (CAF) file that provides the **Server ID** for the single InputAccel Server. You also require two **Profile IDs**. To activate the InputAccel Servers in an Active/Active cluster environment, you require two activation (CAF) files that provide two **Server IDs** for the two InputAccel Servers. You also require four **Profile IDs**. To obtain these Profile IDs, each InputAccel 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 Captiva 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 InputAccel Server to the other node. Now repeat steps 6–7 and obtain the second set of Serial Numbers and Profile IDs.
 10. In the **Server Activations** page in Captiva Administrator, select the **Online InputAccel Server Activation** link, or go to <http://activation.captivasoftware.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 from EMC, you can activate the InputAccel Server for each node. Run Captiva 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 InputAccel Server Profile ID, and then click **OK**. The **State** column for the server displays “Activated”.
 14. Repeat steps 12–13 for the second InputAccel Server.
 15. Run Failover Cluster Manager to move each InputAccel Server to the other node.
 16. Repeat steps 10–14 to activate the InputAccel Servers on the other node.
 17. Use the Failover Cluster Manager to move the InputAccel Server applications to the other node again and verify that they remain activated in Captiva Administrator. In Active/Active cluster, move the InputAccel 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.

Installing Captiva Capture Web Client and Captiva REST Service

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

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

Prerequisites —

- Captiva Capture client applications, such as Captiva Capture Web Client and custom applications, require the Captiva REST Service.
- Captiva Capture Web Client requires the following additional Captiva Capture components:
 - InputAccel Server
 - Module Server

Note:

- No load-balancing is inherently performed among multiple instances of Captiva REST Service in a Web farm.

Procedure

If you want to configure pass-through login in Captiva Capture Web Client, see [Configuring Pass-Through Login in Captiva Capture Web Client, page 85](#) before starting this procedure.

1. Install Captiva Capture Web Client and Captiva REST Service on the first IIS machine in the Web farm, by running the Captiva Capture setup program and on the **Installation Choices** list and selecting **Step 2 - Install Web Components > Captiva CWC and REST** and following the instructions.

Note:

- Both Captiva Capture Web Client and Captiva REST Service use the same IP address and port; however, they use different contexts in their URLs.
 - Even if the specified TCP port is in use by an existing IIS website (for example, the built-in IIS default website), the Captiva REST Service and Captiva Capture Web Client Web site is still created. However, you must stop the existing Web site and start the Captiva REST Service and Captiva Capture Web Client one instead.
 - If you are installing Captiva Capture Web Client and Captiva REST Service in a production environment, do not start Captiva Capture Web Client and the Captiva REST Service immediately; otherwise, users might inadvertently access an incomplete configuration.
2. On the first machine only, configure settings that apply to all Captiva REST Service Web sites in the entire Web farm by selecting **Start > EMC Captiva Capture> REST Service Config** and following the instructions.

To change the current configuration settings, select the shared data folder. The current configuration settings are loaded from the shared configuration file.

Note: In the Captiva Capture installation directory, you can also run `WebComponents\binnt\CaptivaRestServerConfig.exe`.

- **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.

If you are running multiple instances of Captiva 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 session timeout value specified for Captiva REST 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: $500 * 10MB * 20 = 100 \text{ GB}$.

- **Web Server**

- **Custom Base Address:** (Optional) Specifies a Web server's URL to use as absolute links in the JSON response. The default is the default URL supplied by the Web server. 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.
- **Maximum InputAccel Server Connections:** The maximum number of simultaneous connections from the Web server to the InputAccel Server.
- **Session Timeout (Minutes):** The timeout for user sessions. If you do not want them to time out, specify a very large number.
- **InputAccel 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 user perform the following:
 - Assign a Windows user account on Captiva REST Service's Web server so that their Windows access token can be used to validate their permissions on the InputAccel Server.
 - Assign a Captiva role that provides at least the following permissions:

```
Server.Login  
Server.Create.Batch  
System.BatchRead  
System.BatchModify  
System.ProcessRead
```

Note: The user's Windows user account must be in a domain that the Web server trusts.

- **Custom:** Use your own custom authentication plugin. Your custom authentication plugin must return roles that would provide at least the following Captiva permissions:

```
Server.Login  
Server.Create.Batch  
System.BatchRead  
System.BatchModify  
System.ProcessRead
```

For more information, see the *Captiva Scripting Guide*.

- **Central Authentication Service:** Use Jasig Central Authentication Service (Jasig CAS) for Captiva Capture Web Client. For more information, see [Configuring the Jasig Central Authentication Service](#), page 85.
- **Module Allocation Timeout (Seconds):** The maximum number of seconds that a Captiva REST Service request waits to be processed by a Module Server service instance.
- **InputAccel Server**
 - **Server:** The InputAccel Server host name (or IP address).
 - **Connect to server group:** Specifies to connect to a ScaleServer group; otherwise, Captiva REST Service only connects to the specified InputAccel Server.
 - **User and Password:** An InputAccel Server user name (which is also a Windows domain user) and password. The format for the user name is *DOMAIN\username*. Specify * (asterisk) to use the Web server's Windows user account.
- **Service Modules**
 - **Instance Count:** Maximum number of instances to run on a single machine.
 - **Recycle in Hours:** Number of hours after which an instance is restarted.
 - **Debug Trace:** Whether to enable debug tracing.

Tip: At this time, you could configure this IIS instance as instructed in [Step 4](#) before installing and configuring Captiva Capture Web Client and Captiva REST Service on other IIS instances in the Web farm.

3. Install Captiva Capture Web Client and Captiva REST Service on every other IIS machine in the Web farm by running the Captiva Capture setup program and on the **Installation Choices** list and selecting **Step 2 - Install Web Components > Captiva CWC and REST** and following the instructions.
4. 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 `cp-rest` context, 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 Captiva REST Service Web sites associated with the same shared data storage. By default, Captiva 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 Captiva REST Service authentication plugin.
 - 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`

Captiva 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 `Captiva Administrators` role so that it has the necessary permissions on the InputAccel Server.
 - c. Configure the SSL certificate and HTTPS binding in the **IIS Management Console** by adding these bindings in **Sites > Captiva CWC and REST Service > Actions > Bindings**.

Note: Do not block any **HTTP Verbs** under **Request Filtering**.
 - d. Configure Captiva Capture Web Client by setting the following **Application Settings** for the `cp-cwc` context:
 - **CloudCaptureUrl** – (optional) the URL to the location of the Cloud Capture Toolkit runtime.

The Cloud Capture Toolkit runtime must be installed on each browser machine. If the browser machine does not have the Cloud Capture Toolkit runtime installed, then a message with this URL is displayed to the user.
 - **RestServiceURL** – the URL to the Captiva REST Service Web site.

Note: If you specify `localhost` in the URL, then Captiva Capture Web Client is only accessible in a browser running on the same IIS machine.

5. License Captiva Capture Web Client and Captiva REST Service.

Captiva REST Service client (including Captiva Capture Web Client) and Module Server licensing is managed through the Captiva REST Services Licensing tool.

For more information about the Captiva REST Services Licensing tool, see the [Administration Guide](#).

6. (Optional) On each browser machine, run the Cloud Capture Toolkit runtime installer.

Copy the Cloud Capture Toolkit runtime installer from the following path on the installation media:

CCT2.0\RuntimeInstaller\setup.exe

Note: The Cloud Capture Toolkit runtime must be installed on each browser machine. If you do not install the Cloud Capture Toolkit runtime on each browser machine, then specify a location from which users can download it in **CloudCaptureUrl** (see [Step d](#)).

7. (Optional) To set the general amount of noise that can be on an otherwise blank page for it to still be considered blank, specify the *DirtyLevel* setting as follows:

- a. In the IIS <host-name>\Sites\Captiva CWC and REST Service\cp-cwc > **Application Settings (Features View)**, create the *DirtyLevel* setting.
- b. For the *DirtyLevel* setting, assign a value as follows:

Value	Description
0	To be considered blank, the page must be pristine white; that is, no noise is tolerated.
1	(Default) To be considered blank, the page can be dirty white; that is, some noise is tolerated.
2	To be considered blank, the page can be very dirty white; that is, a lot of noise is tolerated.
3	To be considered blank, the page can have a single line on it.
4	To be considered blank, the page can have two lines on it.

Note:

- You must log back into any Captiva Capture Web Client that was already running.
- An exact number of non-white pixels is not used to determine a tolerance; rather, each choice attempts to approximate realistic conditions.

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

For more information, see [Localizing and Rebranding the Captiva Capture Web Client User Interface](#), page 83.

9. (Optional) Configure a Jasig CAS (Central Authentication Service) server for single sign-on with Captiva Capture Web Client.

For more information, see [Configuring the Jasig Central Authentication Service](#), page 85.

Localizing and Rebranding the Captiva Capture Web Client User Interface

You can localize Captiva 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 Captiva 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 Captiva Capture Web Client page, as well as customize a message that is displayed when the required version of the Cloud Capture Toolkit is not installed on the browser machine (and if the **CloudCaptureUrl** in **Application Settings** is not configured).

Localized and branding strings are contained in locale-specific resource files. When Captiva 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 Captiva 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 Captiva Capture Web Client as follows:

Language	Locale Code
English (Default)	<code>en-US</code>
Chinese (Simplified)	<code>zh-CN</code>
French	<code>fr</code>
German	<code>de</code>
Italian	<code>it</code>
Japanese	<code>ja-JP</code>
Korean	<code>ko-KR</code>
Portuguese (Brazilian)	<code>pt</code>
Russian	<code>ru</code>
Spanish (Spain)	<code>es</code>

Related Topics —

- [Creating Resource Files, page 84](#)

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 Captiva Capture Web Client or for new locale resource files that you create.

- **A locale resource file**

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

Locale-specific file name and default path — C:\inetpub\captiva\cp-cwc\strings*<language>*-*<country>*.js

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

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:

- Only the key-value pairs specified in the default locale resource file, *en-US.js*, can be localized using the Captiva Capture Web Client localization mechanism.
- The fallback locale file is C:\inetpub\captiva\cp-cwc\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.

- **A branding string override resource file**

Description — 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-cwc\strings (default path).

Locale-specific file name and default path — C:\inetpub\captiva\cp-cwc\branding\strings*<language>*-*<country>*.js

<code><language></code>	An ISO 639, two-letter, lowercase language code.
<code><country></code>	An ISO 3166, two-letter, uppercase country code. Note: If <code><country></code> 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-cwc\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-cwc\branding\strings\en-US.js` (default path).

Configuring Pass-Through Login in Captiva Capture Web Client

You can configure pass-through login in Captiva Capture Web Client for Windows domain users.

The following restrictions apply:

- Only Internet Explorer 10 or greater is supported.
- Only an intranet is supported.
- Proxy servers are not supported.
- All client browser machines, the IIS Web server, and InputAccel Server must all be on the same Windows domain and have full access on it.
- The hostname in the URL provided to the client browser must be the same as the one in the Captiva 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.

- In order 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 Captiva permissions for the Captiva Capture Web Client browser users.

Configuring the Jasig Central Authentication Service

Captiva REST Service supports the Jasig CAS (Central Authentication Service) server for single sign-on with Captiva Capture Web Client only; that is, no other Captiva REST Service clients (custom, Captiva Mobile SDK, or otherwise) are supported with the Jasig CAS server. For more information about Jasig CAS, see <http://jasig.github.io/cas>.



Caution: Because the Captiva Capture Web Client login dialog that is displayed upon session timeout does not work with CAS, the user must log out completely and log back in resulting in the loss of the current batch. Therefore, you should set the session timeout for Captiva Capture Web Client to an acceptable length of time. You set the session timeout in the **Session Timeout** field on the **Web Server** tab of the Captiva REST Server Configuration tool.

Note:

- In most cases, the Jasig CAS server is installed on a machine other than the one on which Captiva REST Service is installed.
1. Enable Jasig CAS by using **Start > EMC Captiva Capture > REST Service Config** to set **Web Server > Authentication Mode = Central Authentication Service**.
 2. In the Captiva REST Service shared data folder, create a `cas.config` text file containing name-value pairs (using the `parameter=value` syntax) as follows:

Note: If a CAS-authenticated user is specified neither in *AdminUsers* nor in *Users* (either explicitly or using *), then no privileges on the InputAccel Server and Captiva REST Services are provided to that user; however, that user can still access other Captiva REST Services that do not require any privileges.

Parameter	Description
<i>CasServerUrl</i>	(Required) The URL to the CAS server; for example: <code>https://captiva.example.org:8080/cas</code>
<i>LaunchUrls</i>	(Required) A comma-separated list of URLs that CAS can use to launch an application after successful authentication. The Captiva Capture Web Client and the Captiva REST Service Licensing tool URLs must be specified. If CAS attempts to launch a URL that is not specified in this parameter, then CAS authentication fails.
<i>AdminUsers</i>	(Optional) A pipe-delimited () list of CAS-authenticated users for whom to grant the <code>Admin</code> privilege for Captiva REST Services. The <code>Admin</code> privilege allows a user to perform the following actions: <ul style="list-style-type: none"> • View and add Captiva REST Services licenses using the Captiva REST Service Licensing tool. • Use the Captiva Capture Web Client, create batches for the InputAccel Server, and view CaptureFlows and Distributed Scan profiles.

Parameter	Description
	<p>An example of valid syntax is the following:</p> <pre>CapAdmin SysMgr SA</pre> <p>Note: The user that logs in to the Captiva REST Service Licensing tool must be granted the <code>Admin</code> privilege for the Captiva REST Service.</p>
<i>Users</i>	<p>(Optional) A list of CAS-authenticated users who are allowed to use the Captiva Capture Web Client, create batches for the InputAccel Server, and view CaptureFlows and Distributed Scan profiles.</p> <p>Valid values are as follows:</p> <ul style="list-style-type: none"> • A pipe-delimited () list of users. • * (an asterisk) that represents all users. <p>An example of valid syntax is the following:</p> <pre>JohnS WendyM MarthaV</pre>

Installing the Module Server

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

Note:

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

1. For each instance, run the Captiva Capture setup program and on the **Installation Choices** list, select **Step 4 - Client Components** and follow the instructions.

For **Data Folder**, specify the shared data folder. All instances of the Module Server and Captiva REST Service must specify the same shared data folder. For more information, see [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 services, select **Start > EMC Captiva Capture > REST Service Config** and make changes on the following tab:
- Service Modules**
- **Instance Count:** Maximum number of instances to run on a single machine.
 - **Recycle in Hours:** Number of hours after which an instance is restarted.
 - **Debug Trace:** Whether to enable debug tracing.
3. By default, virtual printers (for example, **InputAccel Virtual Printer**) are added and configured for the Image Converter service. For scalability, you can add additional Image Converter services. Each Image Converter service must have its own virtual printer. To add virtual printers, execute \Client\binnt\VirtualPrinterInstaller.exe as follows:

```
VirtualPrinterInstaller.exe -printersToInstall:<integer value> | -printerPort:<Printerport>
| -uninstall
```

where:

<code>-printersToInstall:<IntegerValue></code>	<p>Specifies the number of virtual printers to install in <IntegerValue>. The maximum number of printers installed is equal to the number of available LPT ports. For example, to install 3 virtual printers, specify the following:</p> <pre>VirtualPrinterInstaller.exe -printersToInstall:3</pre> <p>The virtual printers are named as follows:</p> <pre>InputAccel Virtual Printer - <integer></pre> <p><integer> is an integer that is appended for the second and subsequent virtual printers.</p>
<code>-printerPort:<PrinterPort></code>	<p>Specifies the particular port to which to install a virtual printer in <PrinterPort>. For example, to install a virtual printer that uses COM1:</p> <pre>VirtualPrinterInstaller.exe -printerPort:COM1</pre>
<code>-uninstall</code>	<p>Uninstalls all except for one InputAccel virtual printer, just in case it is required by the Image Converter service.</p>

Deploying Modules with the ClickOnce Deployment Utility

Captiva Capture includes these web-deployable client modules: ScanPlus and RescanPlus. Captiva Capture also includes a ClickOnce Deployment Utility that provides administrators with an alternate method to deploy these modules. The utility copies the necessary programs and application files to a the web server or network file share based on the environment. Depending on the parameters set by the administrator, prerequisite software is installed on the client machine during deployment, and updates are automatically downloaded and installed as necessary. This enables administrators to install and maintain software for users in distributed locations.

Prerequisites

- Acquire a valid SSL certificate in PFX format for the application that is deployed using the ClickOnce Deployment Utility. Administrators can use any authorized Signing Authority (VeriSign, for instance) for acquiring the SSL certificate.
- You must have ClickOnce publishing skills and ClickOnce technology know-how before choosing a ClickOnce deployment strategy.
- If the ClickOnce application is to be deployed to a website and downloaded using a URL, use the IIS Manager snap-in feature of the Microsoft Management Console to configure the web server as follows for each installation package:
 - For each installation package, deployed through ClickOnce, create a virtual directory under the Captiva Capture Web Components website.
 - For each of the virtual directories created, set the Virtual Directory Access Permissions to “Read”, “Run Scripts (such as ASP)”, and “Write”. Do not enable “Execute” permissions.
 - For each of the virtual directories created, configure the Security settings so that the connecting user (for example, the Internet Guest Account user) has Read, Write, and Modify permissions set to “Allow.”
 - Under **IIS Web Service Extensions**, change the WebDAV Service Extension **Status** field from **Prohibited** to **Allowed**.
 - Before deploying to a web server, read the prerequisites described in <http://learn.iis.net/page.aspx/350/installing-and-configuring-webdav-on-iis/>. After following these instructions, ClickOnce deployable modules can be uploaded to any WebDAV Server or web server.

Note:

- You cannot deploy the applications directly by HTTP protocol. Instead, deploy these modules to a Windows network file share using the procedure described in [Workaround for Deploying ClickOnce Modules on a Windows Network File Share](#), page 93.
- If deploying ScanPlus, RescanPlus, or IndexPlus on a 64-bit operating system, use the procedure described in [Workaround for Deploying ClickOnce Modules on a 64-bit Operating System](#), page 93.

To deploy modules with the ClickOnce utility:

1. Install the ScanPlus ClickOnce Package, RescanPlus ClickOnce Package, and IndexPlus ClickOnce Package from the client installer.

2. Select **Start > Programs > EMC Captiva Capture > Tools (Standard) > ClickOnce Deployment Utility** to run the ClickOnce Deployment Utility on the machine where the packages have been installed. The **Deploy InputAccel Application** window displays.
3. Select an application to deploy, and supply a URL where application support can be obtained:
 - a. Select **Application** from the navigation panel. The **Application Options** pane displays.
 - b. Select the ClickOnce application to deploy from the **Select an application to deploy** list box.
 - c. Under **Provide application deployment options**, select the options appropriate for the deployment. Also, accept the default values for the options selected or provide the values applicable:
 - **Publish version:** Version of the deployed application.
 - **Publisher:** Name of the organization deploying the module.
 - **Product:** The name of the deployed module.

Support URL: The URL where support information for the module resides. The default location is <http://www.emc.com/captiva>.
4. Set the parameters for deployment:
 - a. Select **Deployment** from the navigation panel to display the **Deployment Options** pane.
 - b. Under **General deployment options**, select the options appropriate for the deployment. Also, accept the default values for the options selected or provide the values applicable:
 - **Application URL:** The URL or network file share that is used to access the ClickOnce application. The URL should not include the deployment manifest name. For example, if the URL is set to `http://server/virtualdirname` for the ScanPlus application, the ClickOnce utility writes `http://server/virtualdirname/ScanPlus.application` to the deployment manifest.
 - **Installation URL:** The URL or network file share where the application files are copied. If this parameter is not specified, the files are copied to the Application URL.
 - **Use a “.deploy” file name extension:** Select to add a “.deploy” extension to application files. This value is set to **Yes** by default.
 - **Allow URL parameters to be passed to the application:** Select to enable query strings to be passed to the application. This parameter is set to **Yes** by default. This parameter ensures that the deployed application (accessed by the application URL) can be run by users in setup mode.
 - c. Under **Choose installation mode**, select the options appropriate for the installation of the application. Also, accept the default values for the options selected or provide the values applicable:
 - **The application is only available online:** Select to make the application available from the location specified in the **Application URL** field.
 - **The application should be installed locally:** Select to make the application available from the Windows **Start** menu. The application can then be uninstalled from the Windows **Control Panel**.



Caution: Setting this parameter to **No** prevents the application from running in setup mode or passing login information.

5. (Optional) Specify options that determine how often the module checks for updates, the location where updates can be obtained, and the base version of the application to use when checking for available updates:

Note:

- Automatic updates can only be scheduled for local installations.
- If the automatic update feature is enabled, the ClickOnce application periodically reads its deployment manifest file to check for updates. If an update is available, the new version of the application is downloaded.

- a. Select **Update** from the navigation panel. The **Update Options** pane displays.

Note: The **Update Options** pane is available only when an application is deployed locally. If the installation mode is set to **The application is only available online** on the **Deployment Options** pane, a warning displays a **Modify deployment options...** link. Click this link to return to the **Deployment Options** pane. Select **The application should be installed locally** option to enable the **Update Options** pane.

- b. From the **Update Options** pane, select the options appropriate for the deployment.
 - **The application should check for updates:** Select to ensure that the application checks for updates based on the frequency and version specified.
 - **Choose when the application should check for updates:** Select the appropriate option so the module checks for updates either before or after starting.
 - **Choose how often the application should check for updates:** Specify how often the module should check for updates.
 - **Specify URL from which the application updates should be downloaded:**
Type the complete URL where the application resides and where updates can be obtained. The URL should include the deployment manifest name. For example, `http://server/virtualdir/ScanPlus.application` for the ScanPlus module.
 - **Specify a minimum required version for the application which can updated:** Specify a base version of the application to be used for updates. You must enter a minimum version number which is a version number higher than the version currently installed.

6. (Optional) Create a bootstrap installation program for installing prerequisites required by the module being deployed. This is selected by default. This enables automatic installation of module prerequisites as part of the deployment process:

- a. Select **Prerequisites** from the navigation panel. The **Prerequisites and Bootstrap Options** pane displays.
- b. Select the options appropriate for the deployment:
 - **Create setup program to install prerequisite components:** Select to create a bootstrap installation program that installs prerequisite components as part of the deployment process.
 - **Specify the install location for prerequisites:** Select a location where the prerequisite components reside. This location can be a vendor's website, the same location as the application being deployed, or any other accessible location. To specify a URL or file path, select the **Download prerequisites from this location** option, and type a valid path in the associated field.

Note:

- Administrator rights may be needed for users to install prerequisites.
 - If the client machine does not have the Visual C++ Runtime prerequisite installed, the module fails to connect to the InputAccel Server.
7. Specify how the application should sign the deployment manifest. Signing can be done from a password protected file, or from a stored certificate, and can be associated with a timestamp to reduce issues that might be encountered if a certificate used for signing has expired.
 - a. Select **Signing** from the navigation panel. The **Deployment Manifest Signing Options** pane displays.
 - b. Under **Choose how to sign the deployment manifest** area, select from the following options:
 - **Sign the deployment manifest with this certificate file**
 - In the **File** field, type the file name and location for the certificate file, or click the **Browse** button to browse to the correct file.
 - In the **Password** field, type the password for the certificate file, if necessary.
 - **Sign the deployment manifest with a stored certificate:**
 - In the **Certificate:** field, type the name and path of the stored certificate, or click the **Select** button to select a certificate stored on the local system.
 - c. In the **Timestamp URL:** field, type the URL of a supported time stamping service to populate the certificate with a current time and date during the publishing process. When a published application's certificate expires, the time stamp service can be called upon by the client to verify whether the application was signed while the certificate was still valid, enabling the expired certificate to remain in use.
 8. If the ClickOnce application is deployed to a website and downloaded using a URL, be sure the necessary prerequisites and permissions have been configured as explained under [Prerequisites, page 89](#).
 9. Click the **Deploy** button to deploy the selected application with the selected settings.
 10. Provide the URLs, IP addresses, or **Share name** of the deployment that users need to install the applications. Examples of the URL that user should run to install ClickOnce applications:
 - **http://server/virtldir/ScanPlus.application** (in case no bootstrap installer was created)
 - **http://server/virtldir/ScanPlusSetup.exe** (in case bootstrap installer was created)
 - **\\server\dirname\IndexPlus.application** (in case of deployment to network share)
 11. To verify that the ClickOnce modules are deployed correctly, click the link provided in the **Deployment successfully finished** window.

If the deployment fails, the ClickOnce Deployment Utility displays a message indicating the error that occurred. The following most likely errors are due to incorrect configuration of items listed in [Prerequisites, page 89](#):

 - (401) Unauthorized: This error will occur if the virtual directory permissions are not set correctly.
 - (404) Not Found: This error will occur if the virtual directory properties grant the user full Execute permissions. Change the permissions to Execute Scripts Only.

- (501) Not Implemented: This error will occur if the WebDAV Web Service Extension is not set to “Allowed.”
- (503) Server Unavailable: This error will occur if deployment is performed onto a machine with the 64-bit operating system. See [Workaround for Deploying ClickOnce Modules on a 64-bit Operating System, page 93](#) for a workaround.

Workaround for Deploying ClickOnce Modules on a Windows Network File Share

Deploying ScanPlus or RescanPlus directly by HTTP protocol is not supported. Instead, deploy these modules to a Windows network file share using the ClickOnce Deployment Utility.

To deploy ClickOnce modules to a Windows network fileshare:

1. On the web server, create a Windows network file share and a virtual directory.
2. When deploying the modules using the ClickOnce Deployment Utility, specify the virtual directory HTTP path in the **Application URL** field. This is the URL required to access the modules.
3. Specify the Windows network file share in the **Installation URL** field. This is the location where the application files are copied.
4. Complete the remaining deployment steps previously listed in [Deploying Modules with the ClickOnce Deployment Utility, page 89](#).

Related Topics —

[ClickOnce Host System Considerations, page 18](#)

Workaround for Deploying ClickOnce Modules on a 64-bit Operating System

If deploying ScanPlus, RescanPlus, or IndexPlus on a 64-bit operating system, either make sure you [deploy the modules to a Windows network file share](#) or that you configure IIS to start 32-bit worker processes.

To configure IIS to start 32-bit worker processes:

1. Open a command window and type `CSCRIPT %SYSTEMDRIVE%\Inetpub\AdminScripts\adsutil.vbs SET W3SVC/AppPools/Enable32bitAppOnWin64 1`.
2. Restart the Application Pool.
3. Complete the remaining deployment steps previously listed in [Deploying Modules with the ClickOnce Deployment Utility, page 89](#).

Related Topics —

[ClickOnce Host System Considerations, page 18](#)

Unattended Installations

The Captiva 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 Captiva 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.

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

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

Refer to the [Command line instructions](#) section for examples of command lines that silently install or upgrade Captiva Capture.

This section includes the following topics:

- [Understanding Installation Command Line Arguments, page 94](#)
- [Command Line Considerations, page 96](#)
- [Installing Captiva Capture from a Command Line, page 96](#)
- [Automating Unattended Installations, page 97](#)
- [Modifying Unattended Installations, page 97](#)

Understanding Installation Command Line Arguments

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

Table 7. Captiva 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 Captiva Capture Microsoft Installer (MSI) files reside: <ul style="list-style-type: none">• Databases\setup.exe: Installs the SQL database.• Server\setup.exe: Installs the InputAccel Server.

Argument	Description
	<ul style="list-style-type: none"> • Clients\setup.exe: Installs the Captiva Capture client modules. • WebComponents\setup.exe: Installs Captiva Capture Web Client and Captiva REST Service.
/s	InstallShield argument that executes a silent setup.
/v	<p>InstallShield argument that passes command line options and values of public properties to msiexec.exe.</p> <p>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:</p> <pre>setup.exe /v"/l*v "c:\temp\logfile.txt"</pre> <p>/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.</p>
/l	InstallShield argument that creates a log file that can be used to troubleshoot installation issues.
Msiexec.exe arguments	<p>Specifies an installer action: For example:</p> <ul style="list-style-type: none"> • /i: Install. • /f: Repair. • /x: Remove. <p>Note: The /i argument is the default and does not need to be specified.</p>
Windows Installer properties	Specifies an installer action.
Features to install	<p>Installs the specified Captiva Capture features. For example, the following command line installs an InputAccel Server:</p> <pre>setup.exe /s /v"/qn ADDLOCAL="ALL" SERVER _INSTANCES="1" IA_SERVICES_RUNAS_LOCAL_SYSTEM="1" /promptrestart"</pre>

Related Topics —

[Supported InstallShield Switches, page 189](#)

[Supported MSI Switches, page 190](#)

[Supported Windows Installer Properties, page 190](#)

Command Line Considerations

There are some important issues to consider when installing Captiva Capture from a command line.

Escape Characters

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

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\"
```

Another issue to consider are characters that require escaping by the Windows command prompt. The ampersand (&) symbol must be escaped using a caret (^) character. For example:

```
SCANNERNAME=\"Canon DR-4580U ^& DR-5580U\"
```

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.

Related Topics —

[Captiva Capture Installer Properties and Feature Names, page 190](#)

[Command-line Installation Failures, page 157](#)

Installing Captiva Capture from a Command Line

Use the InstallShield and Windows Installer command line arguments to create instructions to install Captiva Capture software:

To install Captiva 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 Captiva Capture features. For example, to install one InputAccel 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 Captiva Capture features using a batch file that contains silent installation command line instructions.

Related Topics —

- [Command-line Installation Failures, page 157](#)
- [Supported InstallShield Switches, page 189](#)
- [Supported MSI Switches, page 190](#)
- [Supported Windows Installer Properties, page 190](#)
- [Captiva Capture Installer Properties and Feature Names, page 190](#)

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:

```
//Begin contents of irr_spl.bat batch file
//Install Service Pack 1 and write log file
setup.exe /s /v"/qn ADDLOCAL="ALL" IA_SERVICES_RUNAS_LOCAL_SYSTEM="1" /l*v
"C:\logs\spl_install.log"

//Remove COPY features and write a log file
setup.exe /v"/qn REMOVE="COPY" /l*v "C:\logs\spl_remove.log"

//Repair features and write log file
setup.exe /v"/qn /fvomus /l*v "C:\logs\spl_repair.log"
//End contents of irr_spl.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.

Related Topics —

- [Command-line Installation Failures, page 157](#)
- [Supported Windows Installer Properties, page 190](#)
- [Captiva Capture Installer Properties and Feature Names, page 190](#)

Modifying Unattended Installations

From the directory location of the base Captiva 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. Refer to the examples detailed in the [Supported Captiva Capture feature properties and names](#) section.
- **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 Captiva 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 Captiva Administrator module to delete an InputAccel Server or remove an InputAccel Server from a ScaleServer group before removing the server. Refer to the *Using Captiva Administrator* section in the [Administration Guide](#) for additional information.

- **Repairing a Captiva 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\spl_repair.log"
```

Related Topics —

[Supported InstallShield Switches, page 189](#)

[Supported MSI Switches, page 190](#)

[Supported Windows Installer Properties, page 190](#)

[Captiva Capture Installer Properties and Feature Names, page 190](#)

[Command-line Installation Failures, page 157](#)

Manually Registering a Client Module to Run as a Service

By default, Captiva 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 in order to change the login parameters.

Not all modules can run as services. For a list of client modules that can run as services, refer to [Table 19, page 170](#).

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.x” in [Table 19, page 170](#):

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

- Modules that are listed as “New in 6.x” in [Table 19, page 170](#), 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 [Table 19, page 170](#) (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 [Table 19, page 170](#):

```
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 InputAccel 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 InputAccel Server to which the module should connect when running as a service. The topic [Running Modules as Services, page 20](#) 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 [Table 19, page 170](#).
- **-loginex:username,password@repository** are the credentials used by a custom export module to log into a third-party repository.

Note:

- 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 [Table 19, page 170](#) 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 Captiva 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 Captiva 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.

Related Topics —

[Chapter 2, Installation Planning](#)

[Client Machine Considerations, page 19](#)

[Client Scalability, page 24](#)

[Installing the Captiva Capture Client Components, page 50](#)

[Upgrading Client Modules, page 130](#)

[Appendix B, Captiva Capture Client Modules](#)

Unregistering Client Modules that are Registered as Services

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

To unregister a client module that is 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.x” in [Table 19, page 170](#):

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

- Modules that are listed as “Available Prior to 6.0” in [Table 19, page 170](#):

```
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.)

Related Topics —

[Chapter 2, Installation Planning](#)

[Client Machine Considerations, page 19](#)

[Installing the Captiva Capture Client Components, page 50](#)

[Upgrading Client Modules, page 130](#)

[Appendix B, Captiva Capture Client Modules](#)

Installing Captiva Capture in a Development or Demonstration Environment

This section describes an installation where all Captiva Capture 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.

The following table summarizes the configuration for a single machine installation:

Table 8. Development or Demonstration Installation

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

To install Captiva Capture on a single machine:

1. Make sure the machine meets the system requirements outlined in the *Release Notes*. This document is available from the **Start** menu of your desktop at **All Programs > EMC Captiva Capture > Documentation**. For the best performance, always use the vendor's latest operating system (that EMC supports) for all Captiva 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 Captiva 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 Captiva Capture system.
2. Make sure the locale, globalization, and code page settings are specified as detailed in [Locale Considerations](#), page 14.
3. (Optional) [Install the InputAccel Database components](#) and then [Create a SQL Server user account with minimum permissions to access the InputAccel Database](#).
4. [Install the InputAccel Server components](#).
5. [Install the Captiva Capture client components](#).
6. [Activate the InputAccel Server and install the Captiva Capture licenses](#).
7. [Set the UI language for Captiva Capture components](#).

Upgrading Captiva Capture

This section explains how to upgrade an existing system.

Topics in this section include:

- [Upgrade Planning, page 103](#)
- [Upgrading from 6.0 SP3 and 6.5.x to 7.5, page 123](#)
- [Upgrade Procedures, page 124](#)
- [Sample Upgrade Scenarios, page 133](#)
- [Migration Guidance, page 137](#)

Upgrade Planning

Upgrading requires careful planning and execution. This section explains how to plan for an upgrade.

Upgrade planning includes the following:

- Understanding the valid upgrade paths ([Upgrade Paths, page 104](#)).
- Understanding the compatibility between the various components ([Understanding Compatibility among Captiva Capture Components, page 104](#)).
- Understanding the locale considerations before planning an upgrade ([Understanding Locale Considerations before Planning the Upgrade, page 108](#)).
- Identifying irreplaceable files to archive ([Identifying Irreplaceable Files, page 109](#)).
- Identifying new system requirements and obtaining new equipment as needed ([Identifying New System Requirements, page 113](#)).
- Understanding the upgrade process ([Understanding the Upgrade Process, page 113](#)).
- Granting permissions so users can use the upgraded system ([Permissions, page 121](#)).
- Performing pre-production testing and acceptance ([Performing Pre-Production Testing and Acceptance, page 122](#)).
- Scheduling upgrade phases ([Scheduling Upgrade Phases, page 122](#)).

Upgrade Paths

Customers can upgrade from the following versions only. 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 [Chapter 3, Installing Captiva Capture](#).

- Captiva Capture 7.1
- Captiva Capture 7.0
- InputAccel 6.5 SP2
- InputAccel 6.5 SP1
- InputAccel 6.5
- InputAccel 6.0 SP3

Note: Dispatcher for InputAccel is no longer available as a separate product. Dispatcher functionality is now integrated into Captiva Capture. For client upgrades, the supported upgrade path is determined by a combination of the current version of InputAccel and Dispatcher for InputAccel. The allowed combinations are:

- InputAccel 6.0 SP3 and Dispatcher for InputAccel 6.0 SP3
- InputAccel 6.5 and Dispatcher for InputAccel 6.5
- InputAccel 6.5 SP1 and Dispatcher for InputAccel 6.5 SP1
- InputAccel 6.5 SP2 and Dispatcher for InputAccel 6.5 SP2

Related Topics —

[Identifying New System Requirements, page 113](#)

[Understanding the Upgrade Process, page 113](#)

[Understanding Compatibility among Captiva Capture Components, page 104](#)

Understanding Compatibility among Captiva Capture Components

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

Captiva 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 InputAccel Server 7.5 until you want to upgrade them. The specific versions that can connect to an InputAccel Server 7.5 are shown in [Client Upgrade Compatibility](#) table. The InputAccel Server refuses connections from clients of any other version. Version 7.5 client modules cannot connect to InputAccel 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, page 108](#).

The versions of the following components must be the same:

- The InputAccel Database (if installed), InputAccel Server, and all four components of the InputAccel 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 7.5 version level before client modules are allowed to connect to the 7.5 server.
- All client modules that are installed on a single physical machine (including modules deployed using the ClickOnce Deployment Utility) must be the same version. For example, InputAccel/Dispatcher 6.0 SP3 client and InputAccel/Dispatcher 6.5 SP2 client modules cannot run together on the same machine.



Caution: If you modify a process with version 7.5 setup data or create a new 7.5 process, you can only use this process with 7.5 modules; that is, you cannot use this process with any previous version modules in either setup or production mode. Furthermore, you must not perform any module setup using 7.5 modules or create any new version 7.5 processes until all components have been upgraded to 7.5.

Table 9. Client Upgrade Compatibility with InputAccel Server

InputAccel Client version	Connects to Upgraded InputAccel Server version 7.5?	Connects to New InputAccel Server version 7.5?	Can be upgraded to version 7.5?
6.0	No	No	No
6.0 SP1/SP2	No	No	No
6.0 SP3	Yes (1, 2)	Yes (2)	Yes
6.5			
6.5 SP1			
6.5 SP2			
7.0	Yes (3)	Yes (3)	Yes
7.1	Yes (3)	Yes (3)	Yes

Note: The following notes correspond to the numbers in parentheses in the table:

1. Server and client must be in the same locale and use the same single-byte code page. (East Asian code pages are not supported.)
2. Versions 6.0 SP3, 6.5, 6.5 SP1, and 6.5 SP2 client modules can connect only to a 7.5 server (upgraded or new installation) with an upgraded external database; that is, these client modules cannot connect to a 7.5 server with a newly installed external or internal database; in this case, these client modules must be upgraded to 7.5 in order to connect to the 7.5 server.
3. Versions 7.0 and 7.1 client modules can connect to a 7.5 server (upgraded or new installation) if the 7.5 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 7.5 database must also be external). Furthermore, the external or internal database can be either an upgraded or new installation.

Captiva REST Services

Captiva REST Services versions are as follows:

- Captiva REST Services 1.0
 - Released with Captiva Capture 7.1.
 - Includes the Captiva REST Service Web application.
 - Clients that use Captiva REST Services 1.0 are completely compatible with InputAccel Servers 7.1 and 7.5.
 - Clients that use Captiva REST Services 1.0 are Mobile SDK 1.0 and 1.1 clients and custom applications.
- Captiva REST Services 2.0
 - Released with Captiva Capture 7.5.
 - Includes the Captiva REST Service Web application that runs on Microsoft IIS.
 - Includes the Module Server Windows service.
 - Clients that use Captiva REST Services 2.0 are completely compatible with both InputAccel Servers 7.1 and 7.5.
 - Clients that use Captiva REST Services 2.0 are Captiva Capture Web Client and custom applications.

Custom Modules

It is a best practice for custom modules to use the latest SDK; however, modules can also run with an earlier SDK as follows:

Table 10. Running Custom Modules with an Earlier SDK

Dependency	Running on Pre-7.5 Machine	Running on 7.5 Machine
InputAccel SDK 5.x (IAClient32.dll)	Although a custom module should work as-is on a Captiva Capture client version that is interoperable with InputAccel Server 7.5, it is neither guaranteed nor supported.	Migrate to use a .NET Code module step with scripting.

Dependency	Running on Pre-7.5 Machine	Running on 7.5 Machine
InputAccel SDK 5.x (.NET 1.1) (InputAccel.QuickModule.dll)	Although a custom module should work as-is on a Captiva Capture client version that is interoperable with InputAccel Server 7.5, it is neither guaranteed nor supported. Note: .NET 1.1 can only run on Windows Vista or lower.	Replace the .NET 1.1 dependency with .NET 4.5.2 and your InputAccel.*.dll references with InputAccel.*35.dll and then rebuild. For more information, see MSDN: Migrating from the .NET Framework 1.1 .
.NET 3.5 Compatibility Pack for InputAccel SDK 5.x (InputAccel.QuickModule35.dll)	Although a custom module should work as-is on a Captiva Capture client version that is interoperable with InputAccel Server 7.5, it is neither guaranteed nor supported.	Update in one of the following ways: <ul style="list-style-type: none"> • Replace the .NET 3.5 dependency with .NET 4.5.2 and rebuild. • Modify the configuration file (<customModule>.exe.config) to point to .NET 4.5.2 runtime. Note: An example file is <inputaccel-client-install>\Client\binnt\APConExp.exe.config.
InputAccel SDK 6.0 (.NET 2.0) InputAccel SDK 6.5 (.NET 3.5) Captiva Capture 7.0 - 7.1 (.NET 3.5) (QuickModuleHost.exe -welcomodulename:<customModule>)-	Works as-is on a Captiva Capture client version that is interoperable with InputAccel Server 7.5.	Update in one of the following ways: <ul style="list-style-type: none"> • Replace the .NET 3.5 or .NET 2.0 dependency with .NET 4.5.2 and rebuild. • Your custom module might run as-is under .NET 4.5.2. You can determine if it can by executing the following command: <pre><inputaccel-7.5 -client-install> \Client\binnt\ QuickModuleHost.exe -modulename: <customModule></pre>

Understanding Locale Considerations before Planning the Upgrade

A pure Captiva Capture version 7.5 system (all components and modules upgraded to version 7.5) 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 InputAccel Servers upgrade the client modules to version 7.5.
- 6.0 SP3 client modules can only process tasks containing multiple languages within the single-byte (non East Asian) code page of their host machine. Furthermore, the InputAccel Server refuses connections from these client modules if they are not set to the same locale, globalization, and code page settings as the InputAccel Server.
- If using modules that were developed by your own software developers or EMC Consulting, 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 Captiva 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 InputAccel Server that is using different locale formatting than the client. To successfully continue using custom modules, be sure that they connect to an InputAccel 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 InputAccel 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 InputAccel 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 InputAccel 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 MDFs 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 InputAccel 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 compiled process can be run on InputAccel 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: Refer to the [Administration Guide](#) for details of the multiple language feature in Captiva Capture.

Related Topics —

[Upgrade Paths, page 104](#)

[Understanding Compatibility among Captiva Capture Components, page 104](#)

[Identifying New System Requirements, page 113](#)

[Understanding the Upgrade Process, page 113](#)

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 11. Irreplaceable Files and Data

Data Type	Host location	Default File Location	Notes
Activation files	InputAccel 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 EMC Consulting may have customized MDF files. Retain these files for future maintenance.
Integrated ProcessFlow Project source files	Process Developer machines	C:\program files\inputaccel\client\src\ipp*.ipp client\src\ipp\dia	Your developers or EMC Consulting may have created or customized IPP files. Retain these files for future maintenance.
Captiva Capture System files	Captiva Designer machines	C:\Users\<username>\My Documents\Captiva <version>\Default	This directory is the working directory for Captiva Designer. It includes configuration settings for Captiva Designer as well as files for Captiva Capture systems such as Captureflows (XPPs), profiles, document types, and scripting.

Data Type	Host location	Default File Location	Notes
settings.ini	Client machines	C:\ProgramData\EMC\ InputAccel \Settings.ini	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 Table 19 , page 170.
Batches and stage files	InputAccel Servers	C:\ias\batches*.*	All in-process data (images, intermediate files, and other batch data). Each InputAccel 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	InputAccel 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 InputAccel Servers within a ScaleServer group should contain an identical set of processes; therefore, archiving a single server should be sufficient.
Dispatcher Project Files		InputAccel\Client\Supporting Files\dia\6.5.x\Project Samples	

Data Type	Host location	Default File Location	Notes
Supplemental module configuration files	InputAccel 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	InputAccel Servers	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InputAccel\Parameters	You or EMC Consulting may have modified server registry values to tune performance. Check each server to determine if multiple archives are necessary.

Automatic Backup during Upgrade

When upgrading the InputAccel 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 there is no possibility of returning to the previous version.

Table 12. 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 InputAccel Server files.
C:\Program Files\ InputAccel\Client	\$InputAccelClient<version>	Files that were used in previous versions to restore a previous version of InputAccel client files.

Related Topics —

[Upgrade Paths, page 104](#)

[Understanding Compatibility among Captiva Capture Components, page 104](#)

[Identifying New System Requirements, page 113](#)

[Understanding the Upgrade Process, page 113](#)

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 may not be suitable for Captiva Capture 7.5. 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 EMC supports) for all Captiva 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 Captiva 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 Captiva Capture system.



Caution: Upgrade customers may require higher performing hardware due to the new features. Make sure you test your environment to ensure you have adequate performance.

Note: As always with any upgrade, please go to www.scannerdrivers.com to make sure your scanner will still be supported in the new environment.

Related Topics —

- [Identifying Irreplaceable Files, page 109](#)
- [Understanding the Upgrade Process, page 113](#)
- [Performing Pre-Production Testing and Acceptance, page 122](#)
- [Scheduling Upgrade Phases, page 122](#)
- [Migration Guidance, page 137](#)
- [Upgrading from 6.0 SP3 and 6.5.x to 7.5, page 123](#)

Understanding the Upgrade Process

When upgrading, install or upgrade the following components in this order:

1. (Required for users upgrading from 6.0 SP3, 6.5.x, 7.0, or 7.1 customers that installed an external database.) InputAccel Database hosted by SQL Server ([InputAccel Database, page 113](#))
2. InputAccel Servers ([InputAccel Servers, page 114](#))
3. Captiva Capture Web Client and Captiva REST Services ([Captiva REST Services, page 115](#))
4. Upgraded client modules ([Existing Clients, page 116](#))
5. New client modules ([New Client Modules, page 121](#))
6. New security keys, licenses, and activation files, as needed ([Licenses, Activation Files, and Security Keys, page 115](#))

InputAccel Database

Users upgrading from 6.0 SP3, 6.5.x, 7.0 and 7.1 versions must upgrade their version of the InputAccel Database (if installed). With the exception of development and demonstration systems, the

InputAccel Database should be installed on a dedicated server that meets or exceeds the performance criteria to keep the Captiva Capture system at peak production capacity. System requirements and recommendations for the InputAccel Database host system can be found in the *Release Notes*. For the best performance, always use the vendor's latest operating system (that EMC supports) for all Captiva 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 Captiva 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 Captiva Capture system.

Related Topics —

[Installing the InputAccel Database, page 45](#)

[InputAccel Database Issues, page 160](#)

InputAccel Servers

Regardless of which version you are upgrading, InputAccel Servers must be upgraded. Furthermore, upgrade customers must ensure that the InputAccel 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 EMC supports) for all Captiva 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 Captiva 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 Captiva Capture system.

For more information about upgrading InputAccel Servers in Microsoft Failover Clustering, see [Upgrading InputAccel Server in a Microsoft Failover Clustering Environment, page 127](#).



Caution: For existing customers, be aware that hardware requirements have increased due to increased functionality. Refer to [InputAccel Server Considerations, page 17](#) for more information related to server requirements for better performance.

For all upgrade scenarios, if you have configured multiple InputAccel Servers as a ScaleServer group, the ScaleServer group is maintained during the upgrade procedure. Upgrade each InputAccel Server in the ScaleServer group, and then confirm that it is configured as needed by using Captiva Administrator. Refer to the *Using Captiva Administrator* section in the [Administration Guide](#) for details.

Note:

- 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 InputAccel 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 InputAccel Server to this group, enabling the InputAccel Server to

operate with a LUA. Details of the LUA configuration can be found in [Running Captiva Capture with Minimum Windows Permissions](#), page 28



Caution: When upgrading a ScaleServer group that has one or more InputAccel 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.

Captiva Administrator

For customers upgrading from 6.0 SP3 and 6.5.x versions: on a system where previously client modules and the Administration Console web server were installed on the same machine, Captiva Administrator is installed as a client module and replaces the previous web-based Administration Console.

Note:

- The Administration Console is no longer supported and cannot connect to the InputAccel Database.
- Use Captiva Administrator to perform all administrative tasks. Although the Administrator Console may continue to work for some administrative tasks, it does not support the new features and capabilities. For example, use Captiva Administrator to define roles and permissions and to take advantage of the reporting and logging functionality.

Related Topics —

[ClickOnce Host System Considerations](#), page 18

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.

Note: As of Captiva Capture 7.5, hardware security keys have been deprecated.

Related Topics —

[ScaleServer Licensing](#), page 37

[Licensing for Use in a Microsoft Cluster](#), page 38

[Licensing for Disaster Recovery](#), page 38

Captiva REST Services

You only need to upgrade Captiva REST Services if you want to use the following new product or feature:

- Captiva Capture Web Client
- The new Ad Hoc services feature that was introduced in Captiva REST Services 2.0

To upgrade Captiva REST Services:

- Run the Captiva Capture installer to install the Captiva Capture Web Client and Captiva REST Service on the same machines that Captiva REST Service is currently installed.

See [Upgrading Captiva REST Services, page 129](#).

- (Optional) Install the Module Server, which is required for Captiva Capture Web Client and Ad Hoc services.

See [Installing the Module Server, page 87](#).

Note: You could also install the new Captiva Capture Web Client and Captiva REST Service on different machines and still maintain the existing Captiva REST Services 1.0 installation.

Existing Clients

New client modules are provided as replacements for legacy modules ([Appendix D, New and Legacy Modules](#)). Also, some modules are no longer shipped ([Appendix E, Modules and Components No Longer Shipped](#)).

The following table lists modules that require special upgrade considerations.

Note: The user Help files for legacy modules are removed after an upgrade.

Note: As always, with any recognition engine upgrade, EMC cannot guarantee that the performance, accuracy and behavior will match the previous version. It is recommended that these changes be tested thoroughly and settings be optimized for your environment before deploying.

Table 13. Client Module Upgrade Issues

Module	Upgrade issue
Classification Edit	<p>Classification Edit must be at the same version level as its associated modules:</p> <ul style="list-style-type: none">• Classification• Extraction• Captiva Designer (and hence, Recognition Designer) <p>In addition, the recognition project file (DPP) in the recognition project shared directory must have been saved and deployed by the same version of Captiva Designer/Recognition Designer.</p> <p>Note: If the aforementioned modules were upgraded to version 7.5, then the Classification Edit module must also be upgraded to the version 7.5 legacy Classification Edit module (that is, the legacy module installed by the Captiva Capture 7.5 installer).</p>

Module	Upgrade issue
East Euro / APAC OCR	<p>The East Euro / APAC OCR module no longer supports the following settings:</p> <ul style="list-style-type: none"> • Automatic Print Type format. • Remove all formatting and Editable copy from the Retain Layout list • Microsoft Word from the Format list <p>After an upgrade, processing a batch configured to use an of these settings will fail. You will need to reconfigure the batch or process to use supported settings. Review the <i>East Euro / APAC OCR Guide</i> for more information on the supported settings.</p>
NuanceOCR	<ul style="list-style-type: none"> • 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 <p>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 <i>NuanceOCR Guide</i> for more information on the supported settings.</p> <ul style="list-style-type: none"> • As announced in Captiva 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.
Recognition Designer	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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
6.0 SP3 and 6.5.x modules deployed using Click Once Deployment Utility	<p>If you enabled automatic updates through the Update Options feature and created a bootstrap installation program for installing prerequisites required by the ClickOnce-deployed modules, note the following:</p> <p>When you redeploy these modules due to an upgrade:</p> <ul style="list-style-type: none"> • New prerequisites are not downloaded and installed when ClickOnce automatically asks you to upgrade the modules to 7.5. • ClickOnce upgrades only the modules themselves, and not the prerequisites. • You must manually start the upgraded bootstrapper utility to download and install the updated prerequisites.
Pre-7.0 customers: Captiva Designer is installed when a client machine that has Process Developer or CaptureFlow Designer installed upgrades to version 7.5	<p>After the upgrade completes, both Captiva Designer and Process Developer reside on the machine. Start using Captiva Designer to create new processes using the graphical-based CaptureFlow Designer, create various profiles, setup modules, and so on.</p> <p>Refer to the Captiva Designer Guide for details.</p> <p>To modify pre-7.5 processes in Captiva Designer 7.5, you must upgrade them; furthermore, once you have upgraded them, you cannot modify them in earlier versions of Captiva Designer.</p> <p>Note: You are prompted to upgrade pre-7.5 processes when you open them in Captiva Designer 7.5.</p> <p>Refer to Upgrading Process Developer Processes, page 141 and Migrating Process Developer Processes to Captiva Designer, page 138 for migration guidance.</p>
Administration Console web component from 6.0 SP3 and 6.5.x versions is no longer installed. Instead, Captiva Administrator is installed as a client module and includes all the functionality of the previous Administration Console	<p>After the upgrade completes, Captiva Administrator is installed and replaces the previous web-based Administration Console. The previous version of Administration Console is no longer supported and cannot connect to the InputAccel Database. As part of the upgrade, users can install Captiva Administrator on any client machine.</p>
Client Script Engine from version 6.0 SP3 upgrades to .NET Code version 7.5	<p>Scripts written in Client Script Engine must be refactored so that they provide equivalent functionality in the .NET Code module.</p>
Image Divider from version 6.0 SP3 upgrades to Image Converter version 7.5	<p>After the upgrade completes, Image Converter replaces Image Divider.</p>

Module	Upgrade issue
Image Converter from 6.5.x versions is replaced by Image Converter version 7.5	<p>After the upgrade completes, the 7.5 version of Image Converter replaces the 6.5.x version. The new module has the same Module ID as the module it replaces. The same MDF file, processes, and batches can be used. If users have a 6.5.x version process containing the Image Converter step, then both the 6.5.x and 7.5 version Image Converter can process tasks. However, when the process is upgraded to 7.5, then all Image Converter clients must also be upgraded to 7.5</p> <p>Refer to Migrating to Use Updated Image Converter, page 148 for migration guidance.</p>
Email Import Multi-Directory Watch	As of 7.5, these modules have been replaced with the Standard Import module.
Pre-7.0 customers: Automatic Quality Assurance ECM Web Services Importer Configuration iManage WorkSite Server Export PrimeOCR Plus Excel Graphing 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 may use the ODBC Export module to export statistics to a database.
Pre-7.0 customers: File System Export Image Export Index Export PDF Export Values to XML	<p>As of 7.5, these modules are no longer shipped and are replaced with Standard Export.</p> <p>Refer to Migrating to Use Standard Export, page 148 for migration guidance.</p>

Module	Upgrade issue
Pre-7.0 customers: Image Image Enhancement	As of 7.5, these modules are no longer shipped and are replaced with Image Processor. Refer to Migrating from Image Enhancement to Image Processor, page 147 for migration guidance.
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. Refer to Migrating from Dispatcher Validation to the Completion Module, page 144 , Migrating from Image Quality Assurance to the Completion Module, page 142 and Migrating from IndexPlus and Dispatcher Recognition to Completion and Extraction, page 142 for migration guidance.
Pre-7.0 customers: Dispatcher Recognition	As of 7.5, Dispatcher Recognition is no longer shipped and has been replaced by Extraction. Refer to Migrating from IndexPlus and Dispatcher Recognition to Completion and Extraction, page 142f or migration guidance.
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
Custom modules and process code	<i>Custom modules</i> using the <code>IDateTime</code> class and the <code>IADateTime</code> MDF value must be modified to use the <code>.NET DateTime</code> object and recompiled. The MDFs for these modified modules must be modified to use the <code>Date</code> MDF type in place of the <code>IADateTime</code> . These constructs were both deprecated in the 6.0 SP2 release and are completely removed as of the 6.5 release. No EMC-supplied modules are affected by this change; the only potential impact is to custom modules that were designed with InputAccel Software Development Kit (SDK) release 6.0 SP1/SP2.
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. Review the Captiva Designer Guide for more information.

[Appendix B, Captiva Capture Client Modules](#) 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.

Related Topics —

[Client Machine Considerations, page 19](#)

[Client Scalability, page 24](#)

[Upgrading Client Modules, page 130](#)

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 InputAccel Client setup program also updates all client components.

Related Topics —

[Client Machine Considerations, page 19](#)

[Client Scalability, page 24](#)

[Upgrading Client Modules, page 130](#)

[Appendix B, Captiva Capture Client Modules](#)

Permissions

There are several system **Roles** with permissions available after an upgrade. The Captiva Capture **Administrator** can assign users and groups to these roles without creating new ones. The Captiva Capture administrator may, if required, define additional user roles, possibly additional Administrator roles, and assign appropriate users to each of those roles. The minimum Captiva 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. Refer to the *Using Captiva Administrator* section in the [Administration Guide](#) for more information about permissions and user roles.

Related Topics —

[Security, page 25](#)

[Understanding the Upgrade Process, page 113](#)
[Scheduling Upgrade Phases, page 122](#)

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 InputAccel 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 [Administration Guide](#).

Related Topics —

[Identifying Irreplaceable Files, page 109](#)
[Understanding the Upgrade Process, page 113](#)
[Migration Guidance, page 137](#)
[Upgrading from 6.0 SP3 and 6.5.x to 7.5, page 123](#)

Scheduling Upgrade Phases

After completing upgrade testing and acceptance, carefully schedule each phase of the production system upgrade. Consider each of 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 EMC Support.

Related Topics —

[Identifying Irreplaceable Files, page 109](#)
[Understanding the Upgrade Process, page 113](#)
[Upgrading from 6.0 SP3 and 6.5.x to 7.5, page 123](#)

Upgrading from 6.0 SP3 and 6.5.x to 7.5

The InputAccel Database, InputAccel Server, and client modules from InputAccel 6.x versions can be upgraded. If you do plan to upgrade, then the InputAccel Database and InputAccel Server must also be upgraded.

Not all client modules need to be upgraded. For more information, see [Understanding Compatibility among Captiva Capture Components, page 104](#).

Note: Uninstalling an upgraded component removes the component from the machine; it does not restore to the earlier version of the component.

To upgrade:

1. If either of the following applies, you must complete all tasks from in-process batches through the affected modules prior to upgrading:
 - After upgrading, one or more modules will use a different code page.
 - You are using a custom module that reads or writes binary IA Values.
2. Stop all client modules that are run as applications and services.
3. Stop all instances of the InputAccel Servers.
4. Stop the InputAccel Database.
5. Archive irreplaceable files and data. Refer to [Identifying Irreplaceable Files, page 109](#) for a detailed list of the files and data that must be archived.
6. Only for users that added custom modules in previous versions of CaptureFlow Designer: Backup the `modules.xml` file and copy the contents of the file to `src\MDF\User\UserModules.xml`. See *Adding Custom Modules to the Steps Panel* in the [Captiva Designer Guide](#) for more information.
7. Upgrade the InputAccel Database. Refer to [Upgrading the InputAccel Database, page 125](#) for instructions.
8. Upgrade the InputAccel Server. Refer to [Upgrading the InputAccel Server, page 126](#) for instructions.
9. Run the client setup program on the Administration Console host machine to automatically upgrade this component. After the upgrade is complete, Captiva Administrator is installed.

Note: Administration Console is no longer supported and cannot connect to the InputAccel Database.
10. Optionally upgrade the Captiva Capture client modules and install new ones.

For more information, see [Upgrading Client Modules, page 130](#).

Note:

- Modules that are no longer shipped are removed.
 - These three Web Services components must be the same version. Therefore, when upgrading client modules, make sure these web services components are also upgraded. These client components are:
 - WS Input
 - WS Coordinator
 - WS Hosting
 - If 6.0 SP3, 6.5, 6.5 SP1, or 6.5 SP2 client modules are currently installed, then these client modules work as-is without needing to be upgraded, subject to the considerations explained in [Understanding Locale Considerations before Planning the Upgrade](#), page 108.
11. (Optional) Upgrade or migrate existing processes and customizations.
For more information, see [Migration Guidance](#), page 137.
 12. Set the UI language for the various Captiva Capture components. Refer to [Setting the UI Language of Captiva Capture Components](#), page 61 for detailed information.
 13. (Optional) Review the new features to determine whether to upgrade existing XPP process files.
For more information, see [Upgrading Existing CaptureFlow Designer XPP Processes](#), page 131.

Related Topics —

[Identifying New System Requirements](#), page 113
[Understanding the Upgrade Process](#), page 113
[Understanding Compatibility among Captiva Capture Components](#), page 104
[Upgrade Paths](#), page 104
[Migration Guidance](#), page 137

Upgrade Procedures

This topic describes the procedures to upgrade each component. The following topics are included:

- [Upgrading the InputAccel Database](#), page 125
- [Upgrading the InputAccel Server](#), page 126
- [Upgrading InputAccel Server in a Microsoft Failover Clustering Environment](#), page 127
- [Upgrading Captiva REST Services](#), page 129
- [Upgrading Client Modules](#), page 130
- [Upgrading ClickOnce-Deployed Applications](#), page 131
- [Upgrading Existing CaptureFlow Designer XPP Processes](#), page 131
- [Upgrading Existing Scripts](#), page 132
- [Upgrading Documentum Advanced Export Client-Side Scripting](#), page 132

Upgrading the InputAccel Database

Upgrading the InputAccel Database involves replacing the current version of the InputAccel Database with the new version. This procedure is applicable for users upgrading from 6.x versions. This procedure does not apply for customers upgrading from InputAccel 7.0 or 7.1 customers that did not install the InputAccel Database—if they wish to use the InputAccel Database, they must first install it using instructions in [Installing the InputAccel Database, page 45](#).



Caution: Before attempting an upgrade of the InputAccel Database in a production environment, we recommend creating a backup of the InputAccel Database, copying the backup to a separate development or test environment, and then testing the upgrade steps. If the database fails to upgrade, restore the original backup into the development environment, identify and resolve the errors, and attempt to upgrade again. After a successful upgrade on the development environment, perform the upgrade on the production environment.

To upgrade the InputAccel Database:

1. Create a backup of the InputAccel Database and copy the backup to a separate development or test environment.
2. Shut down all client modules and the InputAccel Remoting Server.
3. Shut down all InputAccel Servers connected to the InputAccel Database.
4. Log off any other applications running against the database.
5. Install any SQL Server service packs or upgrades as required, then make sure the SQL Server service is started. Refer to the *Release Notes* for the InputAccel Database requirements. This document is available from the **Start** menu of your desktop at **All Programs > EMC Captiva Capture > Documentation**.
6. From the **Installation Choices** list of the InputAccel setup program, select **Step 1 - Install the InputAccel Database**.
7. A message appears, verifying that the database components installed on the machine must be upgraded to the latest version. Click **Yes** to upgrade.
8. If prompted to install prerequisite applications, click **Install**. Click **Next**.
9. Accept the license agreement and click **Continue**.
10. In the **Destination Folder** window, click **Next** to install the database and scripts to the default destination folder or click **Change** to select a new location.
11. In the **Configure InputAccel Database** window, select the **Upgrade InputAccel Database** option, specify the DB owner account login credentials for SQL Server, and then click **Next**.
12. If the specified database exists, a message prompts you to confirm the upgrade. Click **Yes**.
13. Click **Install** and then click **Finish**.

Upgrading the InputAccel Server

Upgrading the InputAccel Server involves replacing current versions of all InputAccel Servers with the new version.



Caution: For all upgrade customers, be aware that hardware requirements have increased. Refer to [InputAccel Server Considerations, page 17](#) for more information related to performance.

This procedure is required for all upgrade scenarios.

To upgrade the InputAccel Server:

1. Make sure the server machine meets the InputAccel 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 InputAccel Server on a different operating system and then migrate your current InputAccel Server configuration to the new InputAccel Server. For more information about the operating system upgrade procedure, see [Microsoft TechNet](#).
2. Record the version numbers of the InputAccel Servers. The version number is displayed in the **Properties** window of the InputAccel Server executable. The version number is required if you need to revert to a previously installed version of InputAccel Server.
3. Disconnect all client modules. Use the Administrator module, the Administration Console, or Captiva Administrator to view the list of InputAccel Server connections and then disconnect all client modules.
4. Stop the InputAccel Servers. If the InputAccel 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 InputAccel Server. For more information, see [Automatic Backup during Upgrade, page 112](#).

6. For InputAccel Server 6.x, 7.0, and 7.1 with the InputAccel Database, install or upgrade the InputAccel Database before upgrading the InputAccel Server.
7. Run the setup program with an account that has Administrative privileges. From the **Installation Choices** list, select **Step 2 - Install the InputAccel Server**.
8. Upgrade the InputAccel Servers. Refer to [Installing the InputAccel Server, page 47](#) for instructions.

If you are installing a new InputAccel Server on a different operating system, then copy the backup of the \IAS data directory tree to the new InputAccel Server before starting the InputAccel 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 InputAccel Server and license keys. For more information, see the [Administration Guide](#).

Related topics —

[InputAccel Server Considerations, page 17](#)
[InputAccel Server Scalability, page 23](#)
[Installing the InputAccel Server, page 47](#)
[ScaleServer Issues, page 161](#)

Reverting Back to a Previously Installed Version of the InputAccel Server

In some situations, you may want to revert to a previously installed version of InputAccel Server. This involves completely removing the InputAccel Server and all previous versions from the system while leaving the InputAccel files and data intact and then reinstalling the earlier version.

To revert back to a previously installed version of the InputAccel Server:

1. Remove the InputAccel Server from any ScaleServer group, if applicable.
2. Ensure client modules are compatible with the earlier InputAccel Server. If you have upgraded the client modules, then revert these client modules to versions that are compatible with the earlier InputAccel Server.
3. Stop the InputAccel Server.
4. Uninstall the InputAccel Server.
5. Reinstall the earlier InputAccel Server version as well as any required patches and service packs.
6. Restart the InputAccel Server.

Related Topics —

[Upgrading the InputAccel Server, page 126](#)
[InputAccel Server Considerations, page 17](#)
[InputAccel Server Scalability, page 23](#)
[Installing the InputAccel Server, page 47](#)
[ScaleServer Issues, page 161](#)

Upgrading InputAccel Server in a Microsoft Failover Clustering Environment

To upgrade the cluster environment, you upgrade the InputAccel Servers on both nodes and recreate **Named Resource** types for the InputAccel Server applications/roles.

The upgrade does not affect the batches and processes stored on the InputAccel 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 InputAccel Servers are online in the cluster.

Requirements

- Make sure that your environment meets the requirements as specified in [Requirements for InputAccel Server in Microsoft Failover Clustering](#), page 69.
- Upgrade the InputAccel Database before upgrading the InputAccel Servers in the cluster.

Upgrading InputAccel Server in a Microsoft Failover Clustering Environment

Note: Keep the InputAccel Server principal folders as-is.

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 InputAccel Server upgrade installer on the node hosting both applications/roles and perform these tasks:
 - a.

Automatically start the EMC Captiva InputAccel Server service when the system starts	Deselect this option. The service startup mode for the InputAccel Server services must be set to Manual when running it in a cluster.
Start the EMC Captiva InputAccel Server service when setup completes	Deselect this option. The InputAccel Server should not be started outside of the cluster control.

- b. In the **Configure InputAccel Service Accounts** window, select the same credentials for running the InputAccel 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 InputAccel Server upgrade installer on the second node as in [Step 5](#).
 8. To register the InputAccel Server cluster resource DLLs with the cluster, on one node, in a command prompt (running as Administrator), execute the following file for each InputAccel Server:

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

where <Server#> is the directory for each InputAccel Server.

InputAccel resource type is created for the first InputAccel 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 InputAccel Servers to the cluster application/role, right-click the InputAccel 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 InputAccel Servers are not installed on both nodes:

The resource type Add InputAccel is not configured on all nodes.
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 InputAccel Server: <ul style="list-style-type: none"> • Cluster disk • Name
Policies	Until the InputAccel Server is fully licensed and operational, EMC recommends changing 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 Captiva Administrator.

Upgrading Captiva REST Services

Upgrading Captiva REST Services consists of installing and configuring the new Captiva Capture Web Client and Captiva REST Service as follows:

1. Follow the instructions in [Installing Captiva Capture Web Client and Captiva REST Service, page 78](#).
2. Because Captiva Capture Web Client and Captiva REST Service are configured with a default URL that is different from previous versions, you must reconfigure your system such that existing clients use this new URL.

Note: The previous version of Captiva REST Services is uninstalled.

Upgrading Client Modules

This procedure applies to upgrading from Captiva Capture 7.0 or 7.1 to 7.5.

Note:

- If you installed InputAccel Server 7.0 or 7.1 with the file-based, internal database, then you need to upgrade only the InputAccel Server before upgrading the client modules.
- If you installed InputAccel Server 7.0 or 7.1 with the InputAccel Database, then you must upgrade both the InputAccel Server and the InputAccel Database before upgrading the client modules.

For instructions on upgrading from 6.0 SP3 and 6.5.x, see [Upgrading from 6.0 SP3 and 6.5.x to 7.5, page 123](#).

To upgrade client modules:

1. Log in to each client machine as a user with local administrative rights.
2. Stop all InputAccel 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.

Related Topics —

[Client Machine Considerations, page 19](#)

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.

Related Topics —

[Appendix B, Captiva Capture Client Modules](#)

Upgrading ClickOnce-Deployed Applications

This section applies to users upgrading from InputAccel 6.x and Captiva Capture 7.0 and 7.1. Applications deployed using the ClickOnce Deployment Utility must be upgraded so that remote users accessing the applications get the latest upgraded software. Users will have access to the upgraded software only if the previous version of the application was deployed with the **Automatic Update** feature enabled. If the ClickOnce applications are not upgraded, then certain compatibility restrictions apply as detailed in [Understanding Compatibility among Captiva Capture Components, page 104](#).

To upgrade ClickOnce-deployed applications:

1. Install the upgraded ScanPlus ClickOnce Package and RescanPlus ClickOnce Package. Refer to [Upgrading Client Modules, page 130](#) for instructions.
2. Select **Start > Programs > EMC Captiva Capture > Tools (Standard) > ClickOnce Deployment Utility**. The **Deploy InputAccel Application** window displays.
3. Follow the instructions in [Deploying Modules with the ClickOnce Deployment Utility, page 89](#)) to deploy the applications using the ClickOnce Deployment Utility. Make sure the **Publish version** is set to a version greater than the version specified in the previously-deployed application.

Note:

- If the application was initially deployed with the **Automatic Update** option enabled and the upgraded application is deployed to the same location as its previous version, then the module checks for an upgraded version, and the user can upgrade the module with a single click.
- If the upgraded application is deployed to a different location than its previous version, the user can have access to the upgraded application by clicking the new deployment location.
- For customers upgrading from 6.x: IndexPlus is no longer shipped in this release nor supported.

Related Topics —

[Client Machine Considerations, page 19](#)

[Client Scalability, page 24](#)

[Upgrading Client Modules, page 130](#)

[Appendix B, Captiva Capture Client Modules](#)

Upgrading Existing CaptureFlow Designer XPP Processes

This section applies to upgrade 6.x version users that used CaptureFlow Designer to create processes. CaptureFlow Designer is no longer a standalone module but part of the integrated development

tools provided with Captiva Designer. To continue using CaptureFlow designed processes, do the following:

1. Rename the existing XPP to conform to the current XPP naming conventions and then copy the XPP to the \GlobalData\XPP folder.
2. In Captiva Designer, open the XPP file and upgrade it.

For more information, see the *Captiva Designer Guide*.

Note: If you are a 6.0 SP3 user, be aware that CaptureFlow Designer replaces 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

When opening an XPP file with **Captiva Designer > CaptureFlow Designer**, the process flow is automatically updated to use the Synchronize module in place of some Multi module steps.

Upgrading Existing Scripts

You upgrade your existing scripts as follows:

Complete upgrade to 7.5 (that is, no 7.1 clients remain)	Existing scripting DLLs are built with .NET 3.5 but can run under .NET 4.5.2 without any changes; however, it is a good practice to recompile and test them under .NET 4.5.2.
Partial upgrade to 7.5 (that is, some 7.1 clients remain)	Existing scripting DLLs are built with .NET 3.5 and they must remain as-is for 7.1 clients to use them. Version 7.5 clients, which use .NET 4.5.2, can also run these existing scripting DLLs, but any new script classes and new scripting DLLs must be based on the 7.1 version of <code>Emc.InputAccel.CaptureClient.dll</code> and the APIs that it provides; otherwise, the 7.1 clients cannot run.

Upgrading Documentum Advanced Export Client-Side Scripting

The following issue is for users of InputAccel 6.0 SP3 who are upgrading to the Documentum Advanced Export 7.5. This issue does not require you to modify or recompile your processes; however, you must recompile processes to take advantage of new capabilities of the module.

Documentum Advanced Export client-side scripting has changed to use DFC functionality for .NET interoperability, in part because DFC PIA support has been deprecated within the Documentum

product family. Therefore, client-side scripts that were developed in earlier versions of InputAccel will not work with Documentum Advanced Export version 7.5. These scripts must be updated by someone familiar with both the PIA and Documentum Advanced Export scripting APIs.

Note: Documentum Advanced Export steps that do not use client-side scripting will continue to work without changes after upgrading.

Sample Upgrade Scenarios

Upgrading to Captiva Capture requires thoughtful planning and careful execution. This section provides upgrade scenarios for typical situations to help understand the considerations unique to your environment.

- [Sample Scenario: Upgrade from InputAccel 6.0 , page 133](#)
- [Sample Scenario: Upgrade from InputAccel 6.5 to 7.5, page 135](#)

Sample Scenario: Upgrade from InputAccel 6.0

This scenario is an upgrade from a release that the 7.5 upgrade software does not directly support, InputAccel 6.0. This scenario has the following characteristics:

- Existing 6.0 InputAccel Database.
- One or more 6.0 InputAccel Servers.
- Existing 6.0 Administration Console

Note: Because Administration Console cannot connect to an InputAccel Server 7.5, you must upgrade Administration Console to Captiva Administrator 7.5.

- No custom modules and no special customizations by the customer or EMC Consulting.

When this upgrade scenario is complete, you can process tasks in multiple languages and locales as explained in the [Administration Guide](#).

To upgrade this InputAccel system:

1. Upgrade the entire InputAccel system to version 6.0 SP3 by following the upgrade instructions provided with those releases. After you complete this step, you are upgrading one of the supported releases.
2. Archive irreplaceable system files in the event that you need to roll back to version 6.0 SP3. Irreplaceable system files are listed in [Identifying Irreplaceable Files, page 109](#).
3. Disconnect all client modules and stop all InputAccel Servers and client services.
4. Run the InputAccel Database setup program on your InputAccel Database machine to automatically upgrade this component. [Installing the InputAccel Database, page 45](#) provides step-by-step instructions.

Note: The system requirements for the InputAccel Database have changed. Be sure your SQL Server installation meets or exceeds the new requirements listed in the *Release Notes*.

5. Run the InputAccel Server setup program on each of your InputAccel Server machines to automatically upgrade this component. When finished, make sure the InputAccel Server service is started. Detailed instructions are provided in [Upgrading the InputAccel Server, page 126](#).

Note: The system requirements for the InputAccel Server have changed. Be sure your server machine meets or exceeds the new requirements listed in the *Release Notes*.

6. To install Captiva Administrator, run the InputAccel Client installer.
After the upgrade is complete, Captiva Administrator is installed. Use this module to install your license codes for new modules, and if applicable, activate the product.

Note: You should also run the **Web Components** installer to remove the Administrator Console.

7. At this point, you may continue to use version 6.0 SP3 client modules with no further upgrades, subject to the conditions listed in [Understanding Locale Considerations before Planning the Upgrade, page 108](#). Or you may proceed with the following steps and upgrade some or all client modules to version 7.5.

Note: For the 6.0 SP3 client modules that you continue to use with your 7.5 system, be aware that these modules can only process tasks containing multiple languages within the single-byte code page of their host machine and that InputAccel Servers will refuse connections from these non-upgraded client modules if they are not set to the same locale, globalization, and code page settings as their InputAccel Servers.

8. (Optional) For each client machine you want to upgrade to new module versions, run the InputAccel Client setup program on each existing client machine to automatically upgrade the installed components. Be sure to include the machine(s) on which you run Process Developer, ClickOnce deployment, and the Web Services subsystem. Instructions for using the InputAccel Client setup program are provided in [Upgrading Client Modules, page 130](#). Also, install new client modules as part of this step.



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 Captiva Designer, upgrade your processes, and set up each Standard Export step in every upgraded process.

- When you upgrade Image Divider machines, the setup program replaces the module and installs the Image Converter module.

Note: Unlike Image Divider, Image Converter does not include client-side scripting capabilities.

Note:

- PrimeOCR Plus is no longer shipped. Users of PrimeOCR Plus should work with Prime Recognition to verify the compatibility and latest version of the module.
9. (Optional) The East Euro / APAC OCR module no longer supports the following settings:
 - **Automatic** Print Type format.
 - **Remove all formatting** and **Editable copy** from the **Retain Layout** list
 - **Microsoft Word** from the **Format** list

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 the *East Euro / APAC OCR Guide*.

10. (Optional) 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 the *NuanceOCR Guide*.

11. (Optional) Edit or create new processes to use any new client functionality that you have added (for example, Completion, Image Processor, or Image Converter), and then compile and install them on your InputAccel Servers.

Note: IPPs must be configured using Captiva Administrator. XPPs should be configured directly in Captiva Designer.

Related Topics —

- [Identifying Irreplaceable Files, page 109](#)
- [Understanding the Upgrade Process, page 113](#)
- [Scheduling Upgrade Phases, page 122](#)
- [Upgrading from 6.0 SP3 and 6.5.x to 7.5, page 123](#)

Sample Scenario: Upgrade from InputAccel 6.5 to 7.5

This scenario is an upgrade from a release that the 7.5 upgrade software directly supports, InputAccel 6.5. This scenario has the following characteristics:

- Existing 6.5 InputAccel Database.
- One or more 6.5 InputAccel Servers.
- No custom modules and no special customizations by the customer or EMC Consulting.

To upgrade this InputAccel system:

1. Archive irreplaceable files such that you can roll back to version 6.5, if required.
For more information, see [Identifying Irreplaceable Files, page 109](#).
2. Disconnect all client modules and stop all InputAccel Servers and client services.
3. To upgrade the InputAccel Database, run the InputAccel Database installer.

For more information, see [Installing the InputAccel Database, page 45](#).

Note: The system requirements for the InputAccel Database have changed. Be sure your SQL Server installation meets or exceeds the new requirements listed in the *Captiva Capture Release Notes*.

4. To upgrade each InputAccel Server, run the InputAccel Server installer on each machine. Make sure the InputAccel Server Windows service can be started. For more information, see [Upgrading the InputAccel Server, page 126](#).
Note: The system requirements for the InputAccel Server have changed. Be sure your server machine meets or exceeds the new requirements listed in the *Captiva Capture Release Notes*.
5. To install Captiva Administrator, run the InputAccel Client installer.
After the upgrade is complete, Captiva Administrator is installed. Use Captiva Administrator to install your license codes for new modules and activate the product, if required.

Note: You should also run the **Web Components** installer to remove the Administrator Console.

6. The East Euro / APAC OCR module no longer supports the following settings:
 - **Automatic** Print Type format.
 - **Remove all formatting** and **Editable copy** from the **Retain Layout** list
 - **Microsoft Word** from the **Format** list

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 the *East Euro / APAC OCR Guide*.

7. 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 the *NuanceOCR Guide*.

8. (Optional) To upgrade existing client modules (including Process Developer, ClickOnce deployment, and the Web Services subsystem) or install new ones, run the InputAccel Client installer.

For more information, see [Upgrading Client Modules, page 130](#).



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 Captiva Designer, upgrade your processes, and set up each Standard Export step in every upgraded process.

- When you upgrade Image Divider machines, the setup program replaces the module with the Image Converter module.

Note: Unlike Image Divider, Image Converter does not include client-side scripting capabilities.

9. (Optional) Edit or create new 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 InputAccel Servers.

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 Captiva 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.

Topics in this section include:

- [Migrating Processes, page 137](#)
- [Migrating from Multi-Directory Watch and Email Import to Standard Import, page 141](#)
- [Migrating from Image Quality Assurance to the Completion Module, page 142](#)
- [Migrating from IndexPlus and Dispatcher Recognition to Completion and Extraction, page 142](#)
- [Migrating from Dispatcher Validation to the Completion Module, page 144](#)
- [Migrating from Dispatcher Classification Edit to the Identification Module, page 145](#)
- [Migrating from Image Enhancement to Image Processor, page 147](#)
- [Migrating to Use Updated Image Converter, page 148](#)
- [Migrating to Use Standard Export, page 148](#)

Migrating Processes

Migrating CaptureFlow-developed Processes to Only Use the .NET Runtime

To upgrade CaptureFlow-developed processes to use only the .NET runtime, you recompile and redeploy the process to the InputAccel Server. If associated batches are running on the InputAccel Server, deploy the process with a different name.

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.

Migrating Process Developer Processes to Captiva 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 [Captiva Designer Guide](#) provides detailed instructions on using CaptureFlow Designer and CaptureFlow Script Editor. The [Scripting Guide](#) provides details on the APIs used to create CaptureFlow scripts.

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 Captiva 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. Refer to the [Captiva Designer Guide](#) for this information.

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 [Captiva Designer Guide](#). Document Type Scripting information and APIs are provided in the [Scripting Guide](#).
6. Implement Index Families in a Recognition project. Refer to the [Captiva Designer Guide](#) for this information.
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. Refer to the [Captiva Designer Guide](#) for information on creating a process using CaptureFlow Designer.

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. Refer to the [Scripting Guide](#) for this information.
 - 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 Captiva 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 CaptureFlow Designer. Next, use Captiva 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 Captiva 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.

Migrating CaptureFlow Designer Processes to Captiva Designer

As of 7.0, CaptureFlow Designer was no longer a standalone module but part of the integrated development tools provided with Captiva 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 Captiva Designer and ensure that it opens correctly.

When opening an XPP file with **Captiva 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. Review the [Captiva Designer Guide](#) for more information.

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

Upgrading Process Developer Processes

Your existing Process Developer processes should run as-is in Captiva Capture 7.5.

If you want to add 7.5 modules and functionality to your existing Process Developer processes, then follow these steps:

1. In Process Developer, add module steps for the new client modules in 7.5. Compile the process and reinstall the process to InputAccel Servers.
2. This step is required only if the new client modules added to the process use profiles. Use Captiva Designer to create profiles and deploy the profiles to InputAccel Servers.
3. Use Captiva Administrator to configure process steps.
4. Install .NET Code module assemblies, DPP project files, and client-side scripting assemblies.

Migrating from Multi-Directory Watch and Email Import to Standard Import

1. In Captiva 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.
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,...]
```

Make sure to include the names of any current profiles that you still want to use on each module instance.

For more information, see [Captiva Designer Guide](#) or [Captiva Module Reference](#).

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. Refer to the [Captiva Completion Guide](#) for information on using the module.

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.

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. Refer to the [Captiva Completion Guide](#) and the [Extraction Guide](#) for information on using and configuring these modules.

1. Create a Recognition Project in Captiva Designer.
2. (Optional) Define the OCR and field zones if the Extraction module functionality or KFI mode is required:
 - If NuanceOCR or East Euro APAC OCR engines were 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 in Captiva 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 [Scripting Guide](#).

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 Captiva 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 the [Administration Guide](#).

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 Captiva 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 and/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.

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. Refer to the [Captiva Completion Guide](#) for information on using the module.

1. Import an existing DPP file into **Captiva 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 Captiva 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 the [Administration Guide](#).
 - 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.

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. Refer to the [Captiva Identification Guide](#) for information on using the module.

1. Import an existing DPP file into **Captiva 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 `OcrDataCache` (input and output). The description of each value can be found in the `CPIDENTF.MDF` file and in the [Captiva Identification Guide](#).
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 Captiva Designer.
5. Run setup on the new Identification step(s). The description of all available setup settings can be found in [Captiva Identification Guide](#). The following Classification Edit setup settings are configured differently or not supported:

Table 14.

Classification Edit setup settings	Identification
External IA Values	Not configurable in setup. You can do it Captiva Designer through UIMDataImportMode and UIMData_IA Values. For more information, see the Captiva Designer Guide , section <i>Transferring Document Data</i> .
Process backside images as pages	Identification setup: Select Display Back Side of Images .
Error handling options	Not configurable in setup. The error handling scenario is specified for each CaptureFlow step in Captiva Designer. For more information, see the Captiva Designer Guide , section <i>Adding a Batch Processing Step</i> .
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 the Captiva Designer Guide , section <i>Designing Document Types</i> .
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 Captiva Designer. For more information, see the Captiva Designer Guide , section <i>Defining Shortcuts</i> .
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 Captiva Designer. For more information, see the Captiva Designer Guide , section <i>Defining Styles</i> . System styles do not include custom colors for even and odd pages in the Page List View.

6. Configure system styles in Captiva Designer. Upload the configuration file to the server. For more information, see the [Captiva Designer Guide](#), section *Defining Styles*.

7. Deploy document types and the recognition project using Captiva Designer. For more information, see the [Captiva Designer Guide](#), section *Deploying Components*.
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 the [Administration Guide](#).
 - Remove the use of Dispatcher 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 than during step setup. Error handling can be enhanced with CaptureFlow scripting.

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. Refer to the [Captiva Designer Guide](#) for information on creating Image Processing profiles and [Image Processor Guide](#) to learn how to use the module.

1. For each existing Image Enhancement step in the process, create a new Image Processing profile in Captiva Designer. Refer to the Image Processor profile documentation in the [Captiva Designer Guide](#) to learn more about available filters.
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.

Note:

- 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.

Migrating to Use Updated Image Converter

This section is targeted towards 6.5.x users that used Image Converter in the previous versions and want to update to using profile-based Image Converter from 7.1. Refer to the [Captiva Designer Guide](#) for information on creating Image Conversion profiles and [Image Converter Guide](#) to learn how to use the module.

1. Open an existing Image Converter step setting, and follow the instructions to save the converted profile to a local file. Make sure the profile name conforms to the naming conventions for Image Conversion profiles.
2. Place the converted profile to the \<Capture System>\GlobalData\ImageConversion folder.
3. Deploy the converted profile to the server and then select the profile when you configure the Image Converter module in setup mode.

Migrating to Use Standard Export

This section is targeted towards users that used standard export modules such as File System 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 7.5. Refer to the [Captiva Designer Guide](#) for information on creating export profiles and [Standard Export Guide](#) to learn how to use the module.

1. In Captiva 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 refer to the output file.
3. Deploy your export profiles to the server.
4. Remove File System 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.

Modifying, Repairing, and Removing Captiva Capture

A Captiva Capture installation can be modified, repaired, or uninstalled. Topics in this section include:

- [Modifying a Captiva Capture Installation, page 151](#)
- [Repairing a Captiva Capture Installation, page 152](#)
- [Removing Captiva Capture Components, page 152](#)

Modifying a Captiva Capture Installation

The current installation of Captiva Capture can be modified. Modifying the installation lets you install features that are not currently installed and remove features that were installed.

To modify a Captiva Capture installation:

1. Stop the component that you want to modify.
2. Run the setup program and select **Install Products**.
3. Select the component to modify and then 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 and then click **Next**, **Next**, and then **Install**.
The installation is modified.

Related Topics —

- [Repairing a Captiva Capture Installation, page 152](#)
- [Removing Captiva Capture Components, page 152](#)

Repairing a Captiva Capture Installation

The Captiva Capture installation repair functionality is useful if you have removed a feature or if the program becomes corrupted.

To repair the InputAccel Server after removing a feature, use the same `InputAccel_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 `InputAccel_Client.msi` file used to install the original system.

To repair InputAccel installations:

1. Stop the component that 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. Click **Install**.

Removing Captiva Capture Components

Installed Captiva 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 Captiva Capture components:

1. Stop the service for the component that you want to remove. For instance, stop the InputAccel Server service before removing the InputAccel Server.
2. (When removing the InputAccel Server) From the Captiva Administrator module, navigate to the **Servers** pane and delete the InputAccel 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 then click **Next**. The **Program Maintenance** window displays.
5. Select the **Remove** option and then click **Next**. The **Remove the Program** window displays. Click **Remove**. The component is removed completely from the machine.

Note: The **InputAccel_Server_admin_group** group created by the InputAccel Server setup program is removed when the InputAccel Server is removed. This group cannot be used after the server is removed.

Troubleshooting

This section provides information to help you troubleshoot installation problems. Topics in this section include:

- [Installation Failures, page 155](#)
- [Third-party Component Issues, page 159](#)
- [Post-installation Issues, page 159](#)

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**.

For example, you could 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 logfile"
```

where

/v passes the part of the command line enclosed in quotes to the Microsoft Installer package.

/l*v enables verbose logging.

logfile 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 in order 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.

Topics in this section include:

- [Installation Errors, page 156](#)
- [Command-line Installation Failures, page 157](#)

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. The following table lists common installation errors.

Table 15. 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.	<p>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:</p> <ul style="list-style-type: none"> • 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.	<p>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:</p> <ol style="list-style-type: none"> 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 Captiva user that accesses and creates processes and batches are

Problem	Possible cause / Workaround
	granted the Windows permission (use Windows tools) to access the IAS folder.
When installing the server, an error message is displayed stating that DCOM permissions were not set.	<p>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.</p> <p>To fix this issue users must run <code>dcomcnfg</code> to grant the InputAccel_Server_admin_group permissions to activate and execute DCOM objects.</p>

Command-line Installation Failures

Command-line installation failures include:

- [Syntax Errors, page 157](#)
- [Common Command-Line Installation Errors, page 157](#)

Syntax Errors

[Unattended Installations, page 94](#) explains how to install Captiva 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 (" "). For 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, page 155](#).

Common Command-Line Installation Errors

The following table lists some of the more common errors that customers experience when running setup programs from the command line.

Table 16. 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 <code>/v</code> and the first open quote symbol.
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 <code>setup.exe</code> program.
Windows restarts automatically after setup completes.	<p>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:</p> <p>/norestart: Do not restart after setup completes.</p> <p>/promptrestart: Prompt the user to restart if necessary.</p> <p>/forcerestart: Always restart after setup completes, regardless of whether the setup program determines that a restart is necessary.</p>
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.	<p>Syntax issues can cause various errors when attempting a command-line installation. Note the following rules:</p> <ul style="list-style-type: none"> Properties containing spaces must be enclosed in quotation marks that have been escaped with a backslash character (<code>\</code>). Example: <pre>INSTALLDIR="c:\Program Files\InputAccel\Client\"</pre> Properties containing the reserved characters <code>\</code>, <code>&</code>, <code> </code>, <code>></code>, <code><</code>, and <code>^</code> must escape those characters with a caret character (<code>^</code>). Example: <pre>SCANNERNAME="Canon DR-4580U ^& DR-5580U\"</pre>

Third-party Component Issues

Certain Captiva Capture client modules rely on third-party components provided by the company that produces the application to which they connect. There are two categories of modules with this issue: those that will not install without the required third-party components, and those that will install, but not run, without the required third-party components.

Refer to *Release Notes > Module-Specific Requirements* that contains the list of third-party software requirements for client modules. The *Release Notes* is available from the **Start** menu of your desktop at **All Programs > EMC Captiva Capture > Documentation**.

- Modules that will not install until third-party components are installed:
 - ApplicationXtender Export
 - IBM CM Advanced Export
- Modules that install but will not run until third-party components are installed:
 - .NET Code
 - Archive Export
 - Captiva Administrator
 - Captiva Designer
 - Documentum Advanced Export
 - FileNet Content Manager Export
 - FileNet Panagon IS/CS Export
 - Global 360 Export
 - IBM CSSAP Export
 - Image Converter
 - MS SharePoint Export
 - NuanceOCR
 - ODBC Export
 - Open Text Livelink Advanced Export
 - RescanPlus
 - ScanPlus
 - Standard Export

Post-installation Issues

This section provides troubleshooting tips for issues that can occur after a successful installation, including:

- [InputAccel Database Issues, page 160](#)
- [ScaleServer Issues, page 161](#)
- [Other Issues, page 162](#)

InputAccel Database Issues

The InputAccel Database is an optional component that resides in an instance of Microsoft SQL Server. SQL Server must be configured to enable the InputAccel system to connect and communicate with the InputAccel Database. Following are some common problems that can occur.

Table 17. Common InputAccel Database-Related Problems

Problem	Possible cause
InputAccel Database setup program cannot create the InputAccel Database.	<ul style="list-style-type: none"> • 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 InputAccel Database setup, the account specified to create the InputAccel Database must be assigned the <code>dbcreator</code> Server Role. Typically, you would enable the <code>dbcreator</code> account login and assign it a password within SQL Server and then specify this account to install the InputAccel Database.
Captiva Capture components cannot connect to SQL Server.	<ul style="list-style-type: none"> • 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
Captiva Capture components cannot log into SQL Server	<ul style="list-style-type: none"> • SQL Server Authentication mode is not enabled. Captiva Capture does not support Windows authentication. You must specify a SQL Server user name and password to connect. Consult SQL Server documentation for instructions on enabling SQL Server and Windows Authentication mode. • When enabling SQL Server Authentication mode, the User must change password at next login checkbox was selected. The first time an InputAccel component attempts to connect to the InputAccel 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: <i>hostname\instancename</i>
Captiva Capture components cannot access the InputAccel Database.	<ul style="list-style-type: none"> • 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 InputAccel 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.	<ul style="list-style-type: none"> • Login credentials are not retained when upgrading and must be specified again.

ScaleServer Issues

When InputAccel Servers are configured as a ScaleServer group, client modules must connect to one of the InputAccel Servers in the ScaleServer group by using the machine name of the machine hosting the InputAccel 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.

Other Issues

This section explains some common issues that may occur during InputAccel setup.

Table 18. Other Problems during InputAccel Setup

Problem	Possible cause
InputAccel Server fails to start	<p>The account used to run the InputAccel Server may not have the necessary rights and permissions. Add the user account specified for the InputAccel Server service to the local LUA group that is created when the InputAccel Server is installed: InputAccel_Server_admin_group. If the LUA group has been deleted, follow these instructions to recreate it:</p> <ol style="list-style-type: none"> 1. Stop all instances of the InputAccel Server service on the machine on which the group is to be created. 2. Open a command prompt window on the InputAccel Server machine. 3. Type the following command line: <pre>ias64.exe -repair -r datadir -s servicename [-a1 account1]</pre> <p>where:</p> <ul style="list-style-type: none"> • datadir is the name of the InputAccel Server data directory (default: C:\IAS). • servicename is the instance name of the service that runs the InputAccel 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. <p>Note: 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 <i>a1</i> argument using the syntax: <i>domain\account</i>. To add local accounts, do not specify a domain.</p> <p>Note: Security permissions of the IAS data directory are updated when this command is run.</p> <p>Examples —</p> <ul style="list-style-type: none"> • Create the LUA group using the default InputAccel Server data directory and service instance name: <pre>ias64.exe -repair -r C:\IAS -s InputAccel</pre> • Create the LUA group using the default InputAccel Server data directory and service instance name, adding one local user account to the group:

Problem	Possible cause
	<pre>ias64.exe -repair -r C:\IAS -s InputAccel -al dasna_o</pre> <ul style="list-style-type: none"> • Create the LUA group using the default InputAccel Server data directory and service instance name, adding one domain user account to the group: <pre>ias64.exe -repair -r C:\IAS -s InputAccel -al federal\potus</pre> <ol style="list-style-type: none"> 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 InputAccel Server installed on the machine. 6. Start all instances of the InputAccel Server service.
InputAccel Server installer appears to stop unexpectedly or stop working when installing with an existing IAS folder.	When the InputAccel 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.
InputAccel client fails to connect to InputAccel Server	<ul style="list-style-type: none"> • InputAccel Server service is not running. On the InputAccel Server host machine, use the Windows Service Control Manager to locate the InputAccel Server service and make sure it is started. • Client cannot communicate with server. Verify that the client machines and the InputAccel Server are all configured to communicate on the same port (10099, by default).
InputAccel client fails to connect to InputAccel Server (continued)	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – Configure the InputAccel Server machine to allow anonymous access. – Run the client module on the same machine as the InputAccel Server. – Configure InputAccel to use Kerberos and set an SPN for the InputAccel Server, as explained in Configuring Captiva Capture to use Kerberos authentication, page 22. • The machine name of the InputAccel 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 InputAccel Server.

Problem	Possible cause
	<ul style="list-style-type: none"> • 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 InputAccel 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 <i>servername</i> is not configured properly" occurs during InputAccel 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 InputAccel 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.
Web Services Output does not function	Ensure that you have Web Services Enhancements (WSE) 3.0 for Microsoft .NET installed. Refer to the <i>Release Notes</i> for the system requirements.
Cannot specify -department (or other command-line arguments) when starting a ClickOnce-deployed module	Command-line arguments are not supported when ClickOnce packages are deployed from a file share. Deploy modules from a URL to specify command-line arguments. Furthermore, the command-line arguments have a different syntax when specified as part of a URL. This syntax is explained in each applicable module guide.
In some cases, a notebook machine that does not have a parallel port encounters a STOP error (displays a blue screen with an error message and shuts down) after being undocked from a docking station that has a parallel port (when the notebook machine is running the InputAccel Server).	The Sentinel driver that is installed for use with a parallel port hardware security key is causing the issue. To prevent this problem, use Windows Device Manager to disable the Sentinel driver (found under "Non-Plug And Play Drivers.") in all hardware profiles.

To verify differences in the locale, globalization, and code page settings on the InputAccel Server and client machines:

1. On the machine where a client module is installed, open the `settings.ini` file.
The default location is `c:\Documents and Settings\All Users\Application Data\EMC\InputAccel`.
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 InputAccel Server machine and the client module machine, change the regional settings so that these settings on the InputAccel Server and client machines are identical.

Prerequisite Software Installed by the Captiva Capture Setup Program

The Captiva Capture setup program installs prerequisite software if the software is not already installed. The prerequisite software varies depending on the Captiva Capture component that is installed. This section lists the prerequisite software installed for each Captiva 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.

Prerequisite Software Installed with the InputAccel Server

The following prerequisite software is installed with the InputAccel Server:

- Microsoft Visual Basic for Applications Core
- Microsoft Visual Basic for Applications Core - English
- Microsoft Visual Basic for Applications Security Update

IIS Roles Enabled with Captiva Capture Web Components

The following IIS roles are enabled when Captiva REST Service and Captiva Capture Web Client are installed:

- Application Development
- HTTP Redirection
- IIS Management Script and Tools
- ISAPI Extensions
- ISAPI Filters
- Static Content
- ASP.NET 4.5 (IIS 8.0 and 8.5 only)
- .NET Extensibility 4.5

Prerequisite Software Installed with the InputAccel Client Modules

- Microsoft Visual Basic for Applications Core
- Microsoft Visual Basic for Applications Core - English
- Microsoft Sync Framework 2.0 Synchronization-v2.0 - x86
- Microsoft Sync Framework 2.0 Synchronization-v2.0 - x64
- Microsoft Sync Framework 2.0 ProviderServices-v2.0 - x86
- Microsoft Sync Framework 2.0 ProviderServices-v2.0 - x64
- Microsoft Visual Basic for Applications Security Update
- Microsoft Visual C++ 2005 SP1 Security Update (x86)
- Microsoft Visual C++ 2008 SP1 Redistributable Package MFC Security Update (x86)

Captiva Capture Client Modules

The following table lists all 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 as you may experience data loss. Refer to this table for the list of modules that you can safely run as multiple application or service instances.

Table 19. Captiva Capture Modules

Modules New in 7.0 - 7.x	Modules New in 6.x ¹	Modules Available Prior to 6.0 ²	Executable Name ³	MDF File Name	DBCS ⁴	Scale-Server ⁵	At-tended ⁶	Unat-tended ⁷	Applica-tion ⁸	Multi-application in-stances ⁹	Service ¹⁰	Multi-service ¹¹	Script-ing ¹²
	.NET Code Module		CodeClient.exe	code.mdf	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes ¹³
		ApplicationXtender Export	exax.exe	exax.mdf	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
		Archive Export	exsapal.exe	exsapal.mdf	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Captiva Administrator			CaptivaAdministrator.exe	N/A	N/A	No	Yes	No	Yes	Yes	No	No	No
		Classification	Emc.InputAccel.DPCLSSF.dll	dpclssf.mdf	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes ¹⁴
		Classification Edit	Emc.InputAccel.DPCLSSFE.dll	dpclssfe.mdf	Yes	Yes		No	No	Yes	No	No	Yes ¹⁵
		Collector	Emc.InputAccel.DP Collec.dll	dpcollec.mdf	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes ¹⁶
Completion (previously known as Captiva Desktop)			cpdsktop.exe	cpdsktop.mdf	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes ¹⁷
		Copy	iacopy.exe	iacopy.mdf	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
		DLL Viewer	pixloadadd.exe	N/A	No	No	Yes	No	Yes	Yes	No	No	No

1. Indicated modules were introduced in 6.x

2. Indicated modules were introduced prior to InputAccel 6.0.

3. Executable name of the module.

4. Can process tasks that include double-byte character values, such as Korean and Chinese.

5. Can connect to multiple InputAccel Servers that are configured as a ScaleServer group.

6. Can be operated in attended production mode, displaying an interactive user interface.

7. Can be operated in unattended production mode, without any user interaction.

8. Can be run as an application.

9. Multiple application instances can safely be run on a single machine.

10. Can be configured to run as Windows services.

11. Multiple instances can safely be run as Windows services on a single machine.

12. Can use scripting.

13. .NET Code Module provides a separate programming interface that is independent of the client-side scripting interface used by other modules. The [.NET Code Module Guide](#) provides configuration and reference information.

14. Use Recognition Scripting

15. Use Recognition Scripting

16. Use Recognition Scripting

17. Use Document Scripting

Modules New in 7.0 - 7.x	Modules New in 6.x ¹	Modules Available Prior to 6.0 ²	Executable Name ³	MDF File Name	DBCS ⁴	Scale- Server ⁵	At- tended ⁶	Unat- tended ⁷	Applica- tion ⁸	Multi- -application in- stances ⁹	Service ¹⁰	Multi- -service ¹¹	Script- ing ¹²
	Documentum Advanced Export		DocumentumAdvancedExport.dll	iaexdm.mdf	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes ¹⁸
	East Euro / APAC OCR		EastEuroAPACOCR.dll	abyocr2.mdf	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
		Email Import	EmailImport.exe	emailimp.mdf	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
Extraction			cpextrac.exe	cpextrac.mdf	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes ¹⁹
		FileNet Content Manager Export	exfncm.exe	exfncm.mdf	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
		FileNet Panagon IS/CS Export	iaxfnet2.exe	iaxfnet2.mdf	Yes	No	Yes	Yes	Yes	Yes ²⁰	No	No	No
		Global 360 Export (formerly known as eiStream WMS Export)	iaexwnt.exe	iaexwnt.mdf	No	No	Yes	Yes	Yes	Yes	No	No	No
		IBM CM Advanced Export	exicm.exe	exicm.mdf	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
		IBM CSSAP Export	excssap.exe	excssap.mdf	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Identification			cpidentf.exe	cpidentf.mdf	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes ²¹
Image Converter			imgconv.exe	imgconv.mdf	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Image Processor			cpimgpro.exe	cpimgpro.mdf	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes ²²
		MS SharePoint Export	exshrpt2.exe	exshrpt2.mdf	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
		Multi	iamulti.exe	iamulti.mdf	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
		Multi-Directory Watch	MultiDirectoryWatch.exe	iamdw.mdf	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
	NuanceOCR		NuanceOCR.dll	ssocr.mdf	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes ²³
		ODBC Export	iaxodbc2.exe	iaxodbc2.mdf	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No

18. Use client-side scripting
19. Use Document Scripting
20. FileNet IS/CS Export allows running multiple application instances, but multiple connections may be restricted by the repository.
21. Use Document Scripting
22. Use Document Scripting
23. Use client-side scripting

Modules New in 7.0 - 7.x	Modules New in 6.x ¹	Modules Available Prior to 6.0 ²	Executable Name ³	MDF File Name	DBCS ⁴	Scale- Server ⁵	At- tended ⁶	Unat- tended ⁷	Applica- tion ⁸	Multi -application in- stances ⁹	Service ¹⁰	Multi -service ¹¹	Script- ing ¹²
		Open Text Livelink Advanced Export	exl12.exe	exl12.mdf	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
		Page Registration	pagereg.exe	pagereg.mdf	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
		Pixview	iademon.exe	N/A	No	No	Yes	No	Yes	Yes	No	No	No
	RescanPlus		Emc.InputAccel.ReScan .dll	rescanplus.mdf	Yes	Yes	Yes	-	Yes	Yes	No	No	Yes ²⁴
	ScanPlus		Emc.InputAccel.Scan.dll	scanplus.mdf	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes ²⁵
Standard Export			cpexport.exe	cpexport.mdf	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Standard Import			cpimport.exe	cpimport.mdf	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes ²⁶
		Timer	iatimer.exe	iatimer.mdf	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No
	WS Input		WebServicesInput.dll	wsinput.mdf	Yes	Yes	No	No	No	No	Yes	Yes	Yes ²⁷
	WS Output		WebServicesOutput.dll	wsoutput.mdf	Yes	Yes	No	No	No	No	Yes	Yes	Yes ²⁸

24. Use client-side scripting
25. Use client-side scripting
26. Use Document Scripting
27. Use client-side scripting
28. Use client-side scripting

Client Module Features

This section lists the client modules that can be installed with each feature.

Table 20. Client Components Installation Features

Feature name	Installs
Captiva Administrator	Captiva Administrator
Captiva Designer	Captiva Designer, new samples, and Process Developer
Operator Tools	<ul style="list-style-type: none">• Completion• Identification• ScanPlus• ClickOnce deployable package of the ScanPlus module• RescanPlus• ClickOnce deployable package of the RescanPlus module
Unattended Module Server	
Input/Output Modules	<ul style="list-style-type: none">• Standard Import• Standard Export• ODBC Export• Web Services Input• Web Services Output
Web Services Components	<ul style="list-style-type: none">• Web Services Coordinator• Web Services Hosting

Feature name	Installs
Image Handling	<ul style="list-style-type: none">• Image Converter• Image Enhancement• Page Registration
Recognition	<ul style="list-style-type: none">• East Euro / APAC OCR• NuanceOCR• Extraction
Enterprise Export Modules	<ul style="list-style-type: none">• Archive Export• Documentum Advanced Export• EMC ApplicationXtender Export• FileNet Content Manager Export• FileNet Panagon IS/CS Export• Global 360 Export• IBM CSSAP Export• IBM CM Advanced Export• MS SharePoint Export• Open Text Livelink Advanced Export
Utilities	<ul style="list-style-type: none">• .NET Code Module• Copy• Timer• Multi
Extraction Engines	<ul style="list-style-type: none">• The General-Use OCR engine• The East Euro / APAC OCR engine• The Check Reading engine• The Advanced OCR/ICR engine• The Western OCR engine

Feature name	Installs
Advanced Recognition	<ul style="list-style-type: none">• Classification module• Collector module• Auto-Learning Supervisor service• Advanced Recognition development tools and accessories
Legacy Modules	<ul style="list-style-type: none">• Classification Edit• Email Import• Multi-Directory Watch

New and Legacy Modules

The following modules are new and intended to replace the corresponding legacy modules:

New Modules	Legacy Modules
Standard Import	<ul style="list-style-type: none">• Multi-Directory Watch• Email Import
Identification	Classification Edit

These legacy modules will no longer be shipped nor supported with the next release.

Note: The new modules introduced in this version of Captiva Capture are intended to provide functional equivalence for the legacy modules they replace but may not necessarily provide a one-to-one mapping of features. You may continue to use the legacy module while migrating to the new modules.

Legacy modules have the following additional characteristics:

- The text “(Replaced)” appears in the module name on the **Start** menu.
- Bug fixes are included.
- No enhancements are included.
- No additional localization beyond what was already done in 6.5 is available.
- Documentation is not shipped or installed. In addition, the help files for legacy modules will be removed upon upgrade.
- Patch rollups will be available.

Modules and Components No Longer Shipped

The following modules and components are no longer shipped and no longer supported.

- Administration Console
- Auto Annotate (Image Processor along with Image Processing profiles)
- Automatic Quality Assurance
- Client Script Engine
- Connector for eCopy ShareScan
- Dispatcher License Manager
- Dispatcher Recognition (Extraction)
- Dispatcher Statistics
- Dispatcher Validation (Completion, previously known as Captiva Desktop)
- ECM Web Services Importer Configuration
- Excel Graphing
- File System Export (Standard Export along with Export profiles)
- IBM CMIP-390 Export
- IBM CMIP-390 Index
- Image Divider
- Image (Image Processor)
- Image Enhancement (Image Processor along with Image Processing profiles)
- Image Export (Standard Export along with Export profiles)
- Image Quality Assurance (Completion, previously known as Captiva Desktop)
- iManage WorkSite Server Export
- Index Export (Standard Export along with Export profiles)
- IndexPlus (Completion, previously known as Captiva Desktop)
- InputAccel Remoting

- PDF Export (Standard Export along with Export profiles; most functionality is replaced by the Image Converter module)
- PrimeOCR Plus
- Spawn (no replacement)
- Values to XML (Standard Export along with Export profiles)

Appendix F

Localized Languages

Captiva capture is localized into the following languages. These languages for Captiva Capture are used to control the User Interface (UI) language displayed to the user. The UI language that Captiva Capture components use is independent of the languages that can be part of a batch, task, or page.

Table 21. Localized Languages Captiva 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

Ports Used

The following table lists the ports used by the various components of the Captiva Capture application.

Table 22. Ports Used

Port	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 InputAccel client modules to communicate with the InputAccel Servers. This can be changed during installation and may be different for each InputAccel Server in a side-by-side installation.
443/80	The default HTTPS/HTTP ports for Captiva REST Service and Captiva Capture Web Client Web site.

Running the Database Manager Utility

By default, the database setup program creates an external, SQL Server-hosted InputAccel Database. If customers choose not to install an InputAccel Database, then running the InputAccel 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 InputAccel Database when running the InputAccel Database setup program.
- You have been directed by support personnel to update your InputAccel Database with scripts provided to you.

On Windows 8 and Windows 2012, run the Database Manager utility as an Administrator.

To create or update the external or internal database:

1. From the **Start** menu, click **Programs > EMC Captiva Capture > Tools (Standard) > Database Manager**.
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 InputAccel 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.

- **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 **Update existing database** checkbox to update the InputAccel Database for a patch or upgrade. If you are creating the database for the first time, clear the checkbox.
 5. Click **OK** to save your settings, run the utility, and exit.

Running Database Manager in Silent Mode

The Database Manager utility can be used to silently create the external, SQL Server-hosted InputAccel Database or the file-based, internal database. This utility is run from a command prompt window.

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>
```

Table 23. Explanation of Command-line Arguments used to Install the InputAccel 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 InputAccel Database.
One of the following: <ul style="list-style-type: none"> -all -dbonly -schema 	Installation mode: <ul style="list-style-type: none"> -all: Creates the InputAccel Database, the schema, and data -dbonly: Creates the InputAccel 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.
-password <password>	Password for the specified user name.
dbscripts <path>	Root path to database schema XML files.

Database Manager utility syntax to create a file-based, internal database: Run the following command on the machine that hosts the InputAccel Server:

```
IADBManager -silent -nodb -nodbpath <path> -dbscripts <path>
```

Table 24. 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 InputAccel 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)

Database Manager Command-line Examples

- The following is a sample command line that creates a SQL database "IADB". It specifies a username 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"
```

- 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"
```

- This example upgrades the existing file-based, internal database:

```
IADBManager -nodb -upgrade -silent -nodbpath "C:\IAS" -dbscripts "
C:\Program Files\InputAccel\Server\Server\DBScripts"
```


Command-line Arguments for Installing Captiva Capture

Captiva 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 Captiva Capture features and properties are case sensitive. Use the examples as they are shown. The topics in this section describe the supported command line instructions:

- [Supported MSI Switches, page 190](#)
- [Supported Windows Installer Properties, page 190](#)
- [Captiva Capture Installer Properties and Feature Names, page 190](#)

Supported InstallShield Switches

The following table describes the supported InstallShield switches:

Table 25. Supported InstallShield Switches

Switch	Description
/v	Passes the MSI parameter switches from the InstallShield setup command line to MSI.
/x	Removes a product.

For more information on the supported InstallShield switches, search the Internet for “Setup.exe and Update.exe Command-Line Parameters.”

Related Topics —

- [Supported MSI Switches, page 190](#)
- [Supported Windows Installer Properties, page 190](#)

Supported MSI Switches

Captiva Capture supports the Windows Installer version 4.5 command line parameters that enable you to install, display, restart, log information, update, and repair InputAccel installations. `Msiexec.exe` is the Windows Installer executable program that interprets packages and installs products.

Type **`msiexec.exe /?`** at a command prompt to view a complete list of the Windows Installer command line arguments.

Related Topics —

[Supported InstallShield Switches, page 189](#)

[Captiva Capture Installer Properties and Feature Names, page 190](#)

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.

Refer to the **MSDN Library Windows Installer Property Reference** on the Internet for additional information regarding Installer properties.

Captiva Capture Installer Properties and Feature Names

To perform a silent installation, use InstallShield and MSI command-line parameters in conjunction with the Captiva Capture feature names and properties. You perform silent installations on the appropriate machines to create the InputAccel Databases, InputAccel Server, Web components, and Client Components.

The topics in this section describe installer properties and feature names:

- [InputAccel Database Installer Properties, page 191](#)
- [InputAccel Server Components Installer Properties, page 193](#)
- [Captiva Capture Web Components Installer Properties, page 202](#)
- [Client Components Installer Properties, page 206](#)

InputAccel Database Installer Properties

You can install the InputAccel Database in unattended mode using command line arguments. For 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 username
- 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: SQL Server validation is not possible during a silent installation. It is the responsibility of the user to pass the correct information to the installer.

The following table lists the installer properties that can be specified when installing or upgrading the InputAccel Database:

Table 26. Supported InputAccel Database Installer Properties

Installer property	Value	Required for Upgrade	Description
ADDLOCAL	<i>Features to install</i>	-	A comma delimited list of the features to install. Since there is only one feature in this component to install, users should specify ALL .

Installer property	Value	Required for Upgrade	Description
CREATE_DATABASE	0/1/2	Yes	<ul style="list-style-type: none"> • 0: Do not install the InputAccel Database. Only the database scripts are installed. • 1: Install the InputAccel Database. • 2: Upgrade the InputAccel Database. <p>A default value of 1 is used when this property is not specified.</p>
DB_SERVER	<i>Hostname</i>	Yes	Hostname of the SQL Server. You can use (local) or localhost if you want to use the locally installed SQL Server.
DB_PORT	<i>TCP port number</i>	-	<p>This is the TCP port on which the SQL Server listens for connections.</p> <p>The default value is 1433.</p>
DB_NAME	<i>Database name</i>	-	<p>The name of the configuration SQL database.</p> <p>The database name has the following restrictions:</p> <ul style="list-style-type: none"> • The database name can have a maximum of 122 characters. • The database name can only contain the characters 0–9, A–Z, an underscore, \$, #, @ and must begin with a number, a letter, or an underscore. <p>A default value of “IADB” is used if this property is not specified.</p>
DB_USER	<i>SQL user name</i>	Yes	The name of the SQL Server user name to connect to SQL Server.

Installer property	Value	Required for Upgrade	Description
DB_PASS	<i>SQL password</i>	Yes	The password for the SQL Server that the user specified in the DB_USER property.
INSTALLDIR	<i>Path</i>	-	The destination directory for the database application files. A default value of %ProgramFiles%\InputAccel\Database is used when this property is not specified.

InputAccel Database Installer Command-line Examples

- 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 InputAccel Database on the locally installed SQL Server which listens for connections on the default port of 1433. The default InputAccel Database name is used.

```
setup.exe /s /v"/qn ADDLOCAL=ALL DB_SERVER="(local)" DB_USER="dbcreator"
DB_PASS="password" /promptrestart"
```

- This example installs Database Manager and the database scripts into the directory specified by INSTALLDIR. IADBManager.exe is executed to install the InputAccel Database to the remote SQL Server named "CORP-SQL" which listens for connections on the default port of 1433. The default InputAccel 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"
```

- This example upgrades the InputAccel Database using the minimum parameters.

```
setup.exe /s /v" /qn CREATE_DATABASE=2 DB_SERVER= "(local)"
DB_USER="dbcreator" DB_PASS="password"
```

Related Topics —

[InputAccel Server Components Installer Properties, page 193](#)

[Client Components Installer Properties, page 206](#)

[Captiva Capture Web Components Installer Properties, page 202](#)

InputAccel Server Components Installer Properties

You can install the InputAccel Server in unattended mode using command line arguments. For 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"
```

Note:


- The root directories for each InputAccel 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.

The following table lists the installer properties that can be specified when installing or upgrading the InputAccel Server.

Table 27. Supported InputAccel Server Installer Properties

Installer property	Value	Required for Upgrade	Description
ADDLOCAL	<i>Features to install</i>	-	Features to install. The following features are available: <ul style="list-style-type: none"> • IASERVER: InputAccel Server • SERVER_DOCS: Documentation to assist with the installation process.
INSTALLDIR	<i>Path</i>	-	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 InputAccel Server instances to install. A default value of 1 is used when this property is not specified.
INSTALLATION_TYPE	Specify only if an InputAccel Database is not and will not be installed	-	Available feature: <ul style="list-style-type: none"> • NODE: The InputAccel Database is not installed. The InputAccel Server installer will install a file-based, internal database.
REGISTER_DATABASE	0/1	-	<ul style="list-style-type: none"> • 0: Do not perform DAL registration for the InputAccel Database. • 1: Perform DAL registration for the InputAccel Database. A default value of 1 is used when this property is not specified.

Installer property	Value	Required for Upgrade	Description
DB_SERVER	<i>Hostname</i>	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	<i>TCP port</i>	-	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	<i>Database name</i>	-	The name of the InputAccel Database. A default value of "IADB" is used if this property is not specified.
DB_USER	<i>SQL user name</i>	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	<i>SQL password</i>	Yes, if the previous installation included an external database	The password of the SQL Server user specified in the DB_USER property.
AC_MACHINE_USER_NAME	<i>Username</i>	-	The user account specified as the "Run-as" user for Captiva Administrator. This property is only valid when the InputAccel Server is installed on machines that are members of a Windows domain.
AC_MACHINE_DOMAIN_NAME	<i>Domain name</i>	-	The domain name of the user account specified as the "Run-as" user for Captiva Administrator. This property is only valid when the InputAccel Server is installed on machines that are members of a Windows domain.

Installer property	Value	Required for Upgrade	Description
CONFIGURE_WINDOWS_FIREWALL	0/1	-	<p>This property is only valid when the Microsoft Windows Firewall is running and enabled.</p> <ul style="list-style-type: none"> • 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	-	<p>Automatically starts the InputAccel Server service for the first instance when Windows starts.</p> <ul style="list-style-type: none"> • 0: Manual. Do not start automatically. • 1: Automatically start the InputAccel Server service for the first instance when Windows starts. The default value is 1 unless otherwise specified.
IAS<#>_ROOT_DIR where <#> is a number from 1 through 8. Example: IAS1_ROOT_DIR	<i>Path</i>	Yes, if upgrading more than one instance of the server on the same machine	<p>The destination directory for the root directory used by the InputAccel Server instance that is determined by <#>. You can have instances from 1 through 8.</p> <p>A default path of <i>WINDRIVE\IAS</i> is used when this property is not specified. For example, the path is <i>C:\IAS</i> when Windows is installed on the C: drive.</p> <p> Caution: The path length must not be greater than 109 characters and cannot be the same as the root directory for any</p>

Installer property	Value	Required for Upgrade	Description
			other InputAccel Server instance.
USE_IN_CLUSTER	0/1	-	<p>If this property is defined, the InputAccel Server will be configured for use in a cluster. Do not define this property if you do not want to use InputAccel Server in a cluster.</p> <ul style="list-style-type: none"> • 0: The InputAccel Server will not be configured for use in a cluster. This is the default value when the property is not specified. • 1: The InputAccel Server will be configured for use in a cluster. The IP address for each InputAccel 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	<i>IP address</i>	-	The IP address that the specified instance (determined by <#>) of InputAccel Server listens to for network connections. This parameter should only be used when the property USE_IN_CLUSTER is defined.
IAS<#>_IP_ADDR_V6 where <#> is a number from 1 through 8. Example: IAS1_IP_ADDR	<i>IP address</i>	-	The IP address that the specified instance (determined by <#>) of InputAccel 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	<i>TCP port</i>	-	The specified InputAccel Server instance (determined by <#>) listens to the specified TCP port number. The default value is 10099 when this value is not specified.

Installer property	Value	Required for Upgrade	Description
IA_SERVICES_RUNAS_LOCAL_SYSTEM	1/2	Yes	<ul style="list-style-type: none"> • 1: The InputAccel Server service runs using the Local System account. • 2: The InputAccel Server service runs without using the Local System account. When this option is selected, you must specify a username and password.
IA_SERVICES_RUNAS_USER_ACCT	<i>Domain \Username</i>	-	<p>The InputAccel 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.</p> <p>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.</p>
IA_SERVICES_RUNAS_PSWD	<i>Password</i>	-	<p>The InputAccel Server service uses this password with the user account specified for running this service.</p> <p>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.</p>

Topics in this section include:

- [InputAccel Server Installation Features, page 200](#)
- [InputAccel Server Installer Command-line Examples, page 200](#)

InputAccel Server Installation Features

Note: Multiple features can be specified by delimiting each feature with a comma.

The following are supported feature names that can be specified when installing the InputAccel Server:

Table 28. Supported InputAccel Server Installation Features

Feature name	Description
IASERVER	Installs the InputAccel Server sub-features that manage all client module activity and acts as the repository for all InputAccel batches, processes and other data.
SERVER_DOCS	Installs documentation to assist with the installation process.

Related Topics —

[InputAccel Server Components Installer Properties, page 193](#)
[InputAccel Server Installer Command-line Examples, page 200](#)

InputAccel Server Installer Command-line Examples

- This example installs one instance of the InputAccel 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 InputAccel 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.

```
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"
```

- This example installs one instance of the InputAccel 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"
```

- This example installs eight instances of the InputAccel Server into the directory specified by **INSTALLDIR**. All eight instances of the InputAccel service use the local Administrator user account (which has a password of "password") as the "run-as" credentials. The root directory for each InputAccel 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 InputAccel 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 InputAccel 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 InputAccel 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:\IADaFiles\"
IAS2_ROOT_DIR="\E:\IADaFiles\" IAS3_ROOT_DIR="\F:\IADaFiles\"
IAS4_ROOT_DIR="\G:\IADaFiles\" IAS5_ROOT_DIR="\H:\IADaFiles\"
IAS6_ROOT_DIR="\I:\IADaFiles\" IAS7_ROOT_DIR="\J:\IADaFiles\"
IAS8_ROOT_DIR="\K:\IADaFiles\" 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"
```

- This example upgrades the InputAccel 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" "
```

Related Topics —

[InputAccel Server Components Installer Properties, page 193](#)

[Client Components Installer Properties, page 206](#)

Captiva Capture Web Components Installer Properties

You can install Captiva Capture Web components in unattended mode using command line arguments. For 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. The list of properties is available in the table below. At a minimum you must specify the **ADDLOCAL**, **REGISTER_DATABASE**, **INPUT_ACCEL_SERVER_NAME**, **WEB_SITE_RUNAS_USER**, **WEB_SITE_RUNAS_USER**, and **WEB_SITE_RUNAS_PSWD** properties. For example:

```
setup.exe /s /v"/qn ADDLOCAL="COMMON" WEB_SITE_RUNAS_USER="Administrator"
WEB_SITE_RUNAS_PSWD="password" REGISTER_DATABASE=0 INPUT_ACCEL_SERVER_NAME
="InputAccel" /promptrestart"
```

Note: In a silent installation, SQL Server validation cannot be performed.

The following table lists the installer properties that can be specified when installing or upgrading the InputAccel web components:

Table 29. Supported Captiva Capture Web Component Installer Properties

Installer property	Value	Required for Upgrade	Description
ADDLOCAL	<i>Features to install</i>	-	<p>This is a comma delimited list of the features to install. The following features are available for installation:</p> <ul style="list-style-type: none"> • COMMON: Installs common components. • CRS_DCA_JOINT: Installs both Captiva Capture Web Client and Captiva REST Service on the same machine. <p>Note: After performing a command-line installation of the Captiva REST Service or Captiva Capture Web Client, you must configure their settings. For more information, see Installing Captiva</p>

Installer property	Value	Required for Upgrade	Description
			Capture Web Client and Captiva REST Service, page 78.
CAPWEBFILES DIR	<i>Path</i>	-	Sets the path for either the Captiva REST Service only or both the Captiva REST Service and Captiva Capture Web Client on the same machine. The default value is: C:\inetpub \captiva
CRSDCA_WEB_SITE_DESCRIPTION	<i>Website description</i>	-	The name of both the Captiva REST Service and Captiva Capture Web Client Web site. The default value is: Captiva CWC and REST Service
CRSDCA_WEB_SITE_IP_ADDRESS	<i>IP address</i>	-	The IP address of both the Captiva REST Service and Captiva Capture Web Client. The default value is: * * (asterisk) means All Unassigned.
CRSDCA_WEB_SITE_STARTUP_STATE	0/1	-	Valid values are: <ul style="list-style-type: none"> • 0: (Default) Do not make the Captiva REST Service and Captiva Capture Web Client online after installation. • 1: Make the Captiva REST Service and Captiva Capture Web Client online after installation.

Installer property	Value	Required for Upgrade	Description
CRSDCA_WEB_SITE_TCP_PORT	<i>TCP port number</i>	-	The listening TCP port of both the Captiva REST Service and Captiva Capture Web Client Web site. The default is 80.
REGISTER_DATABASE	0/1	Yes	<ul style="list-style-type: none"> • 0: Do not perform DAL registration for the InputAccel Database. • 1: Perform DAL registration for the InputAccel Database. <p>A default value of 1 is used when this property is not specified.</p>
DB_SERVER	<i>Hostname</i>	-	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	<i>TCP port number</i>	-	The TCP port to use to connect to SQL Server. A default value of 1433 is used if this property is not specified.
DB_NAME	<i>Database name</i>	-	<p>The name of the InputAccel Database.</p> <p>A default value of "IADB" is used if this property is not specified.</p>
DB_USER	<i>SQL user name</i>	-	The name of the SQL Server user to use for connecting to SQL Server.

Installer property	Value	Required for Upgrade	Description
DB_PASS	<i>SQL password</i>	-	The password of the SQL Server user specified in the DB_USER property.
WEB_SITE_DESCRIPTION	<i>Website description</i>	-	The description for the InputAccel Web Components IIS Web site. The default is InputAccel Web Components.
WEB_SITE_IP_ADDRESS	<i>IP address</i>	-	The IP address of InputAccel Web Components IIS Web site . The default is (All Unassigned).
WEB_SITE_TCP_PORT	<i>Website TCP port number</i>	-	The listening TCP port of the InputAccel Web Components IIS Web site. The default is 80. Note: Even if the specified TCP port is in use by an existing IIS website (for example, the built-in IIS default website), the InputAccel Web Components Web site is still created. However, you will need to stop the existing Web site and start the InputAccel Web Components one instead.
WEB_SITE_RUNAS_USER	<i>Username</i>	Yes	The user account under which the InputAccel Web Components run. Note: This is a required property. The silent installation quits if this property is not passed in the command-line argument.

Installer property	Value	Required for Upgrade	Description
WEB_SITE_RUNAS_PSWD	<i>Password</i>	Yes	The password of the user account specified in the installer property WEB_SITE_RUNAS_USER . Do not specify this value if the user account has a blank password.
WEB_SITE_RUNAS_DOMAIN	<i>Domain name</i>	-	The domain the user account specified in the installer property WEB_SITE_RUNAS_USER . Do not specify this value if the user is a local user and not a domain user.

This section includes the following topic:

- [Captiva Capture Web Components Installer Properties, page 202](#)

Captiva Capture Web Components Installer Command-line Examples

This command installs Captiva Capture Web Client and Captiva REST Service.

```
setup.exe /s /v"/qn ADDLOCAL=COMMON,CRS_DCA_JOINT
CAPWEBFILES DIR=c:\inetpub\captiva\test
CRSDCA_WEB_SITE_TCP_PORT=86 CRSDCA_WEB_SITE_STARTUP_STATE=1"
CRSDCA_WEB_SITE_DESCRIPTION=testing
```

Related Topics —

[Captiva Capture Web Components Installer Properties, page 202](#)

Client Components Installer Properties

You can install the client components in unattended mode using command line arguments. For 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=ALL** and **IA_SERVICES_RUNAS_NAMED_ACCT** property. For example:

```
setup.exe /s /v"/qn ADDLOCAL="ALL"
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.

The following table lists the installer properties that can be specified when installing the InputAccel client components:

Table 30. Supported Client Components Installer Properties

Installer property	Value	Description
ADDLOCAL	<i>Features to install</i>	This is a comma delimited list of the features to install. Refer to the features and components section of this document for a list of features.
IASERVERNAME	<i>Hostname or IP address</i>	The hostname or IP address of the InputAccel Server that the InputAccel client services connect to. Note: Some InputAccel client modules will not start if this property is not specified during the silent installation.
IASERVERPORT	<i>TCP port number</i>	The TCP port number of the InputAccel Server that the InputAccel 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	<i>0/1</i>	<ul style="list-style-type: none"> • 0: InputAccel client services will not be set to start when Windows start. • 1: All InputAccel client services will be set to start when Windows start. <p>A default value of 0 is used when this property is not specified.</p>

Installer property	Value	Description
IA_SERVICES_RUNAS_NAMED_ACCT	0/1	<ul style="list-style-type: none"> • 0: All InputAccel client services run using the Network Service account. • 1: All InputAccel client services not run using the Network Service account. When this option is selected, you must specify a username and password. <p>The properties IA_SERVICES_RUNAS_USER_ACCT and IA_SERVICES_RUNAS_PSWD must be specified when the value 1 is passed in.</p> <p>A default value of 1 is used when this property is not specified.</p>
IA_SERVICES_RUNAS_USER_ACCT	<i>Domain\Username</i>	All InputAccel 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.
IA_SERVICES_RUNAS_PSWD	<i>Password</i>	All InputAccel 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.
INSTALLDIR	<i>Path</i>	<p>The destination directory for the Client application files.</p> <p>A default value of %ProgramFiles%\InputAccel\Client is used when this property is not specified.</p>

Topics in this section include:

- [Client Components Installation Features, page 209](#)
- [Client Components Installer Command-line Examples, page 211](#)

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 InputAccel Client:

Table 31. Supported Client Components Installation Features

Feature name	Installs
CAPTIVA_ADMINISTRATOR	Captiva Administrator
PDEV	Captiva Designer, new samples, and Process Developer
MODULE_SERVER	Module Server Windows service.
Operator Tools	
CAPTIVA_DESKTOP	The Captiva Completion module.
SCAN_APPLICATION	The ScanPlus module.
SCAN_CLICKONCE	The ClickOnce deployable package of the ScanPlus module.
RESCAN_APPLICATION	The RescanPlus module.
RESCAN_CLICKONCE	The ClickOnce deployable package of 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.
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.
IMAGE_PROCESSOR	The Image Processor module.
PAGEREG	The Page Registration module.
Recognition	

Feature name	Installs
EASTEURO__APAC__OCR	The East Euro / APAC OCR module.
NUANCE__OCR	The NuanceOCR module.
EXTRACTION	The Extraction module.
Enterprise Export Modules	
SAPAL__EXPORT	The Archive Export module.
DCTM__ADVANCED__EXPORT	The Documentum Advanced Export module.
AX__EXPORT	The EMC 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 IBM CSSAP Export module.
ICM__EXPORT	The IBM CM Advanced Export module.
SHRPNT2__EXPORT	The MS SharePoint Export module.
LL2__EXPORT	The Open Text Livelink Advanced Export module.
Utilities	
DOTNETCODE__MODULE	The .NET Code Module.
COPY	The Copy module.
MULTI	The Multi module.
TIMER	The Timer module.
Extraction Engines	
ENGINE__GENERALUSE__OCR	The General-Use OCR engine.
ENGINE__EASTEUROAPAC__OCR	The East Euro / APAC 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	
Note: Although not listed in the installer, the Dispatcher Manager is also installed.	
DIA__CLASSIFICATION	The Classification module.
IDENTIFICATION	The Identification module.
DIA__PAL__COLLECTOR	The Collector module.
DIA__PAL__SUPERVISOR	The Auto-Learning Supervisor service.
DIA__DEV__KIT	Advanced Recognition development tools and accessories.
Legacy Modules	
DIA__CLASSIFICATION__EDIT	The Classification Edit module.

Feature name	Installs
EMAIL_IMPORT	The Email Import module.
MULTIDIRECTORY_WATCH	The Multi-Directory Watch module.

Related Topics —[Client Components Installer Command-line Examples, page 211](#)[Client Components Installer Properties, page 206](#)

Client Components Installer Command-line Examples

This command installs 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 InputAccel 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"
```

Related Topics —[Client Components Installation Features, page 209](#)[Client Components Installer Command-line Examples, page 211](#)

A

- ACL, 26
- activating, 36
 - after upgrading with a new domain, 115
 - and side-by-side installation, 36
 - considerations, 14
 - file, 36
 - InputAccel Server, 59
 - portal, 36
 - upgrade considerations, 115
- Active/Active cluster, 70
- Administration Console
 - specifying the domain on a single machine installation, 32
- arbitrary SPN, 22
- attended modules, 19
- Audit Logging, 16
- authentication, 26
- automatic
 - backup during upgrade, 112

B

- Backward Compatibility Pack, 121
- balancing client machines, 20, 24
- best practices
 - for cluster configuration, 69
 - for high availability, 34
 - for running modules as services, 20

C

- Captiva Administrator, 115
 - and security, 27
- Captiva Capture, 190
 - installing, 41
 - installing a production system, 41
 - installing on a single machine, 101
 - upgrading, 103, 123
- Captiva Capture web components

- installer command-line examples, 206
- Captiva REST Service
 - security, 27
- CaptureFlow Designer
 - upgrading XPP-based processes, 131, 140
- ClickOnce
 - and command-line arguments, 19
 - and security, 27
 - deploying modules with, 89
 - deployment prerequisites, 89
 - Deployment Utility, 89
 - host system considerations, 18
 - SSL certificate requirement, 89
- client machine
 - machine considerations, 19
- client module
 - balancing, 24
- client modules
 - and high availability, 33
 - balancing, 20
 - command-line examples, 211
 - installer properties, 206, 209
 - installing, 50
 - privileges, 26
 - table of, 169
 - upgrade considerations, 116
 - upgrading, 130
- clustering
 - Active/Active, 70
 - for disaster continuation, 34
 - installing InputAccel Server for, 69
 - licensing, 38
- CODU. *See* ClickOnce Deployment Utility
- command-line arguments
 - and ClickOnce deployment, 19
 - client module installer properties, 206
 - InputAccel Database installer
 - properties, 191
 - InputAccel installer properties and
 - feature names, 190

- InputAccel Server installer
 - properties, 193
- InputAccel web components installer
 - properties, 202
- installer, list of, 94, 96
- InstallShield switches, 189
- /l, 95
- MSI switches, 190
- msiexec.exe, 95
- /s, 95
- serviceName, 99
- setup.exe, 95
- /v, 95
- Windows Installer properties, 190
- command-line arguments for installing
 - InputAccel
 - list of, 189
- configuring
 - ScaleServer group, 67
- considerations
 - activating, 14
 - Audit Logging, 16
 - disaster continuation, 14, 35
 - failover, 14
 - high availability, 14
 - licensing, 14
 - network configuration, 13
 - performance, 13
 - scalability, 13
- Create Database Utility, 185
 - command-line examples, 187
 - silent mode, 186
- customizations
 - upgrading, 141

D

- data sharing, 24
- database
 - server considerations, 15
- demonstration installation, 32
- development installation, 32
- disaster continuation
 - considerations, 14, 35
 - creating a plan, 35
 - implementing a system, 36
 - licensing, 38
 - planning, 34
- domain
 - and activation codes, 115

- installing InputAccel in a
 - workgroup, 32
- multiple, 26, 32
- troubleshooting, 156

E

- EMC Captiva Activation Portal, 36
- escape characters for command-line
 - setup, 96

F

- failover, 33
 - considerations, 14
 - general considerations, 33
- Failover Clustering
 - InputAccel Server, installing, 69
- firewall
 - and Web Services, 19
 - configuring, 28
 - ports to open, 28
 - troubleshooting, 163

G

- general considerations
 - high availability/failover, 33
 - installation, 13

H

- hardened environment, 28
- high availability, 33
 - best practices, 34
 - considerations, 14
 - general considerations, 33
 - modular clients, 33
 - ScaleServer group, 33
- https, 27, 89

I

- identifying system requirements for
 - upgrading, 113
- IIS
 - disabling Machine Administrators
 - account, 27
- InputAccel
 - activating, 59
 - licensing, 59

- list of ports used by, 183
 - modules table, 169
 - InputAccel Database
 - Create Database Utility, 185
 - installer command-line examples, 193
 - installer properties, 191
 - installing, 45
 - security, 26
 - upgrade considerations, 113
 - InputAccel Server
 - activating, 59
 - anonymous access, 163
 - installation features, 200
 - installer command-line examples, 200
 - installer properties, 193
 - installing, 47
 - installing in a cluster, 69
 - installing multiple instances of, 65
 - scalability, 23
 - server considerations, 17
 - upgrade considerations, 114
 - upgrading, 126
 - InputAccel web components
 - installer properties, 202
 - InputAccel_Server_admin_group, 48, 101, 114
 - install planning, general considerations, 13
 - installation
 - maximum length of command line, 96
 - networking considerations, 14
 - troubleshooting command-line errors, 157
 - troubleshooting command-line failures, 157
 - troubleshooting errors, 156
 - troubleshooting failures, 155
 - troubleshooting InputAccel Database issues, 160
 - troubleshooting other issues, 162
 - troubleshooting ScaleServer issues, 161
 - troubleshooting syntax errors, 157
 - troubleshooting third-party component issues, 159
 - installation planning
 - ClickOnce host system, 18
 - client machine considerations, 19
 - client scalability, 24
 - configuring multiple domains, 32
 - database server, 15
 - development/demonstration system, 32
 - disaster continuation, 34
 - failover, 33
 - hardened environment, 28
 - high availability (HA), 33
 - InputAccel Server, 17
 - InputAccel Server scalability, 23
 - licensing and activation, 36
 - minimum Windows permissions, 28
 - performance and throughput, 14
 - running modules as services, 20
 - sample configurations, 38
 - scalability, 23
 - security, 25
 - Web Services subsystem, 19
 - workgroup installation, 32
 - installer properties and feature names, 190
 - installing, 50
 - automating silent installations, 97
 - automating unattended installations, 97
 - Captiva Capture, 41
 - clients, 50
 - command-line arguments, 94
 - command-line arguments, list of, 189
 - command-line considerations, 96
 - command-line escape characters, 96
 - InputAccel Database, 45
 - InputAccel Server, 47
 - InputAccel Servers in a clustered environment, 69
 - Module Server, 87
 - modules as services, 98
 - multiple instances of InputAccel Servers, 65
 - on a single machine, 101
 - planning for, 13
 - Process Developer, 50
 - production system, 41
 - silent installations, 94
 - unattended, 94
 - Web Services subsystem, 50
 - InstallShield switches, 189
 - irreplaceable files, preserving during upgrade, 109
- ## K
- Kerberos protocol, 22, 163

L

- /l command-line argument, 95
- language
 - setting, 61
- least-privileged user account (InputAccel Server), 26, 28, 48, 114
- licensing, 36
 - clustering, 38
 - considerations, 14
 - disaster recovery, 38
 - InputAccel, 59
 - ScaleServer, 37
 - upgrade considerations, 115
- load balancing, 24
- locale considerations, 14
- localhost, 32
- LUA, 26, 28, 48, 114

M

- maximum length of installer command line, 96
- minimum
 - cross-domain trust relationship, 32
 - permissions, 28
- modifying
 - an InputAccel installation, 151
 - unattended installations, 97
- Module Server
 - installing, 87
- modules
 - attended, 19
 - multiple service instances, 99
 - running as service, 20
 - table of, 169
 - unattended, 20
 - unregistering a service instance, 100
- MSCS cluster. *See* clustering
- MSI switches, 190
- msiexec.exe, 95
- Multi module
 - upgrading to Synchronize, 131, 140
- multiple
 - domains, 32
 - service instances, 53, 99

N

- Network Service account issues, 163
- networking

- configuration considerations, 13

P

- page count sharing in a ScaleServer group, 37
- performance, 14
 - considerations, 13
- permissions
 - minimum, 28
 - upgrade considerations, 121
- planning
 - installation, 13
 - upgrading, 103
- ports
 - and firewalls, 28
 - SQL Server, 46
 - table of, 183
 - virtual printers, 53
- pre-production testing and acceptance after upgrading, 122
- process
 - sharing, 24
 - upgrading, 141
- Process Developer, installing, 50

R

- recommendations
 - disaster recovery implementation, 36
 - RAID, 15
- removing an InputAccel installation, 152
- repairing an InputAccel installation, 152
- rolling back
 - client machines, 130
 - InputAccel Server, 127
- running Captiva Capture with minimum Windows permissions, 28

S

- /s command-line argument, 95
- sample
 - configurations, 38
 - images, 50
 - images, installing, 50
 - scripting libraries, 50
- SAN
 - and automatic real-time replication, 34
- scalability, 23
 - client modules, 24

- considerations, 13
 - InputAccel Server, 23
 - ScaleServer group, 23
 - and load balancing, 24
 - and process sharing, 24
 - compatibility, 24
 - configuring, 67
 - high availability, 33
 - licensing, 37
 - page count sharing, 37
 - troubleshooting issues, 161
 - scripting libraries, installing, 50
 - security, 25, 27
 - ACL, 26
 - Administration Console, 27
 - authentication, 26
 - Captiva REST Service, 27
 - ClickOnce, 27
 - client privileges, 26
 - considerations, 13
 - disabling the IIS Machine
 - Administrators account, 27
 - firewalls, 28
 - hardened environment, 28
 - InputAccel Database, 26
 - list of ports used by InputAccel, 183
 - SQL Server, 25
 - user accounts, 27
 - user roles, 26
 - web components, 27
 - security key, 36
 - and side-by-side installation, 36
 - upgrade considerations, 115
 - service principal name, 22
 - ServiceClass, 22
 - serviceName argument, 99
 - services
 - installing modules to run as, 98
 - multiple instances, 99
 - running modules as, 20
 - unregistering modules running as, 100
 - setspn.exe, 22
 - setting UI language, 61
 - setup.exe, 95
 - side-by-side installations, 65
 - and port assignments, 183
 - and scalability, 24
 - and security keys, 36
 - silent installation, 94
 - SPN, 22
 - SQL Server, 45
 - port assignment, 46
 - SSL certificate
 - for use with ClickOnce deployment, 89
 - Synchronize module
 - upgrading from Multi, 131, 140
- ## T
- temporary folder, 56
 - throughput, 14
 - troubleshooting, 155
 - command-line installation errors, 157
 - command-line installation failures, 157
 - domain authentication problems, 156
 - firewalls, 163
 - InputAccel Database issues, 160
 - installation errors, 156
 - installation failures, 155
 - other issues, 162
 - ScaleServer issues, 161
 - setting the UI language, 61
 - syntax errors, 157
 - third-party component issues, 159
- ## U
- UI language
 - setting, 61
 - unattended installation, 94
 - automating, 97
 - modifying, 97
 - unattended modules, 20
 - upgrade planning, 103
 - and permissions, 121
 - automatic backup, 112
 - Backward Compatibility Pack, 121
 - Captiva Administrator, 115
 - client modules, 116
 - considerations, 115
 - Documentum Server Export, 119 to 120
 - Excel Graphing utility, 119 to 120
 - IBM Content Manager Export, 119 to 120
 - identifying irreplaceable files, 109
 - identifying new system
 - requirements, 113
 - iManage WorkSite Server Export, 119
 - InputAccel Database, 113

- InputAccel Servers, 114
- licenses, activation files, and security
 - keys, 115
- new client modules, 121
- performing pre-production testing and acceptance, 122
- scheduling upgrade phases, 122
- understanding the upgrade
 - process, 113
- upgrading
 - Captiva Capture, 103, 123
 - client modules, 130
 - exiting processes and customizations, 141
 - InputAccel Server, 126
 - rolling back to a previous InputAccel Client version, 130
 - rolling back to a previous InputAccel Server version, 127
 - sample upgrade scenarios, 133
 - XPP-based processes, 131, 140
- user account, 27
- user interface language
 - setting, 61
- user roles, 26

V

- /v command-line argument, 95
- virtual printer, 53
- VMware
 - and high availability/failover the last, 33

W

- web components
 - and security, 27
- Web Services
 - Coordinator, 19
 - Hosting, 19
 - subsystem, considerations, 19
 - subsystem, installing, 50
- Windows Installer properties, 190
- workgroup
 - installing InputAccel in, 32

X

- XPP
 - upgrading XPP-based processes, 131, 140