CA IT Client Manager

Implementation Guide

12.8

CA Technologies Product References

This documentation set references to the following CA products:

- CA Advantage® Data Transport® (CA Data Transport)
- CA Asset Intelligence
- CA Asset Portfolio Management (CA APM)
- CA Common Services™
- CA Desktop Migration Manager (CA DMM)
- CA Embedded Entitlements Manager (CA EEM)
- CA Network and Systems Management (CA NSM)
- CA Patch Manager
- CA Process Automation
- CA Business Intelligence
- CA Service Desk Manager
- CA WorldView™
- CleverPath™ Reporter

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 4: Post-Installation Tasks 199

Chapter 5: Infrastructure Deployment 227

Chapter 1: Understanding CA ITCM

CA IT Client Manager is a cross-platform IT resource management solution that delivers state-of-the-art, seamlessly integrated asset management, software delivery, and remote control functionality for any enterprise.

This section contains the following topics:

DSM Architecture

CA IT Client Manager provides a common interface and architecture for asset management, software delivery, and remote control functionalities (DSM architecture), but the integration runs deeper than the administration user interface.

Core pieces of the infrastructure are shared across the asset management, software delivery, and remote control functions and components. For example, the management database, communications, process control, logging, event management, and more are all the same when you install any two or all of the functionalities. This results in useful features and consistent terminology, architecture, interface, and data across all of the functions installed.

In addition, the DSM architecture presents a set of consistent and common concepts that are also shared across the asset management, software delivery, and remote control functionalities. These shared components include the following items:

- Graphical user interface (GUI)
- Manager
- Scalability server
- Agent

The DSM architecture consists of the following tiers:

DSM Explorer/Web Console

Provide administrative control of CA ITCM and its component plug-ins. The DSM Explorer is the graphical user interface for Windows, and the Web Console is a browser-based GUI for both Windows and Linux.

Enterprise Manager

Provides a single point of administration for multiple domains.

Domain Manager

Provides all management services to lower tiers and agents.

Scalability Server

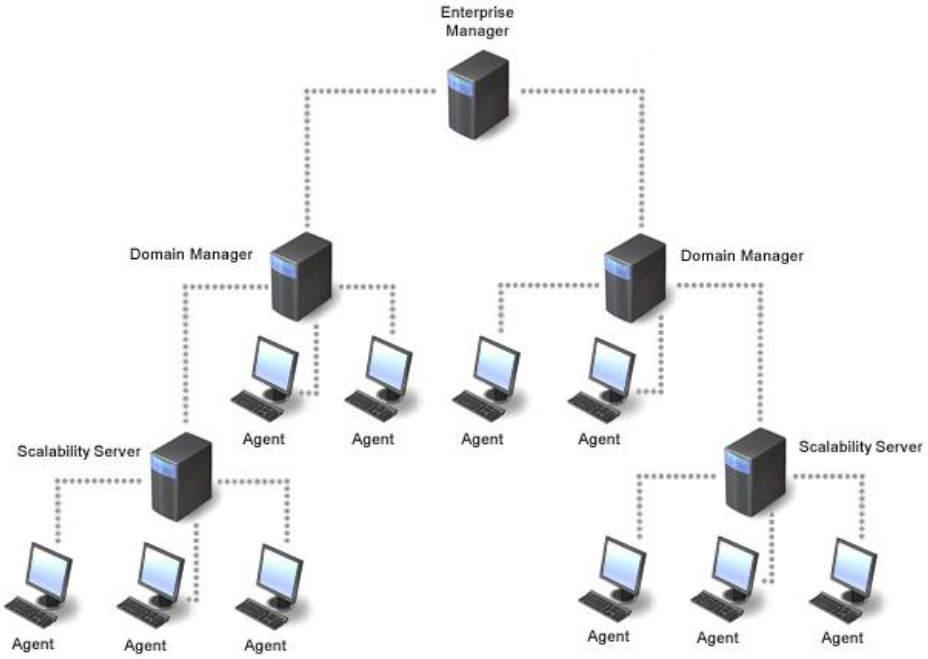
Acts as a distribution point for software delivery and distribution activities and a collection point for asset inventory.

Agent

Provides remote control, software delivery, and asset inventory services on supported hosts.

Each manager tier hosts an instance of the management database (MDB).

The following sample illustration depicts the multi-tier architecture. In this example, an enterprise manager acts as administration point for two domain managers, which each manage directly connected agents and a downstream scalability server. The scalability servers manage the tasks between the agent and the domain manager tiers.



DSM Explorer

The DSM Explorer is the main administration interface for CA ITCM, available on Windows operating environments.

The DSM Explorer bar on the left hand side offers four different views: Tree View, History, Bookmarks, and Search. The tree view is the default viewing mode, which provides the main navigation to the various features of the DSM Explorer.

When selected in the tree view, many tree nodes provide lists in the right hand view.

Many tree nodes also provide a graphical web-based presentation. One example of this is the main portal, which provides a system-wide overview of CA ITCM through four portlets:

Main Features

Provides access to the main areas of the DSM Explorer, such as Computers and Users, Software, Jobs, and so on.

Frequently Used

Provides access to the most frequently navigated tree nodes.

System Status

Displays information about the connected domain, such as statistics, failures, violations, and ongoing tasks.

Quick Start

Provides a quick access to commonly used functions.

You can customize the System Status and Quick Start portlets to your needs.

A tutorial is available in the right pane of the DSM Explorer. The tutorial contains information about navigating the DSM Explorer and getting started with the most common tasks. The tutorial can be enabled or disabled using the DSM Explorer function View, Tutorial Bar.

For additional information and context-sensitive help, see the *DSM Explorer Help*.

Web Console

The Web Console is a browser-based user interface to CA IT Client Manager and can be installed on Windows and Linux operating environments.

The Web Console can be installed on the same computer as the manager or on a different computer (remote Web Console).

Web Console Access

To access the Web Console, simply open a browser and enter the following URL in the address bar:

`http://MyManager/wac`

MyManager is the DNS name, host name, or IP address of the computer the Web Console is installed on. Web Console automatically logs you in based on the credentials you provided to log in to the computer. The Web Console login page has a drop-down that lets you specify a different manager.

Capabilities of the Web Console

The Web Console lets you access DSM objects through a simple but powerful Search panel. After an object has been located, tabs, portlets, page sections and navigation links provide a rich, browser-based interface.

The Web Console exposes the user to a comprehensive view of DSM information. Depending on the installed products and components this can include the following:

- Computers
- Groups
- Users
- Software Packages
- Software Definitions
- Jobs
- Policies
- Queries
- Alerts

The Web Console also lets the user perform the following activities: (provided the appropriate products and components have been installed):

- Create and delete Computers
- Create, modify and remove Groups
- OS installations Jobs
- Install software
- Uninstall software
- Configure software installation job
- Monitor and track Health Monitoring alerts.

The Web Console can be launched in the context of a job or policy through a URL from any other application that has access to an appropriate object's UUID.

The Web Console also has the ability to launch the CA Service Desk Manager application in the context of a ticket (issue) that has been raised as a result of a policy violation or software job failure.

Supported Web Browsers and Web Servers

See compatibility matrix for web server and browser support information.

Manager

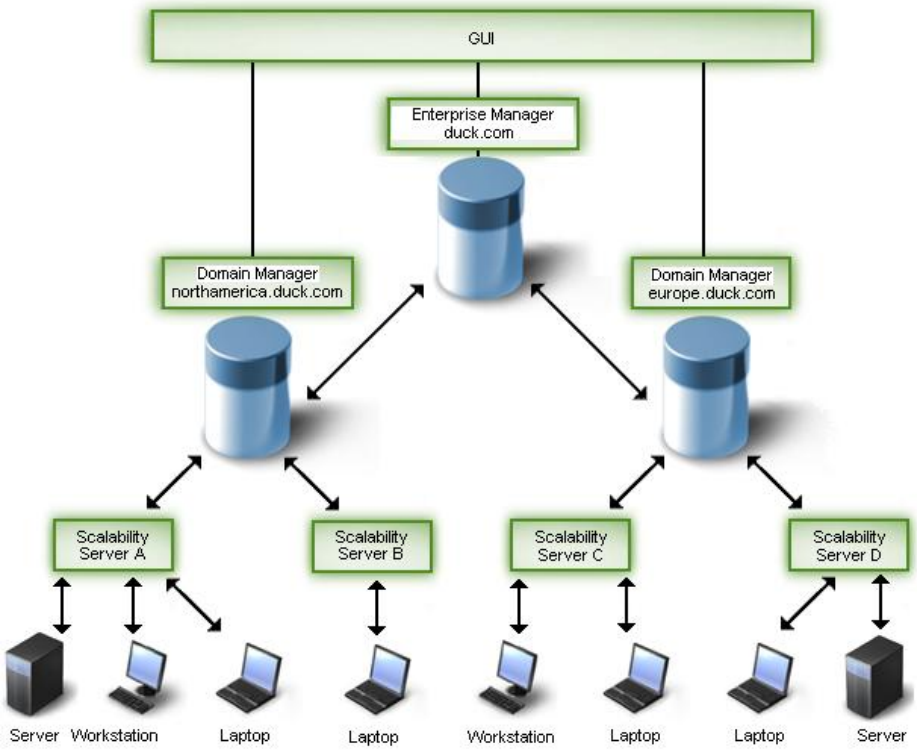
The following aspects of the manager role in CA ITCM are considered:

- Enterprise and domain concept (see page 26)
- Enterprise and domain components (see page 27)
- Engine concept (see page 30)

Enterprise and Domain Concept

CA ITCM has two management tiers, the domain and the enterprise, with management databases being present at both tiers. In situations where multiple domains are deployed within an organization, an enterprise can be deployed to provide a single point of management.

The following illustration shows an example of a two-tier architecture consisting of the company's enterprise manager and two domain managers, which have two scalability servers connected to each of them:



The enterprise manager, called duck.com, and two domain managers, one for managing tasks and devices in the North-America area (northamerica.duck.com) and the other for managing tasks and devices in the Europe area (europe.duck.com). Two scalability servers are connected to each of the domain managers to reduce the workload of the domain managers by managing end user devices such as laptops and workstations and further servers.

Enterprise and Domain Components

The following is a list of terms and definitions that are relevant to understanding the enterprise and domain concept of CA IT Client Manager.

Enterprise Manager

A *DSM enterprise manager* is an optional top management tier for CA IT Client Manager. It provides a single point of management for a group of DSM domains, and also allows setting of configurations and policies on groups of objects located in one or more domains. Only one enterprise manager should exist in a DSM environment.

Domain Manager

A *DSM domain manager* is the central point of management for the other DSM components, including scalability servers and agents.

Scalability Server

A *DSM scalability server* is a distributed process that is the primary interface for the agent. Scalability servers are intended to distribute the DSM workload across many hosts.

Engine

A *DSM engine* is a process that provides communication services between scalability servers and their parent DSM domain and enterprise managers.

The Management Database in the Enterprise and Domain Concept

CA Technologies's product suites are integrated through a common enterprise data repository, the management database (MDB). The MDB provides a unified structure for the storage of management data from all CA Technologies products. The MDB integrates management data from all IT disciplines and CA Technologies products. Customers and third-party partners can extend the MDB to include additional IT management data from non-CA Technologies software products and tools.

CA IT Client Manager is based on MDB r1.5 SP1, which by default installs only the common asset and DSM schemas. If any other CA product is going to use the MDB created by CA ITCM, and that product also supports MDB r1.5, then it should install its own schema on top of the existing MDB.

If, however, a CA product supports MDB r1.0.4 only, the installation will fail. In this case, install the MDB with the “Compatibility mode” option checked. CA ITCM will install the latest MDB r1.0.4 patches first, and afterwards the MDB will be upgraded to MDB r1.5. Hence, all schema definitions are present, and only the schema definitions for common asset and DSM are on the same level as for MDB r1.5. For more information, see either Preparing to Work with a Microsoft SQL Server MDB (see page 118) or Preparing to Work with an Oracle MDB (see page 121).

For general information on the MDB, including deployment and administration, see the *MDB Overview* which is available as part of the CA IT Client Manager documentation set (Bookshelf).

Within the multi-tier architecture, instances of the management database (MDB) can be implemented at the enterprise and domain manager tiers. Both tiers support Microsoft SQL Server and Oracle MDBs. You can also implement MDBs on different database providers on the individual tiers, for example, you can select SQL Server for the domain manager and Oracle for the enterprise manager.

In mixed configurations, for example, a domain manager with SQL Server-based MDB and an enterprise manager with Oracle-based MDB, you need the appropriate database clients on the managers; in this example, you need the Oracle client on the domain and the SQL client on the enterprise manager.

Currently, an Oracle-based MDB is supported only as a remote database on a computer running a Sun Solaris operating environment. For information about the current database versions and operating environments supported, see the *CA IT Client Manager Release Notes* which are available as part of the CA IT Client Manager documentation set (Bookshelf).

The supported database scenarios include:

Local SQL Server MDB

DSM domain or enterprise manager on Windows with the MDB located on the same computer and the MDB based on SQL Server.

Remote SQL Server MDB

DSM domain or enterprise manager on Windows with the MDB located on a remote server computer running Windows and the MDB based on SQL Server.

Remote Oracle MDB

DSM domain or enterprise manager on Windows with the MDB located on a remote server computer running Solaris and the MDB based on Oracle.

All MDBs in the enterprise and domain structure have the same schema. Any domain database holds information about how to connect to the enterprise manager. The enterprise database holds information about how to connect to all the domains that are "linked" to it, and which managers are available and where they are located.

CA ITCM provides a feature that lets you synchronize data collected on a Microsoft SQL Server MDB on a domain or enterprise manager with data on a remote SQL Server MDB or Oracle MDB. This database synchronization feature supports, for example, existing installations of CA Technologies's Service Desk Manager and Asset Portfolio Management products that use an SQL Server or Oracle MDB. For more information about the synchronization feature, see Data Synchronization from an MDB to a Separate Target MDB (see page 33).

Note: To fully support Unicenter Asset Portfolio Management product integration, you must install the RO02252 patch. For installation instructions, see the Unicenter Asset Portfolio Management readme, RO02252. For more information about Unicenter Asset Portfolio Management and CA Service Desk Manager, see their respective documentation.

MDB Installation

The management database (MDB) can be installed locally on the manager or as a remote MDB on a separate computer, depending on the requirements regarding scalability and performance. The installation of the MDB on Windows and Solaris is supported by the DSM install kits.

See the Management Database (MDB) (see page 110) section in the "Installation of CA ITCM" chapter for complete details about MDB installation.

MDB Administration

Database administration is an essential part of maintaining the health and performance of the management database (MDB). To help you with this task, CA Technologies supplies MDB maintenance scripts on the CA IT Client Manager installation media (DVD).

See the Management Database (MDB) (see page 110) section in the "Installation of CA ITCM" chapter for more information about MDB maintenance scripts. Also, for specific requirements of MDB administration regarding configuration and maintenance, see the *MDB Overview* in the CA IT Client Manager documentation set (Bookshelf).

Engine Concept

An engine is a process that provides communications services between scalability servers and the domain manager and the management database.

The functions of an engine include the following:

- Collecting computer inventory from a scalability server
- Writing configuration data to a scalability server
- Copying of data between enterprise and domain databases (replication)
- Performing dynamic query group evaluation
- Performing actions related to query group evaluation
- Executing scheduled reports
- Communicating inventory job status

Administrative Aspects of the Engine

The status of engine tasks can be viewed through the DSM Explorer. From there, engine tasks can be added, modified, or deleted.

Each instance of a domain and enterprise manager includes a default engine called System Engine.

Additional engines can be installed to relieve the workload on the default engine.

Each time a new scalability server is deployed, an engine collect task is automatically created and scheduled for the default System Engine. Another engine can be designated to handle this task during the scalability server installation process.

Each time a domain manager is linked to an enterprise manager, an engine replication task is automatically created and linked to the default System Engine.

Information Collection

The main task of an engine is to collect asset information from scalability servers.

When a DSM agent connects to a scalability server for the first time, it submits a request to be created and stores initial inventory and system information.

When an engine connects to a scalability server, it performs the following tasks:

1. Verifies the integrity of the scalability server.
2. Determines if any agents are connecting to that server for the first time.
3. If the assets are new to the whole system, creates the assets in the database.
4. Processes all inventory information provided by existing agents.

The information collected can be in the following forms:

- Inventory (hardware or template information)
- Software inventory (heuristic or signature-based)
- Configuration files (autoexec.bat or any .INI file configured to be backed up)
- Job status
- Module status
- Agent last execution date and time
- Software usage monitoring data
- Relation information (between computers, users, and devices)

Data Replication Between Enterprise and Domain

Another engine task is to handle the replication of data between domain and enterprise databases. Replication from the management database on the domain manager to the management database on the enterprise manager is carried out by a replication job that runs through the domain manager's engine process.

When replication begins, the engine determines which information needs to be pushed from the domain to the enterprise manager and also which information needs to be pulled from the enterprise down to the domain manager.

Typically, host-specific information, such as inventory attributes, is replicated upward, while configuration information, such as asset groups, is replicated downward.

With each domain manager, a default engine is installed. When the domain manager is linked to an enterprise manager, that engine is configured to perform the domain-to-enterprise replication tasks.

Database Objects Replicated

The following table lists the database objects that are replicated from the enterprise to the domain manager (down) and from the domain to the enterprise manager (up).

Object	Replication Direction
Discovered Computers	up
Discovered Users	up
Discovered Computer Users (relations between Computer and Users)	up
Remote Control Address Book Computers	down
External Assets Definitions	down
External Assets	up
Computers General Inventory	up
Additional Inventory Components **Note:** By default, these objects are not replicated. Their replication can be enabled/disabled by right-clicking the agent's Inventory/Additional/<*name-of-the module*> node and selecting the Replicate Heuristic To Enterprise option. The modified configuration is effective for all computers in this group.	up
External Assets inventory	up
Query Definitions	down
Group Definitions	down
Group Membership	down
Custom Made Software Definitions	down
Custom Defined Manufacturer	down
Enterprise Manager Properties	down
Domain Manager Properties	up
Computers Software Inventory (found based upon signature scan)	up
Software Inventory discovered by heuristic scan **Note:** By default, this object is not replicated. Its replication can be enabled/disabled by right-clicking the agent's Software/Discovered node and selecting the Replicate Heuristic To Enterprise option. The modified configuration is effective for all computers in this group.	up

Object	Replication Direction
Asset Management Jobs	down
Asset Management Job status	up
Asset Management Modules	down
Asset Management Modules Status	up
Asset Management Configuration File Definitions	down
Asset Management Configuration Files **Note:** These files are only replicated to the enterprise manager if the request to collect this information has been defined on the enterprise manager. If the request has been defined on the domain manager, the data is not replicated upwards.	up
Asset Management Template Definitions	down
Asset Management Policy Definitions	down
Health Monitoring Alerts	up

Data Synchronization from an MDB to a Separate Target MDB

In some implementations, customers want CA Technologies products such as Service Desk and Asset Portfolio Management to use management databases (MDB) separate or different from the database used by the DSM manager.

However, in many aspects of their asset management tasks these CA Technologies products rely on CA ITCM data.

Therefore, CA ITCM provides manager features that support and synchronize data discovered by CA ITCM to a separate MDB which may be based on Microsoft SQL Server (SQL Bridge) or Oracle (Oracle Bridge). The synchronization features synchronize CA ITCM assets and inventory data that are collected in an SQL Server MDB on the DSM domain or enterprise manager on Windows with the accordant data in the target SQL Server or Oracle MDB.

The synchronization is initiated through an engine task that runs at a scheduled time. You create this engine task and define the scheduling for the task using the engine task creation wizard from the DSM Explorer GUI. It is possible to use a separate engine on a remote computer to perform the synchronization.

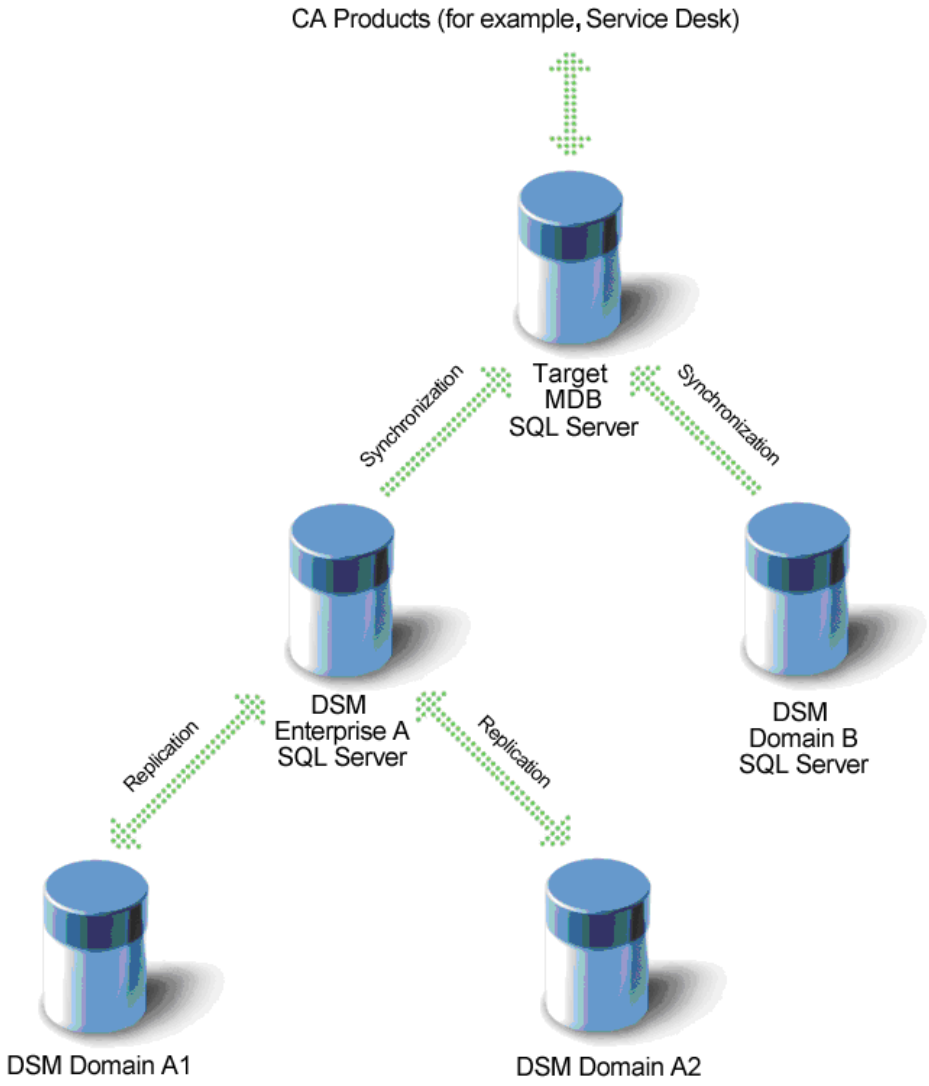
See the Management Database (MDB) (see page 110) section in the "Installation of CA ITCM" chapter for more detailed information.

Architecture of the Synchronization Mechanism

The synchronization mechanism is similar to the replication mechanism used between the DSM domain manager and enterprise manager.

The synchronization is performed in one direction, from the managers to the target MDB. This means that if synchronized data is modified on the target MDB by another process, it will be overwritten the next time the synchronization method moves that particular data set from the manager's MDB to the target MDB.

The following illustration shows a special scenario where synchronization is performed from an enterprise manager and domain manager, both hosting their MDBs on Microsoft SQL Server, to one SQL Server target MDB.



In another scenario, the target MDB may be based on Oracle. It is also possible to synchronize from one SQL Server MDB on an enterprise or domain manager to two different target MDBs.

Supported Database Scenarios

See Compatibility Matrix for the SQL Bridge and Oracle Bridge synchronization features support.

Supported Database Scenarios for SQL and Oracle Bridges

If you have installed CA Service Desk Manager or CA IT Asset Manager on an MDB based on SQL Bridge or Oracle Bridge, you can synchronize the tenant information populated by them into the CA ITCM database.

- See Compatibility Matrix for SQL Bridge and Oracle Bridge synchronization features supported database scenarios.

Support of CA Technologies Products

See Compatibility Matrix for SQL Bridge and Oracle Bridge synchronization features for SQL Server and Oracle-based MDBs supported CA Technologies products, CA Service Desk Manager and Unicenter Asset Portfolio Management:

- **SQL Bridge:**

  To take full advantage of the SQL Bridge, the test fix T5D6008 for Windows must be applied on the machines where CA Service Desk Manager r11.2 and Unicenter Asset Portfolio Management r11.3 are installed. The test fix is available at CA Support Online. Download the test fix and follow the detailed installation instructions in the readme that is provided with the test fix.

- **Oracle Bridge:**

  To take full advantage of the Oracle Bridge, a new parameter, dsm_oracle_ddl, must be added to the AMS.Properties file for CA Service Desk Manager to enable the Oracle Bridge:

  ```
  dsm_oracle_ddl=1
  ```

For more information about the installation of the SQL Bridge and Oracle Bridge in your application environment, see the Installation of SQL Bridge (see page 210) and Installation of Oracle Bridge (see page 211) sections.

Scalability Server

In CA ITCM, a scalability server provides the interface between agents and their domain manager.

At its most basic level, the scalability server allows the workload of managing individual agents to be distributed across several hosts. Rather than having all agents communicating directly with a single manager the load can be shared across multiple scalability servers. For example, software packages are staged on a scalability server before downloading to end systems, and inventory can be stored at the scalability server before being uploaded to the manager.

With virtual applications, the scalability server also functions as the streaming server for virtual application packages that are streamed to target computers running Windows operating systems.

A scalability server consists of a number of system processes that run in the background without a visible user interface.

Basic Scalability Server Subcomponents

A basic scalability server installation is made up of the following subcomponents:

- Application Framework (with registration function)
- Common server functionality

  The scalability server is able to receive registration requests and basic inventory information from agents, and to register with managers and receive or transmit various management information and notifications from and to the manager.
- File store database

  The file store database is a local repository used by the scalability server to store the information required to service the agents. In a minimal scalability server installation the file database consists of a dictionary of registered agents and the basic inventory reported by these.

Basic Scalability Server Tasks

A basic scalability server installation is able to do the following tasks:

- Provide a registration mechanism for connecting agents.
- Receive basic inventory pushed by agents.
- Register the scalability server with a manager.
- Receive scalability server configuration pushed by the manager.
- Forward agent registration and basic inventory information requested by the manager.
- Forward agent configurations pushed from the manager.

In addition, product-specific tasks can be enabled for the asset management, remote control, and software delivery (including OS installation management) functionalities.

For correct operation of the software delivery (SD) functionality of the scalability server, an SD agent is installed with each scalability server. To avoid malfunction of the scalability server, do not try to remove the SD agent from the scalability server.

In addition, it is required for the agent of the scalability server to register with that scalability server and no other. This can be verified by running "caf setserveraddress" on the scalability server with the result of "localhost" or equivalent address pointing to the local host. If the address returned points to a different scalability server, this can be rectified by running the command "caf setserveraddress localhost" on the scalability server in question.

Scalability Server and Virtual Application Deployment

The Virtual Application Package Registration Wizard (which you use to import virtual application images and create packages in the Software Package Library) creates the following software packages for each virtual application image:

- Staging—This package provides access to the virtual application for both standalone and streaming modes of package delivery. This package contains the virtual application image.
- Standalone—This package is used to install and execute the virtual application locally on the target computer.
- Streaming—This package is used to downstream the virtual application from a streaming server and execute it on the local computer.

You deploy the virtual application Staging package to the scalability server. The scalability server also functions as the streaming server for virtual applications. Therefore, Staging packages are deployed to the scalability server for streaming of the virtual application to the target computers.

The Microsoft App-V streaming server uses two protocols for streaming communications: RTSP (not secured) and RTSPS (secured). The default protocol and port for the Microsoft App-V streaming server are RTSP and port 554. If you want to use the secured RTSPS protocol with port 322, you must configure the streaming server. For information about configuring the Microsoft App-V streaming server, see the Microsoft product documentation.

You deploy the Standalone and Streaming packages from the domain manager to the target computers. You can also stage packages on the scalability server before deployment to target computers. You can use standard Software Delivery deployment methods to deploy virtual application packages to target computers.

Note: For more information about virtual application packaging and deployment, see the *Software Delivery Administration Guide*.

OS Installation Management Boot Server Installation Aspects

The OS Installation Management (OSIM) Boot Server is installed as part of a scalability server. The Boot Server installation automatically provides a TFTP server (with reduced access rights) and a PXE server.

If you do not want to use this functionality you can disable the Boot Server service during installation of the scalability server or afterwards by issuing the following CAF commands:

```
caf stop sdmpcserver

caf disable sdmpcserver
```

If you want to enable the Boot Server service again, enter these CAF commands:

```
caf enable sdmpcserver

caf start sdmpcserver
```

Agent

Agents exist on all managed end systems on all supported operating environments, where each of the agents performs individual tasks.

When an agent is registered to the ITCM Manager, the host UUID is the main attribute used to match the computer to any existing computer record in the MDB. If the host UUID does not have a match, the host name and the MAC addresses are used to match the computer.

If a match with the host name and MAC addresses is found, that means the computer's host UUID is changed. For example, OS re-installation results in the change of the respective computer's host UUID. The computer record is then updated with the new host UUID and a "Reinstall After Crash" (RAC) Software Delivery job container is created.

If no match is found on the host name and the MAC addresses, a new computer is created and no "Reinstall After Crash" job container is created.

In some scenarios, a duplicate computer could get created instead of matching to an existing record. To address these scenarios, the matching algorithm on the host name and the MAC addresses is improved. Previously, only the primary MAC address is used to match against the existing MAC addresses. Now, the complete set of the regular MAC addresses from the computer is used in the matching. The regular MAC addresses exclude the transient MAC addresses, for example, from a VPN, which could lead to the false matches.

The table below summarizes the cases, where a new computer is created and where an existing one is matched to, when any one of the host UUID, the host name or the MAC addresses change.

Note: The hyphen (-) used in the table indicates that the system ignores the search for changes.

Host UUID Changed	Host Name Changed	Regular MACs all Changed	Primary MAC Changed	New Asset Created	RAC
N	-	-	-	N	N
Y	N	N	-	N	Y
Y	N	-	N	N	Y
Y	N	Y	Y	Y	N
Y	Y	-	-	Y	N

Note: In an environment with virtual machines, e.g. XenServer, Hyper-V, ESX, the Administrator must ensure that each virtual machine has a unique MAC address within the domain space.

Note: When a computer is pre-registered, the Administrator should ensure that a regular MAC address is entered.

Concept of Agent Packages

The concept of agent packages (DSM agents) in CA ITCM separates the actual agent functionalities from individual language resources. This concept provides the following benefits with regard to agent deployment and installation:

- **Language-specific agent-only language packages**

  The agent packages concept lets you separately install language packages. A language package contains all language resources in a single language required by an agent installation.

- **Ability to create a single installation package containing just the required components**

  The dsmPush script lets you create customized single installation packages, for example, a single package containing asset management and software delivery functionalities with six language packages.

The agent packages format is a combination of agent functionality with zero or more language packages. If no language package is specified, ENU (English (U.S.)) is used by default. The ENU resources are always included as part of the agent functionality and therefore, are not in a separate language package. It is possible, however, to deploy a stand-alone language package to an agent.

Note: For more information about language packages, see Changing the Product Language After Installation in the "Installation of CA ITCM" chapter.

The DSM agent can have the following plug-ins:

- CA DSM Agent + Software Delivery plugin (SD agent)
- CA DSM Agent + Remote Control plugin (RC agent)
- CA DSM Agent + Asset Management plugin (AM agent)
- CA DSM Agent + Basic Inventory plugin (BHI agent)
- Software delivery catalog (SD catalog)
- Remote control viewer (RC viewer)
- All agent-side dependent components, for example, Data Transport Service (DTS)

Agent Configuration

Agents are centrally managed and configured by their domain manager. These tasks are performed through the DSM Explorer.

Remote Control Viewer

The remote control viewer (RC viewer) is the user interface that provides access to remote control services. When installed, you can access the RC viewer from the DSM Explorer tree or through the command line.

Remote control functionality supports a Win32 or web browser client. The browser client requires Microsoft Internet Explorer 6.0 be installed.

Some of the distinctive features of the RC viewer include:

Remote Control

Lets you feel as if you are right in front of the computer you are controlling.

File Transfer

Transfers files between viewer and host computers.

Chat

Establishes an interactive chat session with a user during a remote control session.

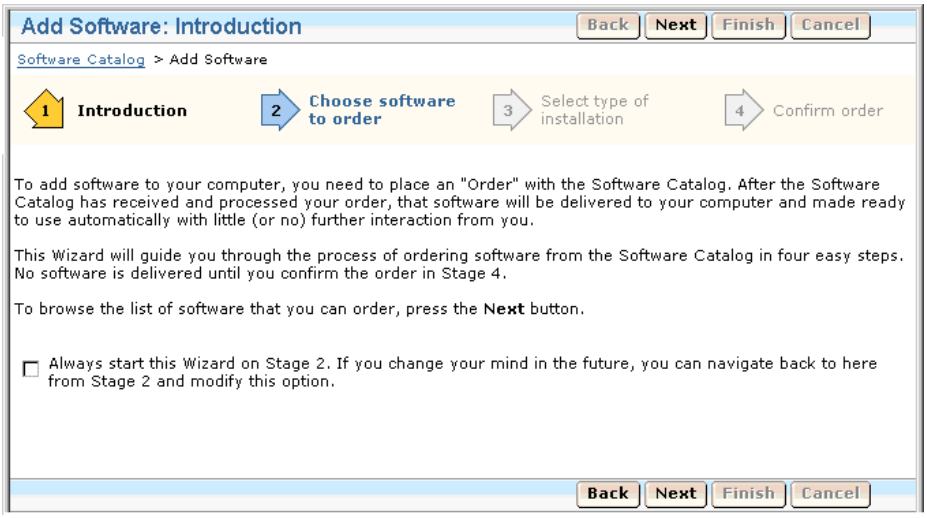
Session Recording

Starts and stops recording of the remote control session.

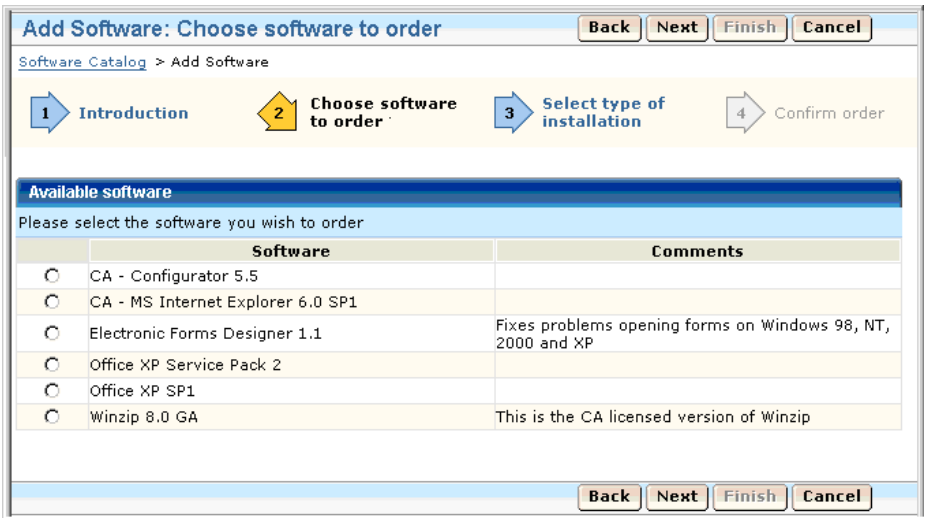
Software Catalog

The software catalog (also known as software delivery catalog or SD catalog) is an agent plug-in, which allows you "self-service". Using the software catalog's wizard based interface, you can install or remove software on your computer from a library provided by the administrator.

The following screenshot shows the "Introduction" page of the Add Software wizard:



The following screenshot shows a sample "Choose software to order" page of the Add Software wizard:



AM Remote Agent

CA ITCM supports the platform virtualization, including the following virtualized UNIX environments:

- HP nPartitions and Virtual Partitions
- HP Integrity Virtual Machines
- IBM Logical Partitions
- SUN Dynamic System Domains
- SUN Dynamic System Domains on Sun SPARC Enterprise M-series servers
- Virtual Machines running under VMware ESXi.
- Virtual Machines running under Citrix XenServer.

The AM remote agent supersedes the r12 Partitioned UNIX Server agent, but its functionality has been fully integrated with the AM remote agent. This agent is configured exclusively in the DSM Explorer to collect information for virtual hosts.

Note: For detailed information about the AM remote agent, see the *Asset Management Administration Guide*. For the most current list of supported platforms, see the Compatibility Matrix.

DSM Reporter

The DSM Reporter is a query tool used to extract information from the database.

Reports can be generated on an ad-hoc or scheduled basis. The DSM Reporter enhances the value of CA ITCM data by organizing, filtering, and presenting it. The DSM Reporter also gives the option of exporting data into CSV (*.csv) or HTML files (*.html). You can import these files later on into spreadsheets, budgeting tools, and so on.

The look-and-feel of the DSM Reporter is similar to that of the DSM Explorer. Drag-and-drop options for printing CA ITCM units and groups, and for creating new reports based on queries, add to the perception of the DSM Reporter as an extension to the DSM Explorer.

Note: When you launch the DSM Reporter for the first time after installation, make sure that you give enough time to import all the report templates into the database. However, if anything goes wrong while importing the report templates, as a workaround, open the registry editor and delete the subkey in HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Unicenter ITRM\Reporter\Library. After deleting the subkey, launch the DSM Reporter again.

Supported Operating Environments

CA IT Client Manager (CA ITCM) supports all major operating environments. For the current list of supported operating system platforms, see the Compatibility matrix.

Note: In this document, the term UNIX refers to the UNIX derivatives AIX, HP-UX, Solaris, and Mac OS X. If a system component or software feature of this release does not apply to all UNIX derivatives, this is specified in the description of the component or feature.

Common Application Framework

Each of the DSM components uses the common application framework (CAF). CAF is a cross-platform service controller that provides a single point of control for all DSM components.

CAF dynamically provides DSM services as required using an extensible plug-in model. Each CAF plug-in is a program that provides agent, scalability server, or manager functionality. A CAF plug-in can also be an extension of CAF itself and provide some common service, for example, registration with scalability servers or system event detection.

Normally, CAF starts all plug-ins automatically at boot time. CAF can also start and stop plug-ins on demand from the command line and at particular times and regular intervals using its scheduler. For a description of how to specify scheduled jobs that run in CAF, see the "CAF Scheduled Jobs" (see page 557) appendix.

CAF is also able to query plug-ins for status information and route messages from other plug-ins.

Important! On Windows, CAF is installed by default to log on as the Local System account. If for security reasons you need to change this Net Logon property, you must do this after the installation using the Computer Management, Services console from the Windows control panel. However, changing to an account with reduced privileges may result in unexpected behavior or reduced functionality of CA IT Client Manager.

Application Framework User Interface

Normally, it is not necessary to have any interaction with the application framework (CAF), as it runs as a service in the background. However, CAF provides a command line interface (caf command) that allows administrators local and remote access to CAF functionality, as in the following examples:

- Query the current status of all CAF plug-ins
- Start and stop CAF and all associated plug-ins and processes
- Start, stop, and question the status of an individual plug-in
- Enable and disable plug-ins

The CAF command line interface, in most cases, sends a message to CAF telling it to execute the command. The exceptions to this are the commands to start and stop the CAF service or daemon itself and a few configuration commands.

Note: On Windows Vista, most caf commands require full administrator rights to work. If you are a member of the administrators group but logged in as any other user apart from administrator, then a command line window will normally be running under user rights. To run caf commands, you must run the command line window by left clicking on the relevant icon and selecting Run as administrator.

System Tray

The system tray is a tool that provides user access to system services, such as the common application framework (CAF).

The system tray appears as an icon in the taskbar of desktops on any operating system except UNIX. When you right-click the icon, you can select one of the services available from the context menu. If necessary, the system tray function requests further user interaction before the service is started.

The services that are available through the system tray and the visibility of the system tray icon in the taskbar (show or hide) are determined in the configuration policy.

During the run time of CA ITCM, you can control the system tray and its icon from the command line using the following commands:

cfSysTray

Starts the system tray if its state is set to Show in the configuration policy. The icon appears in the taskbar.

cfSysTray show

Starts the system tray (if not yet started) and sets its state to Show in the configuration policy. The icon appears in the taskbar.

cfSysTray stop

Stops the system tray. The system tray icon disappears from the taskbar.

cfSysTray hide

Stops the system tray and sets its state to Hide in the configuration policy. The system tray icon disappears from the taskbar.

The CA ITCM System Tray on Linux requires that the GIMP Toolkit GTK+ 1.2 (minimum version) is installed. The GTK is not shipped with CA ITCM; you must download the required version from www.gtk.org.

Logging

The common component library (CCL) supports comprehensive tracing and has a crash handler to help you diagnose fatal errors. These services are available to and exploited by most plug-in components.

The common application framework (CAF) services log their activities into log files. The degree of detail depends on the trace level, which can be customized. The log files support you in analyzing problems.

The trace level is set to ERROR by default. If you need to get more trace information, you may want to set the trace level, for example, for the software delivery functionality or Data Transport Service to DETAIL, by running *one* of the following cftrace commands:

```
cftrace -c set -f USD -l DETAIL -s 30000
```

```
cftrace -c set -f DTS -l DETAIL -s 30000
```

The -s option sets the log file size to 30,000 KB. The default size is 2,000 KB, which might be too small for the DETAIL trace level. (The trace file is overwritten when the size limit and the number of configured trace files is reached.)

On Windows, the log files for all CAF services are located at *install_dir*\logs (Default: c:\Program Files\CA\DSM\logs).

Log files created during installation of CA IT Client Manager are located under your user temp folder. Usually the environment variable %temp% points to this folder.

On Linux, the log files for all CAF services are located at $CA_ITRM_BASEDIR/logs.

Log files created during installation of CA IT Client Manager are located under /opt/CA/installer/log.

Trace Log Files

CA ITCM components produce trace log files of their system activities while they are running. You can use these log files to analyze and troubleshoot problems that may occur.

Each CA ITCM process writes to its own trace log file. If the comstore contains a trace configuration for a process, the process writes its trace information to the defined file. If the comstore does not contain a trace configuration for a process, the process writes its trace information to a file that is named based on the process name. If there are multiple instances of the same process, you can set each instance to write to its own uniquely named trace log file. However, this function is turned off by default to prevent the creation of numerous trace files. You can turn this function on (through common configuration) to troubleshoot system problems.

If the trace level for a process is set to ERROR and an ERROR-level trace is raised, then CA ITCM writes additional INFO-level trace information to the trace log file. This additional INFO-level information gives you more data about the context of the error by providing the lower-level traces that caused the error.

You can set the parameters that control the tracing function through the ccnfcmda command line.

Note: For more detailed information about the ccnfcmda configuration agent command, type <command> /? at the command prompt.

The dsminfo Diagnostic Tool

CA Technologies provides the dsmInfo tool, which collects diagnostic information from systems that have CA ITCM installed. The data collected is compressed into a single file that contains log files, system information, directory structures, and registry and environment information. This diagnostic tool is available in the CA ITCM product installation media under the DiagnosticTools folder.

If a problem with CA ITCM is reproducible, then run the following command to change the trace level to DETAIL:

```
cftrace -c set -l DETAIL
```

Reproduce the problem and collect the diagnostic information with the dsmInfo tool.

Notes:

For more information about this tool, see the DSMInfoReadMe.txt file available under the DiagnosticTools folder in the product installation media.

The dsmInfo tool produces ".7z" files by default. These files provide better compression than zip files, so uploading to CA Technologies is easier.

Common Configuration

CA ITCM is configured centrally through a common configuration component. The common configuration component provides functions to access, store, and manage the configuration data of CA ITCM.

Configuration Parameters

The smallest unit of a configuration is a parameter. Parameters can be grouped in configuration policies that you can assign to computers or computer groups.

In the configuration model, the following objects are defined:

Parameter

Contains configuration data. A parameter has a name and contains at least one value.

Parameter information

Contains additional information about a parameter.

Parameter section

A collection of parameters that logically belong together. For example, they configure certain related functionality. Parameter sections are used to establish the hierarchical structure of parameter sets.

Configuration policy

A collection of group-specific or computer-specific parameters.

Configuration

Represents the configuration state and is assigned to a computer or computer group. The value of configuration can be planned, scheduled, active, or error.

Management of Configuration Parameters

The Default Policy, that is, the default parameter set at the manager, contains parameters intended for remote management. The Default Policy does not include those parameters that are only important for local applications running on the local computer.

There are two types of management modes for the parameters in the Default Policy: locally managed or centrally managed. The management mode of a parameter can be changed at the manager only.

- Locally managed parameters are controlled by applications that run on the local computer.
- Centrally managed parameters are controlled through policies of the manager and are read-only for local applications. Centrally managed parameters take precedence over locally managed parameters.

Some applications, for example, Remote Control, can be installed in a standalone mode. One consequence of standalone installations is that their configuration parameters are not controlled by the Default Policy of the manager and the parameter values are not reported back to the manager. The standalone mode takes precedence over the locally and centrally managed modes. You establish the standalone mode during installation of the application, for example, Remote Control.

Configuration Policies

For administrative purposes, you can group parameters into configuration policies. These policies can be assigned to computers or groups of computers.

A single computer or group can also be subjected to multiple configuration policies. In that case, the parameter settings defined in one policy may overlap with those defined in another policy. To resolve conflicts, you must comply with the following rules when configuration policies overlap:

- Policies assigned to a group are inherited by the children of the group. A child can be a group or computer.
- In a hierarchy, policies assigned on the child level override the ones on the parent level. This means that all parameters defined on the parent level are also defined for the child, but if a child policy overlaps with a parent policy, the child policy takes precedence.

Configuration Report from Agents

Each time an agent's parameter settings are changed, it reports those changes to its manager. On the manager, these settings are visible on the DSM Explorer as Reported Configuration.

Enterprise Manager Agent Configuration

The CA IT Client Manager infrastructure uses a common configuration architecture and methodology. Administrators use the DSM Explorer interface to make configuration policy changes. These changes are stored by a domain manager in the management database (MDB). Then, changes are transmitted to an agent that applies them.

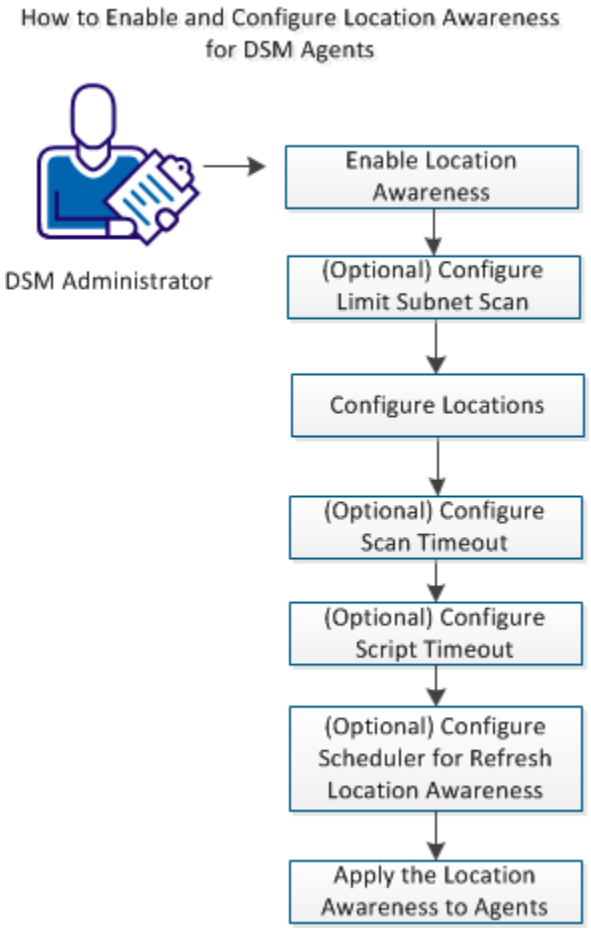
In all cases but one, this is a simple solution. However, in cases where an enterprise manager is present, the configuration management architecture becomes slightly less intuitive.

To support managed configuration, an enterprise manager must itself be managed. This requires the installation of an agent. Agents communicate with scalability servers, which then communicate with domain managers. You must decide which scalability server and domain manager will manage the enterprise manager computer.

Most organizations deploy one, and only one, enterprise manager.

How to Enable and Configure Location Awareness

As an administrator, your responsibility includes creating location awareness policy. You can configure the computer to report to an appropriate scalability server when it detects a change in location. You can apply the location awareness feature to a policy on the DSM Agents to allow the computer to evaluate the location awareness rules.



Follow these procedures:

1. Enable Location Awareness (see page 55)
2. (Optional) Configure Limit Subnet Scan (see page 56)
3. Configure Locations (see page 57)
4. (Optional) Configure Scan Timeout (see page 62)
5. (Optional) Configure Script Timeout (see page 63)
6. (Optional) Configure Scheduler for Refresh Location Awareness (see page 64)
7. Apply the Location Awareness to Agents (see page 66)

Enable Location Awareness

The location awareness feature is not enabled by default for either a clean installation or an upgrade. By enabling the location awareness policy, you can detect changes in the geographic location of an agent. When it detects a change, the agent evaluates the rules and then connects to an appropriate scalability server.

Important! Before you enable the location awareness feature, disable any other location awareness solutions that are present in the ITCM environment.

Follow these steps:

1. Navigate to DSM, Agent, Common Agent, Common, Location Awareness.

   The following location awareness parameters are displayed.

   - Enabled
   - Limit Subnet Scan
   - Locations
   - Scan Timeout
   - Script Timeout

2. Select Enabled, then click Setting Properties in the Tasks portlet.

   The Setting Properties dialog opens.

3. Select True from the Value field, then click OK.

   The feature is enabled in the policy. The policy becomes active only after you seal it and apply it to an agent..

Note:

- If the agent is running on the same computer as a scalability server, the location awareness policy is always disabled.
- If the Agent Scalability Server is marked as centrally managed, the location awareness functionality of the agent cannot modify the value after rules evaluation.

(Optional) Configure Limit Subnet Scan

You can configure the Limit Subnet Scan to allow or prevent scanning the subnet to find scalability servers in other domains.

Follow these steps:

1. Navigate to the location awareness configuration policy.

   The location awareness parameters are displayed in the right pane.

2. Double-click Limit Subnet Scan.
3. Click Setting Properties in the Tasks portlet.

   The Setting Properties dialog opens.

4. Modify the Value field as appropriate for your environment.

   Default: True

5. Click OK.

   The Limit Subnet Scan parameter is configured.

Configure Locations

Define the location rules to support changes in geographic location and let the agents connect to appropriate scalability servers. The agents evaluate the rules that you create to determine which scalability server to connect.

Follow these steps:

1. Select Locations, then click Setting Properties in the Tasks portlet.

   The Setting Properties dialog opens.

2. Click Add Row to configure the rules.

   The feature adds a row with the following parameters to the current table structure:

   - Location Name
   - Priority
   - Address Range
   - Scalability Server
   - Subnet Scan
   - Script

3. Configure each parameter, then click OK.

   The locations parameter settings are configured.

Important! The feature does not fully verify Address Range or validate the Server Name, Subnet Scan, and Script values. Be careful when you set these parameters.

Configure Priority for Locations Rule

You can specify the priority with which the feature selects which location rules to process. The agent evaluates the rules, and uses the specified priority to determine which rule to apply.

For example, you create two rules (Rule A and Rule B). Assume that you configure Rule A with priority 1 and Rule B with priority 2. If you configure all other parameters with the same values for Rule A and Rule B, the agent finds two matches. However, it applies Rule A because Rule A has the higher priority.

Follow these steps:

1. Double-click the new value under Priority.

   The Setting Properties dialog opens.

2. Specify the priority for the location rule in the Value field, then click OK.

   Highest Priority: 0

   Lowest Priority: 99999

   The priority of the location rule is configured.

Configure Address Range for Locations Rule

If the agent address matches the IP Address Range criteria, the location rule is included in the selection. The location awareness feature supports both IPv4 and IPv6 addresses. When the agent matches multiple rules, the feature uses the priority value of the rules to decide which server to use.

Follow these steps:

1. Double-click new value in the Address Range column.

   The Setting Properties dialog opens.

2. Enter the address range in the Value field, then click OK.

   Limits: The minimum value is 1 character.

   If you use IPv4, you can specify the IP Address, IP wildcard, or IP Range in the address range column. For example:

   - **IP address format:** 192.168.1.1
   - **IP wildcard format:** 192.168.1.*
   - **IP range format:** 192.168.2.1-192.168.2.100

   If you use IPv6, you can specify the various IPv6 address prefixes in the address range column. For example:

   2001:DB8::/48

   Identifies the organization, site, subsite, and subnet.48 is the length of prefix in bits, maximum allowed number of bits is 64.

   Special address prefixes:

   FE80::/64

   Used to match a link-local prefix; that is, local subnet.

   FEC0::/64

   Used to match a site-local prefix.

   ::/0

   Used to match all IPv6 addresses.

   Multicast group addresses:

   FF02::1

   Used to match all nodes on the local network segment (link-local).

   FF05::1

   Used to match all nodes on the site network (site-local).

   FF08::1

   Used to match all nodes on the organization network (organization-local).

The address range to the location rule is configured.

Configure Scalability Server for Locations Rule

The Scalability Server column values You can specifydefine the IP address FQDN (Fully Qualified Domain Name) of a scalability server for the agent to connect to, using the Scalability Server column.

Follow these steps:

1. Double-click the new value under Scalability Server.

   The Setting Properties dialog opens.

2. Enter the IP address or FQDN of the scalability server to which the agent that resides in the address range connects.

   The scalability server to the location rule is configured.

Note: If you specify the Scalability Server, leave the Subnet Scan and Script columns empty. If you are not using the Scalability Server, leave the Scalability Server column empty.

Configure Subnet Scan for Locations Rule

The subnet scan configuration defines the rule for scanning the specified subnet, and discovers any active scalability servers on that subnet. The agent then evaluates the other rules and the estimated response times of the active servers to select the best server. The location awareness feature supports both IPv4 and IPv6 addresses.

Follow these steps:

1. Double-click the new value in the Subnet Scan column.

   The Setting Properties dialog opens.

2. Enter the subnet scan in the Value field, then click OK.

   If you use IPv4, you can specify the IP Address, IP wildcard, or IP range in the Subnet Scan column.

   If you use IPv6, you can specify the various IPv6 address prefixes in the Subnet Scan column.

   The subnet scan for the location rule is configured.

Note: If you specify the Subnet Scan, leave the Scalability Server and Script columns empty. If you are not using the Subnet Scan, leave the Subnet Scan column empty.

Configure Script for Locations Rule

You can add a script to run on the agent and determine which scalability server to use. Your responsibility includes delivering the script to the agent computer.

Follow these steps:

1. Double-click the new value in the Script column.

   The Setting Properties dialog opens.

2. In the Value field, specify the name of the DM script, then click OK.

   Note: You can specify the script location as an absolute or relative path. A relative path is relative to the ITCM installation directory, which is typically at one of the following locations:

   Windows:

   C:\Program Files(x86)\CA\DSM

   Unix, Linux:

   /opt/CA/DSM

   The feature passes the following parameters to the server selection script:

   -o <output file name>

   Names the file where the script writes the name of the scalability server that it identifies.

   -x <error file name>

   Names the file where the script writes any error information it generates.

   -a <matching address>

   Identifies the address that matched, resulting in running this script.

   The DM script is configured for the location rule.

   Note: If you specify the script, leave the Scalability Server and Subnet Scan columns empty. If you are not using Subnet Scan, leave the Subnet Scan column empty.

Example:

```
rem ---------------------------------------------------------------------
rem Simple location aware server identification script
rem This script writes a hard coded server name to the output file
rem ---------------------------------------------------------------------

dim sMatchingAddress as string
dim sOutputFileName as string
dim sErrorFileName as string

dim X as Integer
FOR X=0 to argc()
```

```
            rem Read the output file from the provided parameters

            if ( argv(X)="-o") THEN
            sOutputFileName = argv(X+1)
            ENDIF

            rem read the matching address from the provided parameters

        if ( argv(X)="-a") THEN
            sMatchingAddress = argv(X+1)
            ENDIF

            rem read the matching address from the provided parameters

            if ( argv(X)="-x") THEN
            sErrorFileName = argv(X+1)
            ENDIF

    NEXT X

    dim fHandle as integer

    fHandle = OpenFile(sOutputFileName,O_WRITE)
    IF NOT(EOF(fHandle)) Then
            WriteFile(fHandle,"sampleserver.ca.com")
            CloseFile(fHandle)
            exit
    ENDIF
    exit
```

(Optional) Configure Scan Timeout

If you use the Subnet Scan, the Scan Timeout configuration determines the maximum interval that the scan waits for a scalability server to respond.

Follow these steps:

1. Double-click Configure Scan Timeout, then click Setting Properties in the Tasks portlet.

   The Setting Properties dialog opens.

2. Modify the Value field as appropriate for your environment, then click OK.

   Default: 30

   The Configure Scan Timeout parameter is configured.

(Optional) Configure Script Timeout

The Script Timeout configuration determines the maximum interval during which to run the script. The scripts stop running when the specified interval elapses.

Follow these steps:

1. Select Script Timeout, then click Setting Properties in the Tasks portlet.

   The Setting Properties dialog opens.

2. Modify the Value field as appropriate for your environment, then click OK.

   Values:

   - **0:** Infinite Timeout
   - **>0:** Number of seconds to run the script before timeout
   - **Maximum allowed timeout value:** 600 seconds (10 Minutes)

   Default: 300

   The Script Timeout parameter settings are configured.

(Optional) Configure Scheduler for Refresh Location Awareness

The Refresh Location Aware policy group folder contains a job that registers the CAF with the server at regular intervals. To change a policy parameter value, double-click a policy to display the Setting Properties dialog.

CAF Scheduler: command line

Defines the CAF command that performs this job.

Default: location aware

CAF Scheduler: Days to exclude

Lists the days to exclude from the schedule. Specify any combination of the following values: monday, tuesday, wednesday, thursday, friday, saturday, and sunday. Separate multiple values with spaces.

Default: empty

CAF Scheduler: Enabled

Specifies whether to enable the refresh registration job.

Default: True

CAF Scheduler: Hour

For daily schedules, defines the hour at which to run the job. This policy is not used for hourly and minute schedules.

Default: 12

CAF Scheduler: Hours to exclude

Lists the hours to exclude from the schedule. Specify the hours, based on a 24-hour clock. Separate multiple values with spaces.

Default: empty

CAF Scheduler: Minute

For daily schedules, defines the minute after the hour at which to run the job. This policy is not used for minute jobs.

Default: 0

CAF Scheduler: Random minutes

Defines how many minutes the feature adds to a random_minute job. The job runs at the specified time plus a random number of minutes up to the specified value. The policy runs a job "fuzzy" regular intervals to spread the server load by partially randomizing when the agents make contact.

Default: 90

CAF Scheduler: Random now time

Defines the time (in seconds) within which to initiate a random_now job. The job runs within a random number of seconds up to the specified value. This policy ensures that computers that start together do not initiate their jobs simultaneously.

Default: 0

CAF Scheduler: Repeat Number

Defines the interval between repetitions of the job. This value depends on the job type. For example, if the type is day, this value represents the number of days between the job runs.

Default: 1

CAF Scheduler: Type of Job

Specifies the type of schedule interval. The valid values are day, hour, and minute. You can also add the following optional qualifiers:

random

Runs the job with a random time added to the specified job time, up to the value of Random Minutes.

random_hour

Runs at a random hour during the day.

random_minute

Runs at a random minute during the hour.

now

Starts the job immediately after the specified job time.

Separate multiple values with spaces.

Examples:

Run the amagent job every day at 2:30 p.m.:

```
type="day", repeat=1, hour=14, minute=30, cmd="start amagent"
```

Run the amagent job when CAF starts and every day thereafter (except weekends) at a random time between 1:00 a.m. and 2:30 a.m.:

```
type="day now random", hour=1, minute=0, randomminutes=90,
excludedays="Saturday Sunday", cmd="start amagent"
```

Apply the Location Awareness to Agents

After you create and seal a policy, apply it to an asset (a computer or group).

Follow these steps: (To an Asset)

1. Navigate to the Configuration Policy folder under the Control Panel node in the tree view.
2. Right-click the policy to apply, and select Copy from the context menu.
3. In the tree view, navigate to the asset, right-click it, and select Paste from the context menu.

   The policy is applied to the asset.

Follow these steps: (To Multiple Assets or Groups)

1. Select the assets or groups in the tree view.
2. Right-click the highlighted targets and select Paste from the context menu.

   Another context menu appears.
3. Click Configuration Policies.

   The Schedule Policies dialog opens.
4. Schedule the policy to be activated.

   Note: When you apply policies to a single asset or group, the feature enables the Customize and Preview button. The feature disables the button if you paste a policy to multiple assets or groups.
5. Click OK to apply the policy to the multiple assets or groups.

You have successfully enabled and configured the location awareness feature for the DSM agents.

Inventorying and Management of Devices

The asset management functions in CA IT Client Manager (CA ITCM) provide administrators with a simple automated mechanism for inventorying and managing devices on an enterprise network, through a process of discovery and agent deployment. The provision of an installed agent onto the discovered devices allows for ongoing centralized management and control of the devices.

This section provides information about the following asset management features:

- Basic Inventory Component (see page 67)
- Non Resident Inventory Support (see page 68)

For more information about the asset management functions, components, and requirements see the *Asset Management Administration Guide*, which is part of the CA IT Client Manager documentation set.

Basic Inventory Component

The basic inventory component detects a dynamic subset of hardware information about the local computer, and makes this information available to other DSM components. The detail of inventory information depends on the hardware environment and the platform it is running on.

The basic inventory information includes the following hardware information:

- System (for example, Asset Tag, Model, Processors, or Memory)
- Operating System (for example, Language, Operating System, Service Pack, or Version)
- System Devices (for example, Network or Video Adapters)
- Network (for example, Computer and Domain Name, IP Address / IPv6, or TCP/IP)
- File Systems (for example, Local file systems or partitioning)
- System Status (for example, Last Hardware scan)

Note: Regardless of the language that CA IT Client Manager is running on, this inventory information is always available in English.

Non Resident Inventory Support

The asset management Non Resident Inventory support function (NRI) complements the inventorying functionality by letting enterprise administrators inventory their networks without making any permanent impact on the devices inventoried. NRI provides an Elective solution where end users are directed to use a Web page to collect the inventory for their system, and also a Managed solution where the enterprise administrator initiates an inventory collection through, for example, logon scripts.

NRI support uses components from the regular DSM agent in conjunction with the Asset Collector and the Web Console.

To use NRI, at least one Web Console (and the associated Web Services) and one Asset Collector must be installed for each domain manager where non resident inventory is to be collected and stored. In the simplest scenario each domain manager may co-host a single Web Console and Asset Collector. For larger and more scalable scenarios, a number of scalability servers may co-host Web Consoles and Asset Collectors.

NRI is installed as part of the asset management functionality through the setup program of CA IT Client Manager. Configuration of NRI is achieved through a simple configuration file (script file).

NRI supports inventorying on Windows, Linux and UNIX target computers. Also, the management components of NRI are supported on managers and scalability servers on Windows only.

Limitations of NRI

If you run NRI using a standard domain user account that has fewer privileges compared to the user "root" (in the case of UNIX and Linux) or administrator account (in the case of Windows), there will be less inventory reported by the NRI agent compared to the regular CA ITCM agent.

Based upon the privileges under which NRI is being executed, the NRI agent collects as much information as it can.

Note: For more information about NRI, see the *Asset Management Administration Guide*.

Chapter 2: Planning the Infrastructure Implementation

This chapter discusses important information about the requirements and scalability of CA IT Client Manager. This information should be read and understood prior to deploying any DSM components.

This section contains the following topics:

IPv6 Support

IPv6 (Internet Protocol version 6) follows IPv4 as the second version of the Internet Protocol to be formally adopted for general use. IPv6 is intended to provide more addresses for networked devices, allowing, for example, each cell phone and mobile electronic device to have its own address.

IPv6 operates on a 128-bit address base and therefore provides a tremendous address space. This huge address space allows for almost unlimited hierarchies and assignment of addresses with specific domains. It also brings improvements in auto-configuration, security, simplified routing, and other services.

CA ITCM is IPv6 compliant and can function in a pure IPv4, a pure IPv6, and a mixed IPv4/IPv6 environment.

With IPv6, network adapters may have more than one IPv6 address and also have both IPv4 and IPv6 addresses. We strongly recommend that you use fully qualified domain names (FQDN) to identify managers, scalability servers, and so on.

Restrictions in Context of IPv6 Support

The following restrictions apply in the context of IPv6 support in CA IT Client Manager (CA ITCM):

- If you have set the protocolprecedence parameter in comstore to “ipv6,ipv4” and you are using an Oracle MDB, you will find that the product tends to run slowly. This is because database connections will first try IPv6 addresses, which will fail to connect to the Oracle database, before trying an IPv4 address. To prevent this performance degradation, while continuing to use IPv6 addresses by preference in other parts of the product, please create the following DWORD with a value of 1 in the registry, HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Unicenter ITRM\ UseIPv4ForDB.
- OS Installation Management (OSIM) is only available in networks supporting IPv4. The reason is that OSIM relies on PXE, which relies on IPv4.
- CA ITCM does not support link local addresses when addressing infrastructure components, except for the following two cases:
  - When connecting from a remote control viewer to a remote control host, a link local address may be entered into the remote control viewer.
  - When using remote control to browse the local network, link local addresses are displayed and can be selected.

  Note: Link local addresses are collected and displayed as part of Inventory Collection and Display.
- The NOS download method for a software delivery (SD) job is not supported over pure IPv6 under the following conditions:
  - The agent on any platform is using Samba or NFS
  - The agent is a Windows platform older than Windows Vista and is using Microsoft NOS

  If however the Windows platform is Windows Server 2003, the following steps can be taken to enable NOS download:

  1. The following registry key must be set to 1 on the agent computers:

     HKLM\System\CurrentControlSet\Services\smb\Parameters\IPv6EnableOutboundGlobal (REG_DWORD)
  2. The two hot fix updates listed below must be applied to any agent computers wishing to mount its DSM scalability server library share:

     http://support.microsoft.com/kb/947369/en-us

     http://support.microsoft.com/kb/950092/en-us
  3. The host name of the scalability server computer must resolve to a global IPv6 address.

4. The scalability server library share (as held in the scalability server comstore) must use a host name (and not an IP address). To verify whether an IP address is being used, run the following commands:

   ```
   ccnfcmda -cmd GetParameterValue -ps itrm/usd/shared -pn exportarchive
   ccnfcmda -cmd GetParameterValue -ps itrm/usd/shared -pn msiadminpathunc
   ```

   If either command returns a value that includes an IP address, replace the address with a hostname using the following commands:

   ```
   ccnfcmda -cmd SetParameterValue -ps itrm/usd/shared -pn exportarchive
   -v IP_replaced_with_hostname
   ```

   ```
   ccnfcmda -cmd SetParameterValue -ps itrm/usd/shared -pn msiadminpathunc
   -v IP_replaced_with_hostname
   ```

   For example, if the GetParameterValue for msiadminpathunc returned \\2001:db9:1:2:f045:c89:5c2:bdf5\SDMSILIB, the new value would be \\foobar.testarea.ca.com\SDMSILIB.

   Note: For more detailed information about the ccnfcmda configuration agent command, type <command> /? at the command prompt.

In practice, if the above NOS download method fails, software delivery will fall back to using the NOSless download method. However, if the fallback is disabled by changing the default policy, the SD job will fail under these circumstances.

- Data Transport Service (DTS) WorldView dynamic container membership only supports IPv4 address ranges.
- Infrastructure Deployment and Continuous Discovery support IPv4 address ranges only.
- The Unmanaged Computers wizard, which lets the user enter one or more subnets used to filter out unmanaged computers, only supports IPv4 subnets.
- The CAF Service Locator may only work in a local subnet, which may affect the Packager that will find managers only in the local subnet. (This depends on whether routers allow scoped multicast.)
- The DTS PPP protocol does not support IPv6.
- CA ITCM does not support disabling IPv4 on Windows Server 2003 and Windows XP, because disabling IPv4 on these Windows platforms is generically not supported.
- On Windows Vista and Windows Server 2008, CA ITCM supports pure IPv6. IPv4 needs to be removed on these platforms using the following command from a command prompt:

  ```
  netsh interface ipv4 uninstall
  ```

  A message is displayed if a reboot is required.

Configuration Considerations in Context of IPv6 Support

In context of IPv6 support in CA IT Client Manager (CA ITCM), you should observe the following configuration notes and aspects.

- Configuration parameters (policy entries) in the DSM Explorer control the IPv6 and IPv4 connections, as follows:

  Define precedence of DNS lookups

  Defines the precedence of DNS queries when performing DNS queries directly, that is, not using common functions. In pre-Windows Vista operating environments, DNS is supported over IPv4 only.

  Default: ipv4,ipv6

  Define precedence of name resolution

  Defines the order of precedence of name resolution functions. In some environments, WINS and NETBIOS name resolution may be more reliable than DNS. In these cases, you can specify that NETBIOS resolution should be used in precedence to DNS lookups.

  If this parameter is set, the value of the Use NETBIOS short name fallback configuration parameter is ignored, and the name resolution will first query NETBIOS by stripping the FQDN to a short name before falling back to try DNS and other methods. If a short-name lookup due to this policy has already been performed, the short name fallback will be skipped, if enabled. This parameter is supported only on CA ITCM systems that support NETBIOS lookups.

  Note: This parameter is not currently used.

  Default: dns,netbios

  Define precedence of resolved addresses

  Defines the precedence of the IP address family (IPv6 or IPv4), when multiple IP address families are used.

  When resolving addresses, this centrally managed parameter specifies what precedence should be applied to each address family. The default is to order IPv4 addresses before IPv6 addresses to maintain maximum interoperability.

  Default: ipv4,ipv6

  Enable IPv4 resolution

  Enables support for IPv4 address resolution. This parameter is only a placeholder in the current version of the software, and therefore end nodes will ignore the setting and always support IPv4 resolution.

  Default: True

Enable IPv6 resolution

Enables support for IPv6 address resolution, allowing IPv6 addresses to be returned. If disabled (False), the resolver removes any IPv6 addresses from the name resolution results.

Note: This parameter is honored by end nodes, as opposed to the mirror IPv4 control.

Default: True

Use database for name resolution fallback

Specifies a fall back to an IP address stored either on a manager's MDB database or a server's database when a live name cannot be resolved through address location services (DNS) or NETBIOS.

Note: The default fallback option should be left as is in most cases and only changed if requested by CA technical support personnel.

Valid values are as follows:

1 = All fallback modes enabled

2 = Use server database fallback

4 = Use MDB fallback

Default: 1

Use NETBIOS short name fallback

Indicates whether NETBIOS short names are used as a fallback if the fully-qualified name (FQN) lookup fails.

Default: True

Note: These configuration parameters are located in the Configuration Policy/Default Computer Policy/DSM/Common Components/Networking/General pane. For more detailed information, see the General Policy Group (Networking) topic in the Configuration Policy section of the *DSM Explorer Help*.

- If CA ITCM is installed on an IPv4 only computer, and at a later date, IPv6 is enabled, the computer should be rebooted and the CAF service restarted.
- If your network supports IPv6 only (that is, IPv4 routing has been disabled or stopped) or is predominantly using IPv6 connections, we recommend that you change the value of the "Define precedence of resolved addresses" configuration parameter to ipv6,ipv4. This setting will improve the performance of communications between the different computers in the enterprise or domain.

- If you have a manager with a remote MDB and only IPv6 routing between manager and remote MDB, opening the DSM Explorer for the first time is very slow, because the configuration parameter "Define precedence of resolved addresses" is initially set to ipv4,ipv6 by default. In this case, the name resolves first to an IPv4 address, the database connection fails after a timeout, then the IPv6 address is tried, which succeeds. The configuration policy can be changed only after the DSM Explorer opens.
- If there are a significant numbers of Windows 2003 and Windows XP computers in your network, the configuration parameter "Define precedence of DNS lookups" should be left as ipv4,ipv6, because on these platforms DNS messages are sent only over IPv4 connections.

DNS Name Resolution for Computers Hosting DSM Components

All the computers hosting the DSM components such as, enterprise manager, domain manager, scalability server, and agents must support both forward and reverse DNS lookup. Verify that the communication between the DSM components works correctly.

Assigning a Hostname to Loopback IP

CA ITCM requires that the hostname is resolvable at all times for internal and external communications. The interactive installer contains an option, Assigned hostname to the loopback IP, which allows for the former option to be set.

For unattended installation, set the write_hostname entry to True in the networking or DNS section of autoinst.xml, as follows:

```
<networking>
  <dns>
    <dhcp_hostname config:type="boolean" >false</dhcp_hostname>
    <dhcp_resolv config:type="boolean" >true</dhcp_resolv>
    <hostname>$HostName$</hostname>
    <write_hostname config:type=boolean>true</write_hostname>
  </dns>
</networking>
```

You can find the autoinst.xml file at the following location:

DSM_Install_Folder\server\SDBS\var\managedpc\images\IMAGE_NAME\IMAGE_NAME\suse

FIPS 140-2 Support

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2) is a U.S. government computer security standard used to accredit cryptographic modules. The standard is issued and maintained by the National Institute of Standards and Technology (NIST).

Computer products that use FIPS 140-2 accredited cryptographic modules in their FIPS-accredited mode can only use FIPS approved security functions such as AES (Advanced Encryption Algorithm), SHA-1 (Secure Hash Algorithm), and higher level protocols such as TLS v1.0 as explicitly allowed in the FIPS 140-2 standard and implementation guides.

Cryptography in CA ITCM deals with the following aspects:

- Storage and verification of passwords
- Communication of all sensitive data between components of CA products, and between CA products and third-party products

FIPS 140-2 specifies the requirements for using cryptographic algorithms within a security system protecting sensitive but unclassified data.

CA ITCM supports FIPS-compliant techniques for cryptography. CA ITCM incorporates the RSA BSafe and Crypto-C ME v2.1 cryptographic libraries, which have been validated as meeting the FIPS 140-2 Security Requirements for Cryptographic Modules.

FIPS 140-2 Platform Support

To be FIPS 140-2 compliant, the use of a FIPS 140-2 certified cryptographic module is required in its certified mode and configuration. The certified RSA cryptographic module is not available for all platforms where CA ITCM is available. On those platforms where a certified module is not available but domain policy specifies FIPS 140-2 only cryptography, then the cryptographic support on those platforms only uses algorithms and functions that are FIPS approved; however, they will be provided by a non-approved cryptographic module (CA OpenSSL).

The following platforms are FIPS 140-2 compliant when operated in the FIPS-Only mode:

- Windows NT x86 Platforms
- Linux
- Solaris SPARC/32

All other platforms are currently not FIPS 140-2 compliant although, when configured to operate in FIPS-Only modes, they will only use FIPS approved algorithms and functions but not with a certified cryptographic provider.

Supported FIPS Modes

CA ITCM supports FIPS-compliant cryptography in two modes—FIPS-preferred and FIPS-only. The two modes are applicable for storage and verification of passwords, and the communication of all sensitive data between components of CA products, and between CA products and third-party products.

FIPS-Preferred mode

Refers to the mode that provides backward-compatibility with the previous releases of CA ITCM. In this mode, the Release 12.8 components use FIPS-compliant cryptography while communicating to another Release 12.8 component. However, when they communicate with the components of previous releases, they may use security functions that are not FIPS-compliant to support backward-compatibility. While FIPS-preferred is the default mode for new installations, it is the *only* supported mode for upgrades.

Note: After you have upgraded all the DSM components in your environment, you can switch to FIPS-only mode.

FIPS-Only mode

Refers to the mode that uses only the FIPS-compliant techniques for cryptography. Use this option for *new* CA ITCM installations. This mode is not backward-compatible with the previous releases of CA ITCM.

Note: After you switch to FIPS-only mode, the components cannot use legacy cryptography. You can switch back to FIPS-preferred mode if necessary.

More information:

How to Switch to FIPS-Only Mode (see page 418)
How to Switch to FIPS-Preferred Mode (see page 419)

Failover Support and Hardware Replacement

CA IT Client Manager supports failover in a clustered environment and also replacing manager hardware in case of a hardware failure or hardware upgrade.

For detailed information see the sections:

- Failover Support (see page 77)
- Replacement of Manager Hardware (see page 79)

Failover Support

The failover support is available only for Windows operating environments and Microsoft SQL Server databases.

Failover supports installation of the manager components on two different computers running Microsoft Cluster. One system needs to be the active node running the manager functionality and the other (or maybe others) are standby passive systems, having the manager software installed but not activated.

Installing on a Cluster

CA ITCM has no functionality in place to detect system failures and to automatically switch from the active to the passive node in case of a system failure.

CA ITCM can be installed in two modes: either as an Active ITCM Manager or as a Passive ITCM Manager. The terms "Active" and "Passive" refer to whether the DSM manager is active or passive; they do not refer to the Cluster Node (which may itself be active or passive).

When installing CA ITCM in a cluster, one instance of the DSM manager will be installed as the Active ITCM Manager and each of the other instances will be installed as a Passive ITCM Manager.

To install an Active ITCM Manager

1. On the cluster's Active Node, launch the CA ITCM installer in the usual way and perform a custom installation.
2. Select the Manager components plus CCS and any other components that are to form part of the installation.

   CCS is a mandatory component when installing in a clustered environment; CCS will install the High Availability Service option, which is needed for cluster support.
3. In the Configure Manager dialog, enter the name of the Management Database Server.
4. Click the Recovery button.
5. In the dialog that appears, select the Enable Recovery Support and Active options.
6. Enter the name of the cluster and the location of the shared drive.

   Note: If you want to install a DSM domain manager with a local Microsoft SQL Server in a Microsoft Cluster environment, CA ITCM must be installed into the Microsoft SQL Server Cluster Group using the Microsoft SQL Server virtual name.

7. Continue through the installation, until you reach the Choose Destination Location dialog where you configure the Destination folder .

   The Destination folder must be somewhere on the computer's local disk (not the shared cluster disk).

   The location of the configuration data must point to the cluster's shared disk. This is done automatically based upon the information entered in the "failover" dialog. However, you may review these locations by clicking on the Advanced button. The location of the Shared Components must also be on the computer's local disk; this location is configured using the same Advanced button.

8. Click Next and continue through the installer dialogs until the installation starts.

   The installation of a manager on a cluster computer is slightly different from that on a standalone, non-clustered computer. Usually the installation of CCS is silent. However, on a cluster CA ITCM will invoke an interactive installation of CCS.

   Important! Do not change any of the information in any of these dialogs, as CA ITCM has populated them with the appropriate values; simply click Next through the dialogs until the CCS install starts.

To install a Passive ITCM Manager

1. Before installing on the other computer (or computers) in the cluster, you must make sure that the cluster groups are available and the shared resources are functional. Alternatively, make the computer the active node in the cluster.
2. Launch the CA ITCM installer in the usual way and perform a custom installation.
3. Select the same components that were selected in the Active ITCM Manager installation.
4. In the Configure Manager dialog, enter the name of the Management Database Server.
5. Click the Recovery button.
6. In the dialog that appears, select the Enable Recovery Support and Passive options.
7. Next, the installer asks for the location of the DSMRecovery.ini file.

   This is located in the CA ITCM configuration data directory, which will be on the cluster's shared disk. The actual location would have been defined during the installation of the Active ITCM Manager.

8. Click Next and continue through the installer dialogs, and start the installation.

   As with the Active ITCM Manager installation, the installation of CCS is performed interactively.

   Important! Again, do not change any of the information in any of these dialogs, as CA ITCM has populated them with the appropriate values; simply click Next through the dialogs until the CCS install starts.

Once the installations are complete, then the cluster resources can be moved back to the cluster's active node.

Now when the Active Cluster Node switches between computers in the cluster, the Passive ITCM Manager must be notified. This is achieved by running the ActivateManagerNode.bat file that is located in the bin directory of the DSM manager's installation location. Alternatively, if a cluster management system is to be used, then the cluster manager can be configured to execute the content of the ActivateManagerNode.bat file.

Notes:

- For more information about setting up clusters, see the green paper titled CA ITCM/CA Unicenter Desktop & Server Management at http://ca.com/greenbooks.
- If installing to a non-default named SQL instance ensure that the TCP/IP port numbers of the instance are the same on all nodes of the cluster. If this is not the case, modify the port numbers accordingly. Also ensure that SQL-Server Browser is running.
- Currently, a boot server is not supported on a cluster.
- On Windows 2008 (and Windows Vista) the ActivateManagerNode.bat command file must be run with full administrator rights. If you are logged in as the administrator user, this user automatically has full rights by default. If, however, you are logged in as some other user who is also in the Administrators group, then Windows arranges matters so that this user only has ordinary user rights and, therefore, cannot run this command file successfully. To change this, the ActivateManagerNode.bat command file must be run as the elevated user. For example, to open an elevated command line window, right-click the Command Prompt icon and select Run as Administrator. The command file can then be run from there.

Replacement of Manager Hardware

It is possible to replace the manager system hardware in case of a system failure or hardware upgrade in that way that the original MDB and configuration settings can be used furthermore.

There is no need to reinstall the MDB or reconfigure the software delivery library or remote control address books because the original configuration can be used.

To prepare for cases where the manager system needs to be replaced, you must do some settings in the installation wizard. In the Configure Manager dialog a button called 'Recovery' leads into the failover dialog. In the failover dialog, you must select the 'System Replacement' and 'Enable Replacement' options. In the dialog for the install directories, set the directories for manager data (MDB and configuration data) to a path which needs to be backed up regularly. During installation all input given through the various dialogs is stored in a file called DSMRecovery.ini and is saved at the specified configuration data location. With this file, it is possible to replace the hardware in case of a crash.

If the hardware has been replaced and the manager needs to be reinstalled, run the 'Recovery' dialog again, select 'Enable Replacement', and the option 'Replacing system'.

At the bottom, the installation path for the configuration data must be entered so that the installer can find the originally stored DSMRecovery.ini. The installer reads all installation parameters and uses the same MDB, software library, and so on, as in the original manager installation.

The relative path to the configuration data must be the same as it was for the active manager.

Replacing the manager system requires that the old manager hardware and the new manager hardware are using the same system name.

Note: In case of computer hardware failure consistency of data cannot be ensured.

Configuring CA HIPS for CA ITCM Installation

If you are installing CA ITCM on a machine that has a CA Host-Based Intrusion Prevention System (CA HIPS) client installed, you must configure the CA HIPS server before you can install CA ITCM on the client machine.

To configure CA HIPS for CA ITCM installation

1. On the CA HIPS server machine, log on to the CA HIPS console.
2. Click Policy Management, Definitions, Application Repository.
3. If the groups list does not contain a SafeApps group, create a group called SafeApps and follow these steps:
    a. Click Policy Management, Definitions, Common Settings, OS System Security Globals.
    b. Select SafeApps in the Application Group to Bypass User Mode Hooks drop-down list and click OK.
    c. Click Policy Management, Definitions, Application Repository.
4. Select the group SafeApps.

5. Click Add New and enter the following details to define the setup.exe:

Field	Value
Member Type	Application
Member Name	setup.exe
Identify By	FileName
Path	setup.exe
Groups	SafeApps

6. Click OK.
7. Click Add New and enter the following details to define the CACMS.MSI:

Field	Value
Member Type	Application
Member Name	CACMS.MSI
Identify By	FileName
Path	CACMS.MSI
Groups	SafeApps

8. Click OK.
9. Click Policy Management, Deployment.
10. Click Deploy.
11. Specify a version number and click OK.
12. Wait for the policy to be activated on the CA HIPS client machine.

    The CA HIPS client machine is now ready for the CA ITCM installation.

Infrastructure Component Considerations

The relationship between the various components of CA ITCM is as follows:

- Agents have a many-to-one relationship with their scalability server. Each agent must report to one, and only one, scalability server.
- Scalability servers have a many-to-one relationship with their domain manager. Each scalability server must report to one, and only one, domain manager.
- Domain managers have an optional many-to-one relationship with an enterprise manager. Each domain manager may report to one, and only one, enterprise manager.

Infrastructure Installation Steps

A successful infrastructure installation is achieved by the following high-level methodology:

- Determine appropriate component placement

  This step includes deciding which machines will take on what role, based on considerations such as network bandwidth, existing system load, and other aspects.
- Check your network for proper configuration

  The DNS configuration must allow for successfully operating “nslookup *IP_address*” among vertical connections down the CA ITCM tier hierarchy (enterprise manager – domain manager, domain manager – scalability server, scalability server – agent, domain manager – agent).
- Install the enterprise and domain managers
- Install scalability servers
- Install agents
- Install DSM Explorer administrative consoles

Infrastructure Sizing Key Factors

There are a number of key factors having a considerable impact on the infrastructure sizing and system performance.

Load on Asset Management Tasks

The infrastructure size is affected by the load on the following asset management tasks:

- The number of inventory attributes collected
- Frequency of inventory collection

Load on Software Delivery Tasks

The infrastructure size is affected by the load on the following software delivery tasks:

- Size of software packages to deliver
- Quantity of software packages to deliver
- Network bandwidth management
- Frequency of software package delivery (daily, weekly, monthly, and so on.)

Computer Identification in CA ITCM

CA ITCM assigns each managed computer a CA Technologies-specific Universal Unique Identifier (UUID). It is stored on each computer at the following locations:

Windows registry:

`HKEY_LOCAL_MACHINE\Software\ComputerAssociates\HostUUID`

Linux/UNIX:

`/etc/cadmuuid`

The CA ITCM application framework (CAF) checks the locations for a CA Technologies-specific UUID periodically. If a UUID is found, CAF assumes that this asset has already been registered in the database. If the UUID is not found, CAF creates a new UUID and registers the asset to the database.

If you have copied an installation (physical dump of the hard disk using an imaging tool such as GHOST or image file of a virtual machine using a tool such as VMware) to install on another computer or to use as a backup, the copied installation contains a CA-specific UUID of the original computer. If you start the copied installation on a computer other than the original one, the CA-specific UUID would appear twice.

To prevent the duplication of CA-specific UUID, CA ITCM performs the following actions:

1. When CAF starts or when the “caf register” command is issued, an algorithm that verifies if the target computer is the original computer or another computer is executed.
2. If the target computer is the original computer, the original CA-specific UUID is used; else, a new CA-specific UUID is created.

To detect the need for a unique CA-specific UUID, CA ITCM can use either the default algorithm (recommended) or the legacy algorithm. The algorithm checks for the following characteristics of the target computer against the values in the database:

Virtual machine

System ID (a system BIOS attribute) is the only characteristic checked by the algorithm.

Physical computer

- MAC address compliance

  If one of the MAC addresses matches with one of the original MAC addresses of the target, this criterion is fulfilled.

- Hard disk serial number compliance

  If one of the hard disk serial numbers matches with one of the original hard disk serial numbers of the target, this criterion is fulfilled.

- System ID compliance

  If the System ID matches with the original System ID of the target, this criterion is fulfilled.

A change in the values of the preceding characteristics does not necessarily require a change in the CA-specific UUID. The following are the considerations for the algorithm to initiate a change in the CA-specific UUID:

- A change in the value occurs only if the original value of the characteristic exists in the database and the new value is different from the original value.

  For example, if the old list of MAC addresses is not available in the database for comparison, a change in the CA-specific UUID will *not* be initiated.

- A change in the value occurs only if the new values of MAC addresses or disk serial numbers match with the existing values in the database.

Lock Host UUID

A hardware change usually results in the change of the host UUID. If you do not want to change the host UUID, you can lock the host UUID.

- To lock the host UUID on Windows, you must create a string value LockHostUUID with value “1”, under the registry key HKLM\Software\ComputerAssociates\HostUUID.
- To lock the host UUID on Linux or UNIX, create a file named /etc/calockuuid.

Default Algorithm (Recommended)

The default algorithm detects both the IDE and SCSI disks (Legacy algorithm detects only the IDE disks) and determines the change in host accurately when compared to the legacy algorithm.

After the algorithm checks the characteristics of the target computer, a CA-specific UUID is generated in the following scenarios:

- The hard disk serial numbers have changed; in addition, the MAC addresses or the System ID has changed.
- The hard disk serial numbers are not detected and both System ID and MAC addresses have changed.

Note: For a virtual machine, a change in the System ID triggers a new host UUID.

Legacy Algorithm

To use the legacy algorithm for computer identification in CA ITCM, you must enable the legacy algorithm.

Important! You should enable the legacy algorithm before you upgrade or start a new installation. If you change to legacy algorithm after the upgrade or installation, the legacy algorithm will generate incorrect CA-specific UUID's.

To enable legacy algorithm, use one of the following methods on Windows, Linux, or UNIX:

- To enable legacy algorithm on Windows, you must create a string value LegacyHostUUID with value “1”, under the registry key HKLM\Software\ComputerAssociates\HostUUID.
- To enable legacy algorithm on Linux or UNIX, create a file named /etc/calegacyuuid.

Note: You must enable legacy algorithm on every computer running a CA ITCM agent.

For a physical computer, the algorithm checks for the three characteristics described earlier. If at least two of these three criteria are not met, the target system is regarded as a new computer and a new CA-specific UUID is generated.

Important! UUIDs generated by earlier versions of CA Technologies’s desktop management software, such as Unicenter® Software Delivery, Unicenter® Asset Management, and Unicenter® Remote Control, may not be globally unique.

Computers Roaming Between Domains

A computer can report to several different domain managers. Roaming functionality avoids duplicate entries on the enterprise manager when a computer moves between domains that are linked to the same enterprise manager.

Computers that report to a different domain will have their information (that is, delivered software, inventory attributes, and so on) moved to their new domain manager.

The computer will be deleted from the domain that it has roamed from. By default, this task is done by software delivery functionality (if installed). If software delivery functionality is not installed or configured to not preserve job history, removing the computer is done by the replication job.

Example: A Roaming Computer

Domain managers A and B are both linked to the same enterprise manager. A computer X registers to domain manager A and gets replicated to the enterprise manager. Then computer X registers to domain manager B.

Before domain manager B replicates computer X to the enterprise manager, it checks if a computer with the same UUID (that is, CA Technologies-specific UUID or hostuuid) already exists on the enterprise. It finds computer X from domain A and knows now that this computer X has roamed from domain manager A to domain manager B. The “domain A/computer X” account is deleted on the enterprise manager by the domain manager B replication and a roaming notification is stored in the enterprise manager's database. The “domain B/computer X” account is replicated to the enterprise manager. Before domain manager A replicates changes or new computers, it checks if there are any roaming notifications. It will find the one for computer X and delete it on domain manager A. (If there is a software delivery agent installed on the roaming computer, it is not deleted immediately.)

The computer X has now successfully roamed and now only exists as “domain B/computer X” in the enterprise manager's environment.

Customizable Logoff or Reboot Banner

When software delivery or remote control functions initiate a logoff or a reboot of the target computer, the application framework (CAF) displays a dialog that shows a banner bitmap and tells the user what is happening.

You can replace the default banner bitmap with one of your own by creating a bitmap image file (with file extension .bmp) 500x65 pixels in size. Store this file on a local disk or a network share and set the Common Components/CAF/General/CAF Dialog: bitmap filename configuration policy to the path name of the file. When the dialog is displayed, it reads this file and displays the image.

Use of a Custom Reboot Program

The Common Application Framework (CAF) usually forwards system reboot requests to the operating system to perform the actual reboot. It is possible to use a custom reboot program, which is able to take special requirements into consideration.

To enable and to configure the use of a custom system reboot program, the following configuration policy settings are available in the ...DSM/common/caf/general configuration policy group:

CAF: Reboot command

Specifies the name of the custom reboot program to use instead of the operating system API. If no reboot program is specified, the operating system API is used.

CAF Dialog: Enable dialog

Specifies whether a countdown dialog is displayed (value = True) or an immediate reboot without countdown dialog takes place (value = False). This is useful on specialized hardware which may not allow user interaction with a dialog.

Reboot and Log Off Dialog on Terminal Servers

During a reboot operation, a dialog is displayed that tells you what is happening and when. It provides a number of buttons which grant some control over the process.

Reboot now

Starts the reboot now rather than wait for the indicated timeout.

Defer

Defers the reboot for a while, allowing you to complete or save your work.

Cancel

Aborts the reboot.

On a computer where you are the only user, this works fine because no one else is affected. On a terminal server, however, there could be many users so the rules have to change. In this case, all the buttons are disabled because pressing any one could affect all other users without their knowledge or consent. In addition, since the computer is "owned" by the system administrator, only he or she has the rights to control the reboot process.

During a log off operation, however, the Logoff now button is enabled because that affects only you. The Defer and Cancel buttons are still disabled.

Location of Web Services Documentation and WSDL File

The *Web Services Reference Guide* can be found in the following places:

- Main CA IT Client Manager documentation system
- At the following locations if the Web Services have been installed:

  http://%*machine_name*%/UDSM_R11_WebService/help/index.htm (on Windows)

  http://%*machine_name*%/UDSM_R11_WebService/help (on Linux)

If the Web Services have been installed, the *WSDL file* can be found at the following locations on Windows:

- http://%*machine_name*%/UDSM_R11_WebService/wsdl

%*your_install_directory*%\CA\DSM\webservices\wsdl

On Linux the *WSDL file* can be found at the following location:

- %*your_install_directory*%/CA/DSM/webservices/wsdl

Web Console and Web Services Considerations

Following are the installation and integration considerations involving the Web Console and Web Services.

Installation Packages Required for the Web Console

The following table lists the third-party and CA Technologies packages that are prerequisites for the Web Console:

Package	Operating System	Description/Comment
AMS	Windows and Linux	CA Technologies component for Asset Maintenance System AMS is used by the Web Console to view information about owned and discovered assets.

Package	Operating System	Description/Comment
AMS	Windows and Linux	CA Technologies component for Asset Maintenance System AMS is used by the Web Console to view information about owned and discovered assets.
Apache Webserver	Linux	Component that hosts the Web Console application. If you want to use a specific version of the Apache Webserver, you must set the CA_DSM_USE_APACHE_PROG variable to the full path of the binary rather than its parent directory before you start the installation of CA IT Client Manager. For example: CA_DSM_USE_APACHE_PROG=/apache2.2.8/bin/httpd
Apache Tomcat	Windows and Linux	Servlet container for the Web Console
Apache Tomcat Connector for ISAPI	Windows	Connector between Internet Information Services (IIS) and Tomcat
Apache Tomcat Connector for Apache (mod_jk)	Linux (32, 64 bit)	Connector between Apache Webserver and Tomcat
Oracle JDBC Driver	Windows and Linux	JDBC driver used to connect to an Oracle database.
Apache Axis	Windows and Linux	WebService toolkit
CA CMDB	Windows and Linux	Configuration management database
CA Service Desk	Windows and Linux	
Microsoft IIS	Windows	Microsoft Internet Information Services Component that hosts the Web Console application
Log4j	Windows and Linux	Logging toolkit
Microsoft SQL Server JDBC Driver	Windows	JDBC driver used to connect to an SQL Server database.
Microsoft SQL Server JDBC Driver	Linux	JDBC driver used to connect to an SQL Server database.

Package	Operating System	Description/Comment
AMS	Windows and Linux	CA Technologies component for Asset Maintenance System AMS is used by the Web Console to view information about owned and discovered assets.
Sun JRE	Windows and Linux	Sun Java Runtime Environment Required for Web Console when using IPv6.

Important! The modification of the key SQLServer.PortNo with the database port number in the file wacconfig.properties is no longer supported. You must provide the correct port number during the installation as it cannot be modified later.

Installing Web Admin Console (WAC) or Web Services on 64-bit Linux Machines

CA ITCM does not support 64-bit Apache Web Server on the Linux machines. Uninstall any 64-bit Apache Web Server before you install CA ITCM Web Console or CA ITCM Web Services on a 64-bit Linux machine.

Tomcat Port Usage by Web Console

The Web Console uses the Apache Tomcat web servlet engine. The default Tomcat port numbers used are 8090 (startup), 8095 (shutdown), and 8020 (AJP).

The Tomcat ports screen gets populated during the installation. The user is expected to give the proper port number during installation.

The Tomcat port used by the Web Console can be found in the server.xml file under the system install path.

On Windows, the location of the server.xml file is as follows:

`[installpath]\Web Console\conf\server.xml`

On Linux, the location of the server.xml file is as follows:
`[install_path]/webconsole/conf/server.xml`

Tomcat Port Configuration for Web Console

It may be the case that one or all of the default Tomcat ports are already used by other CA Technologies applications already installed on the computer. The Web Console installer checks for ports that are already in use and automatically allocates new port numbers appropriately.

The applications using the clashing port numbers must be running at the time of installation in order for them to be detected. If they are not running, manual steps need to be taken post-install to resolve the port number clashes. Different applications that try to use the same port numbers may fail to start. Typically the first one to start will succeed and subsequent applications will fail.

To change the port numbers that the Web Console uses

1. Stop the Web Console instance of Tomcat, if it is running, by opening a command console and typing:
   `caf stop tomcat`
2. Open the server.xml file in a text editor.

   The file should contain entries that look something like this:

   ```
   <Server port="8095" shutdown="SHUTDOWN" debug="0">
   ```

   ```
   <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
       port="8090" minProcessors="5" maxProcessors="75"
       enableLookups="true" redirectPort="8443"
       acceptCount="100" debug="0" connectionTimeout="20000"
       useURIValidationHack="false" disableUploadTimeout="true" />
   ```
3. Modify the port numbers *nnnn* in the port="*nnnn*" assignments (there are two of them in the example above) to available free ports.
4. Save the file and exit the text editor.
5. Start the Web Console instance of Tomcat by opening a command console and typing:
   `caf start tomcat`

If you are unsure of what port numbers may be being used by other applications try incrementing all the port numbers by 1. Then start the applications, and if you still have problems repeat the above process.

Deploying a Standalone Web Console

You can deploy Web Console either on the DSM Manager computer or on a different computer. We recommend that the computer that hosts the standalone Web Console, and the computer that hosts the MDB and the domain manager are in the same subnet (in the same geographical location) to achieve optimal performance.

Web Console: CMDB Viewer

The Configuration Management Database (CMDB) viewer (or visualizer) is a web-based user interface that displays the relationship between the different configuration items in the CMDB database. Two prerequisites are that the CMDB should be installed on the same MDB as the domain manager, and that the Service Desk Integration configuration policy should be applied on the computer where WAC is installed.

The CMDB viewer can be launched from the Quick Launch section of the homepage, as follows:

computer/Homepage/Quick Launch/External Applications/CMDB Visualizer

The CMDB viewer must be separately installed and is not included as part of the CA ITCM installation.

Internal Dependencies

Some of the DSM components have internal dependencies to other DSM components. During installation, the selected components are checked for internal dependencies. If they depend on other DSM components, these components are automatically also installed.

For example, in the context of software delivery (SD) functionality, the scalability server functionality requires an SD agent on the same system. Therefore, even if the agents have not been selected for installation, the SD agent gets automatically installed, if the scalability server has been selected for installation.

The following lists show the dependencies resulting in automated installation of additional DSM components:

Manager:

Component	Requires ...
Manager (SD)	All DTS components (manager and agent) on the same system. Scalability server, if it is a domain manager.
Manager (enterprise or domain)	Asset management manager plug-in. Engine
Enterprise manager	DTS agent
Web Console	Web Services

Server:

Component	Requires ...
Scalability server (SD)	SD agent on the same system DTS agent

Agent:

Component	Requires ...
Catalog (SD)	SD agent on the same system

Dependencies to Other Products on Windows

Some of the MSI installation packages have dependencies to other third-party products. Some of them are installed automatically by the CA ITCM Installer, whereas others must be ordered and installed by the customer.

CA ITCM Installation Package	Third-party Prerequisite	Part of the Install Image?	Master Setup installation? (*)
Explorer - Reporter plug-in	DB Client	No	No
Manager - all plug-ins	For MDB - DB Client or local DB Server	No	No
Manager - Asset Management plug-in	SUN Microsystems J2SE JRE (Java Runtime Environment)	Yes	Yes - JRE is part of the Manager install and gets automatically installed during custom installation or by installing the manager using MSI command line
Web Services	Microsoft Internet Information Server (IIS) 7.0 **Note:** The default installation of IIS 7.0 does not install the components required Web Console, install ISAPI Extensions and Filters before you install Web Console	No	No

CA ITCM Installation Package	Third-party Prerequisite	Part of the Install Image?	Master Setup installation? (*)
Web Console	Apache Jakarta Tomcat 5.5.12	Yes	Yes - Tomcat is part of the manager install and gets automatically installed during custom installation or by installing the manager using MSI command line
	Oracle J2SE JRE 1.7.0_17 (Java Runtime Environment)	Yes	Yes - JRE is part of the manager install and gets automatically installed during custom installation or by installing the manager using MSI command line
	AMS 1.6.2	Yes	Yes, only during custom installation

(*) Some of the packages marked with 'Yes' for automated installation are installed only when using the interactive installation wizard. They are not installed by calling the MSI package directly. This behavior depends on the technology and format used for these packages provided to the CA ITCM Installer.

Therefore, when distributing manager components to other systems using software delivery functions or the deployment wizard, some prerequisites must be manually installed first before the component package gets installed.

How to Install the Prerequisites Manually on Windows

To support you with the installation of the prerequisites for installation packages, some command examples and proceedings are provided here.

- **Installing CA Asset Maintenance Sytem (AMS):**

  ```
  WindowsProductFiles_x86\AMS\setupwin32console.exe -P
  installLocation="c:\Program Files\CA\DSM\Web Console\webapps\AMS" -V
  SERVERNAME="manager_system_name" -V WEBPORT="Tomcat_startup_port" -V
  DASSERVERNAME="mdb_servername" -V INGRESLISTENER="db_instance_name" -silent
  ```

- **Installing MSAARDK:**

  ```
  WindowsProductFiles_x86\MSAARDK\MSAARDK.exe /R:N
  ```

If anything is required to be installed from the command line or a batch procedure, we suggest the following approach. The best way to figure out what needs to be installed and what command lines are to be executed, a template install for the particular combination of manager functionality should be done. The Installer creates several log files under the %temp% directory. The command can be found by opening the DSMSetup.log and searching for 'Launch ciCCSSetup'. This leads to the section of commands executed to install the different components.

Further searches for 'Launch' can be done, which will show you the sequence of msiexec commands to install the following:

- AMS
- Agents
- Scalability server
- DSM Explorer
- Manager
- and so on

Each command line shows the properties to be used when calling the command and may be copied into the automation script. All relevant parameters are explained in the Installation Tool msiexec (see page 161) section.

In the case of a manager installation, the MDB needs to be installed and configured as the first package before installing anything else.

Dependencies to Other Products on Linux and UNIX

In the Linux and UNIX versions of CA IT Client Manager, third party components such as the Java Runtime Environment are embedded in the DVD images as PIF or RPM packages, and are installed as required when a DSM package is installed. No separate manual installation steps are usually required.

However, on some Linux versions, runtime compatibility libraries must be installed prior to installing DSM components. For further details see Compatibility Libraries for Linux.

The System Tray on Linux requires that the GIMP Toolkit GTK+ 1.2 (exactly this version) is installed. The GTK is not shipped with CA IT Client Manager; you must download the required version from www.gtk.org.

Comprehensive control of package selection is available during Linux and UNIX installation using response file settings in conjunction with the /R command line option to the installation command. Full details of the options available are described under Installation of CA ITCM Using the Command Line in Linux and UNIX (see page 183).

Restarting Apache on Linux

If you need to restart Apache, do not restart Apache using a Linux GUI because it does not pick up the environment required by CA IT Client Manager. Instead, for example, you can go to a shell and start Apache from there by using this command:

```
dsm_restart_apache [-f]
```

The -f option starts Apache if it is not currently running.

If you do not specify the -f option and Apache is not running, Apache will not be started. If Apache is already running, it will be restarted.

Chapter 3: Installation of CA ITCM

The following chapter provides information about the general process and requirements of CA ITCM installation. You may skip some sections at the beginning of the chapter that contain very specific notes and information regarding installations of DSM components and read the introduction to the installer and the installation process. Descriptions of interactive installation and installation using the command line then follow.

This section contains the following topics:

Understanding the Installation Process

The installation process consists of three major steps:

1. Preparation Phase
2. Interview Phase
3. Execution Phase

During the preparation phase, you investigate the product options and gather all required information necessary for installation as delineated in the first sections of this chapter. You will need to verify existing or install missing software prerequisites, and select and start the installation of any other product functions shipped with the installation media.

During the interview phase, you provide the information that you gathered in Step 1 by stepping through the installation wizard pages or by preparing a response file. For example, you specify the language of the installation and the product to install, the installation type (express or custom installation), and relevant configuration settings to get the installed components up and running.

Lastly, you execute the installation instructions using the information entered in Step 2.

You can install and remove product components interactively using the installation wizard. In addition, many installation and configuration parameters and properties can be specified and changed through a command line interface.

Introducing the Installer

The CA ITCM Installer provides install routines to install basic product functionalities and optionally further CA Technologies products as plug-ins.

Express and custom installation options are available. The express installations provide quick availability of some management features, whereas the custom installation option provides greater flexibility and more granular feature selection options.

You can select the product functionalities you have purchased, and proceed with either an express or custom installation. All users have the option of selecting product functionality for which they have not purchased a license, which will result in a 30-day trial period.

Prerequisites and Restrictions

Please note the following prerequisites and restrictions when installing CA ITCM Release 12.8:

- You must have Microsoft SQL Server or Oracle as database provider.
- For Oracle, the manager installation requires the database administrator "sys" password to be provided during the installer interview. For SQL Server, the DB Administrator and DB Administrator Password fields are hidden; the installer will use a trusted SQL Server connection to install the MDB and set up the DSM manager.

Installation Methods

After selecting the product functionalities to be installed, you can choose the installation method and continue through the prompts in order to start distribution and configuration of the product.

The following installation methods are available:

Express Installation

Installs a standalone domain manager including scalability server, agent, DSM Explorer on Windows

Express Agent Installation

Installs all features required to manage an end system. Ideally, the domain manager or scalability server that will manage this end system should already have been installed somewhere on your network

Custom Installation

Lets you select or deselect individual product components and modify installation settings.

Installation Considerations

The following considerations apply when you want to install the MDB on Oracle 11g:

- At a minimum, an Oracle 11g Client must be installed.
- While installing a DSM manager with an Oracle MDB, if you choose to install the CCS component, you must have a C: drive and must leave the default installation path for the CCS component unchanged.
- CA ITCM supports only the EZCONNECT method of connection from the DSM manager to the Oracle database. For more information about setting the connection method to EZCONNECT, see the Oracle documentation.
- The DSM manager cannot be installed on the same computer as the Oracle 11g 64-bit Server or Client, because it requires the Oracle 11g 32-bit Client. If the MDB is installed on an Oracle 11g 64-bit Server, this server has to be remote from the DSM manager.
- Both IPv4 and IPv6 are supported between the DSM manager and the MDB.
- A minimum of 2 GB is recommended for both the System Global Area (SGA) and Program Global Area (PGA).
- The installation log is found in the temp directory and is named mdb-schema-setup.log.
- Enter the correct sys, mdbadmin, and ca_itrm passwords during a reinstall or upgrade.
- The MDB PIF package supports unattended installation from a response file on Windows and Linux/Solaris.
- If the underlying database is Oracle, provide the mdbadmin credentials to connect to datasource. Also, add the AIADMIN role to mdbadmin before running the extraction.
- Verify that JRE 1.7 it is available on the Windows computer where you want to install the MDB Admin Console. Also verify that the environment variable JAVA_HOME is set and points to the JRE installation folder.
- MDB Admin Console uses Hibernate technology for accessing MDB objects. Download Hibernate 3.2.0 from http://sourceforge.net/projects/hibernate/files/ and make it available on the computer where you want to use MDB Admin Console.

More information:

Installation Prerequisites (see page 105)

Miscellaneous Installation Considerations

When Windows Terminal Services is configured in Application Server Mode, The following settings are required:

- Use the CONSOLE mode when performing installation from remote access.
  Example:

  mstsc /v:HostName /console

- Change the terminal server USER settings to INSTALL before the installation.
  Example:
  change user /install

- Execute the following command to verify the user settings:
  `change user /query`

Note: For more information about the Windows Terminal Server CHANGE USER utility, see support. microsoft.com/kb/186504.

More information:

Installation Prerequisites (see page 105)

Installation Considerations Related to FIPS

The following installation considerations apply when you are installing CA ITCM in one of the FIPS modes:

- All the DSM components on a computer use the same FIPS mode. For example, if you are installing an asset management agent on a computer that already has the Release 12.8 software delivery agent, the former will operate in the same FIPS mode as the latter.
- All the manager components, such as engine, web services, Web Console, and Reporter, must use the same FIPS mode that the manager uses.
- For clustered deployments, you can select the FIPS mode only for the first node; all the other nodes operate in the same mode as the first node.

Selecting the FIPS Mode During Installation

You can select the FIPS mode when you install CA ITCM interactively using the installer, or silently using command line, msiexec, or infrastructure deployment (DMDeploy). The default mode is FIPS-preferred.

Note: You cannot specify the FIPS mode when you modify or repair CA ITCM installation. If you want to change the FIPS mode of the DSM components after installation, switch to the required mode. For more information about switching to a particular FIPS mode, see Security Features section.

This section describes how you can modify the FIPS mode when you use various installation methods and options:

Interactive Installation

The CA ITCM installer provides an option to select the FIPS mode in the FIPS-compliance section when you install the product. Select the check box to enable the FIPS-only mode for the components you are installing. The installer does not provide this option when you modify or repair an installation.

Note: You can select the FIPS mode only during a custom installation. Express installation always installs CA ITCM in the FIPS-preferred mode. For a stand-alone remote control agent installation, you can specify the FIPS mode during both custom and express installations.

Installation using Command Line, msiexec, or DMDeploy

You can specify the following parameter for setting the FIPS mode when you perform a silent installation using command line, msiexec, or DMDeploy:

Windows:

```
FIPS_MODE=1 //(FIPS-preferred)
FIPS_MODE=2 //(FIPS-only)
```

Linux or UNIX:

```
/RITCM_FIPS_MODE=1 //(FIPS-preferred)
/RITCM_FIPS_MODE =2 //(FIPS-only)
```

Note: The FIPS mode parameter is ignored if you are modifying or upgrading an existing DSM component, or installing an additional DSM component on the target. In the former case, the FIPS mode is set to FIPS-preferred; in the latter case, the FIPS mode of the new component is the same as the existing component.

Installation Using Software Delivery

You cannot specify the FIPS mode when you use software delivery to install or upgrade DSM components. The FIPS mode is decided based on the following factors:

- If the target already has a DSM component installed, any further installation through software delivery will use the same FIPS mode as the existing component. Otherwise, the FIPS mode is set to FIPS-preferred.
- If you are upgrading a DSM component, the FIPS mode is set to FIPS preferred, just like any other upgraded component.
- You cannot specify the FIPS mode when you modify or repair a CA ITCM installation.

In all the cases, the manager can override the FIPS mode by applying the configuration policy that sets the FIPS mode.

Installing Automated Migration

Installation Prerequisites

Verify that the following installations are available in your enterprise before you begin the installation:

- CA IT PAM Version 03.0.00 and Service Pack 03.0.01 or CA Process Automation 03.1.00 and Service Pack 03.1.01 or CA Process Automation 4.1 SP1.

  Note: Optionally, you can install CA EEM for identity and access management. If you want to install CA EEM on a Windows 64-bit environment, follow the instructions in *EEM_Install_64.pdf* before the installation.

- If you are using Oracle MDB and CA IT PAM Version 03.0.00, you must install the CA IT PAM patch, ITPAM_3.0_11182010_OracleJar_HF_19813962 on your CA IT PAM installation.

  Important! Stop the CA IT PAM Orchestrator service before applying the patch.

Installation Considerations

The following considerations apply to Automated Migration:

- Automated migration supports DSM domain managers and hence cannot be applied on DSM enterprise managers.
- Automated migration applies only to the default domain manager linked with the Web Console. If the Web Console is linked to multiple domain managers, the automated migration functionality will only be available when connected to the default domain manager.
- Automated migration can be installed only on one Web Console instance per domain manager. If multiple Web Console instances have the same default manager, you must install Automated Migration on only one of the Web Console computers.
- Automated migration is only supported on Windows operating environments.
- When you modify or uninstall Automated Migration, if WAC Manager is installed on a remote computer, verify that CAF is enabled.

Configure Automated Migration

Before you can use automated migration, complete the following tasks:

1. Configure CA IT PAM User Account in CA ITCM
2. Enable SSL for Web Console and Automation Web Services
3. (Optional) Modify Automation Servunice Configuration File

Note: For more information see Automation Service Configuration File (see page 497)

Multi-Language Installation

At the beginning of a CA ITCM installation a dialog invites you to select the language during installation. If your local environment is in one of the supported languages, this language is already pre-selected as the default language. If you select another language the installer runs in that language.

To support multi-language installation of CA IT Client Manager, the installation media (DVD) has, in addition to the original English version, the product available in other languages.

The language in which you select to run the installer is not necessarily the language in which the product will operate. During the installation, you will be asked to select the languages in which the product should operate, and the languages you want to be made available for the product in the Software Delivery and Infrastructure Deployment software libraries.

Irrespective of the language you have chosen for the installation of CA ITCM, CA Common Services (CCS) will always appear in English.

If no language setting is supplied (during an unattended installation), the system default locale is used, provided such a language package is available. If the system default locale is not one of the supported languages, the installer falls back to English (U.S.).

Important! To support localized hostnames, that means, hostnames in non-US English (non-ENU) language locales, it is required that the underlying Domain Name System (DNS) infrastructure supports UTF-8 character encoding in DNS.

More information:

Changing the Product Language After Installation (see page 199)

About Agent Language Package Creation and Installation

CA IT Client Manager provides language-independent base packages for the Basic Hardware Inventory (BHI) agent, asset management (AM) agent, remote control (RC) agent, and software delivery (SD) agent. The language-independent base packages already include the English (ENU) language package; therefore, there is no separate English (ENU) language package.

Administrators can create their own set of agent packages using the dsmPush script and specify which agent they want with which language. This must be done on the manager computer with the DVD inserted in the disk drive.

The dsmPush script builds installable units that contain a language-independent base package for an agent role plus the desired language packages. If specified in the command line, dsmPush imports these installable units in the software delivery or infrastructure deployment libraries. Using dsmPush with the "-single" parameter, the administrator can force that only a single package is imported in the libraries.

A language package can be installed at the same time as the base package or it can be subsequently installed in a separate step. The installation of a language package runs completely unattended.

We recommend that you register language packages with software delivery and infrastructure deployment using the dsmPush script.

Note: For detailed information about the dsmPush tool, see the *CLI Reference Guide*.

The agent installation does not import packages into the Infrastructure Deployment library; it only installs the agent and a language package (if it is not an ENU installation). But if there are multi-language agent packages already installed, the Installer will upgrade the multi-language agents without installing a language package.

The interactive installation offers a selection of different language packages that can be installed and in which the product will operate, and which will be imported into the Software Delivery and Infrastructure Deployment software libraries.

Special Agent Installation Scenarios

The following list provides some relevant information about special agent installation or upgrade scenarios:

- **Agent Procedures on Composite Packages**

  When the dsmPush script is used to build composite packages consisting of one or more agent base package and language packages, the only procedures available for the composite package in the Software Package Library (displayed in the DSM Explorer under *domain*, Software, Software Package Library, Software Packages, *package*, Procedures) are Install for Linux, and Install and Uninstall for Windows.

  If you want to run a product-specific action, for example, the software delivery (SD) agent's Scan SWD procedure, run the procedure from the language-independent SD agent base package in the Software Package Library.

- **Installation of a Stand-alone Remote Control Agent**

  A stand-alone remote control (RC) agent cannot be installed using SD functions, because an SD agent must already be present on the agent host. (And a stand-alone RC agent must really be stand-alone; it cannot coexist with any other agent plug-in.)

  The only way to install a stand-alone RC agent is either interactively or using the Infrastructure Deployment wizard and specifying the extra parameter /RITRM_RC_AGENT_STANDALONE=1. Therefore, the 'Standalone Agent' RC agent procedure is not relevant for a composite package in the Software Package Library.

Required Hardware Configuration

Hardware specifications depend on numerous parameters including network architecture, available bandwidth, frequency of operations, size of operations, and number of end systems. For example, if you are installing a software delivery manager, the total amount of hard disk space required depends largely on the size and number of software packages and OSIM operating system images being managed.

See the "Hardware Specifications and Requirements" section of the *CA IT Client Manager Readme* for the hardware requirements that must be met or exceeded for CA IT Client Manager to install and run properly.

Management Database (MDB)

The DSM manager requires a management database (MDB). For the most current list of supported platforms, see the Compatibility Matrix on CA Support.

MDBs can appear in the following configurations:

- **Local configuration**—The manager and the database are running on the same computer.

  In CA IT Client Manager, this applies only to an MDB based on Microsoft SQL Server. Both the manager and the MDB are installed in a Windows operating environment.

- **Remote configuration**—The database is located on computer A and the manager is installed on computer B and is using a client to connect to the database on computer A.

  In CA IT Client Manager, this applies to both Microsoft SQL Server and Oracle MDBs.

  For an Oracle MDB, the remote configuration is mandatory. Actually, the DSM manager is located on a computer running Windows and the Oracle MDB is installed on a computer running a supported Sun Solaris operating system.

Within the multi-tier architecture, instances of the management database (MDB) can be implemented at the enterprise and domain manager tiers. Both tiers support Microsoft SQL Server and Oracle MDBs. You can also implement MDBs on different database providers on the individual tiers, for example, you can select SQL Server for the domain manager and Oracle for the enterprise manager.

In mixed configurations, for example, a domain manager with SQL Server-based MDB and an enterprise manager with Oracle-based MDB, you need the appropriate database clients on the managers; in this example, you need the Oracle client on the domain and the SQL client on the enterprise manager.

Before the installation of CA IT Client Manager starts, either the database server (for local configuration) or the database client (for remote configuration) has to be installed.

During the installation of CA IT Client Manager, you select the database type.

MDB PIF Package

You can use the package as a standalone MDB installer.

Standalone MDB Installation

You can invoke the MDB PIF package as a standalone MDB installer by running the setup script (setup.bat or setup.sh) from the appropriate MDB directory:

```
<DVDROOT>\WindowsProductFiles_x86\mdb
```

```
<DVDROOT>/LinuxProductFiles_x86/mdb
```

```
<DVDROOT>/SolarisProductFiles_sparc/mdb
```

The MDB PIF package as a standalone installer supports new MDB installations, reinstallations, and upgrades to a local or a remote target database server.

For Oracle, the standalone MDB PIF package tests whether the Oracle Client is at the Oracle 11g Release 2 level.

More information:

Remote MDB Installation for Oracle (see page 128)
How to Install an Oracle MDB (Standalone) (see page 123)
Install the DSM Manager: Oracle MDB (see page 125)
Install the DSM Manager: Microsoft SQL Server MDB (see page 120)
Unattended MDB Installation Using a Response File (see page 117)
Remote MDB Installation for Microsoft SQL Server (see page 120)

PIF Installation Records

The MDB installer does not leave any PIF installation records on the source computer that is invoked. As a result, you can reuse the source computer to install the MDB to a different target remote computer. No PIF installation records are left on the latter.

The MDB installer does, however, write its version number into the ca_settings table to assist maintenance.

Old PIF installation records on the remote MDB computer are not removed on an MDB upgrade, whether performed locally or remotely. You can remove these old installation records manually on Solaris with the lsm –e command.

CCS Considerations

There are two variants of CA Common Services (CCS) installed with CA IT Client Manager: a pared-down version, known as Micro-CCS (English-only), and the original full version. Micro-CCS (English-only) supports Event Management and Calendars, but does not support WorldView (used for DTS network configuration) or discovery (including continuous discovery). The full version of CCS r11.2 (English-only) is for use only with a Microsoft SQL Server MDB.

The Installer automatically chooses the appropriate variant during installation. Note that the variants cannot coexist on a single host, although they can coexist on different hosts within a network. Also note that Micro-CCS cannot be upgraded to full CCS.

The following tables summarize which variant of CCS is installed with the various operating environments and MDBs:

Linux:

Installed Component	CCS Variant
Agent	None
Scalability server without calendars	None
Scalability server with calendars	Micro-CCS; event agent only

Note: CA IT Client Manager never uses full CCS on Linux.

Windows:

Installed Component	CCS Variant
Agent	None
Scalability server without calendars	None
Scalability server with calendars	Micro-CCS; event agent only
*Manager with local SQL Server MDB	Full CCS
*Manager with remote SQL Server MDB	Full CCS; must be installed on MDB host, should also be installed on CA ITCM host
Manager with remote Oracle MDB	Micro-CCS on CA ITCM host only; event agent plus event manager

* Makes no difference whether clustering is used or not.

UNIX:

No variant of CCS is installed.

Note: When installing a Domain Manager with CCS, using a SQL Server named instance causes the CCS installation to fail. For CCS to install successfully using a named SQL instance, the SQL Server Browser service must be running. You can start the SQL Server Browser service from the SQL Server Configuration Manager.

CCS Installation Error Messages

Note that installation of CCS calendars only with a scalability server is reliable. The following messages can occur when a *full* CCS installation is performed with a DSM manager. All the failures here relate to interaction between CCS and a SQL Server-based MDB.

Error Text (in %TEMP%\ TRC_Inst2_ITRM.log)	Conditions	Diagnoses and Solutions
The MSSQLServer service is not running on \\local_host.	The MDB is remote; local and remote hosts are not in the same domain.	This message is misleading because contact is not being established with the remote MDB host. Add the local host to the same domain as the remote host.
Specified password for user nsmadmin is invalid.		■ The nsmadmin account already existed in SQL Server and the password specified during the DSM install was different. Either (a) delete all DSM/CCS logins and DB users from SQL Server before starting the install, (b) specify a matching password during the DSM install, or (c) change the nsmadmin password in SQL Server to match what will be specified during the DSM install. ■ The nsmadmin password does not satisfy the system password strength criteria. Make the password stronger.
The supplied MDB credentials are not valid		The nsmadmin account was already defined to SQL Server; the MDB itself may or may not exist. We get this even if the nsmadmin password matches what is already in SQL Server. Delete the DSM/CCS login(s) and DB user(s) from SQL Server so that it is clean.

Error Text (in %TEMP%\ TRC_Inst2_ITRM.log)	Conditions	Diagnoses and Solutions
The MSSQLServer service is not running on \\local_host.	The MDB is remote; local and remote hosts are not in the same domain.	This message is misleading because contact is not being established with the remote MDB host. Add the local host to the same domain as the remote host.
There are active processes connected to one or more databases that will be used by this product. Gracefully shut down those processes to close database connections before initiating the installation so as to maintain data integrity and system stability. [In %TEMP%\ITRM.CCS\wizint.log or %TEMP%\DSM_CCS_wizint.log.]		Other remote CA ITCM managers are sharing the MDB, for example: 11:36:50 ** Active DB Processes ** 11:36:50 DB Processes for 11:36:50 DB Name = mdb, Node = UNI6505L3-065, Process = CA IT Client Manager r12 11:36:50 DB Name = mdb, Node = CMQA158, Process = CA IT Client Manager r12 11:36:50 DB Processes for 11:36:50 ** End DB Processes ** 11:36:50 There are active processes connected … This is unlikely to happen in practice unless the whole CA ITCM system is misconfigured or is being configured in the wrong sequence. Temporarily shut down the remote processes. The log file shows which remote hosts are involved.

Error Text (in %TEMP%\ TRC_Inst2_ITRM.log)	Conditions	Diagnoses and Solutions
The MSSQLServer service is not running on \\local_host.	The MDB is remote; local and remote hosts are not in the same domain.	This message is misleading because contact is not being established with the remote MDB host. Add the local host to the same domain as the remote host.

A Dependency checker test has failed.	Terminal Services is enabled on the host.	Temporarily disable terminal services while installing CCS. Installing on the console may work, also.
		Or, as the *CCS/NSM Implementation Guide* states: "…this release supports installations through Windows Terminal Services even when configured in Application Server Mode." However, the following settings are required:
		■ CONSOLE mode must be used when performing installation from remote access.
		Example:
		`mstsc /v:HostName /console`
		■ Terminal server USER settings should be changed to INSTALL prior to the installation.
		Example:
		`change user /install`
		To verify the user settings, execute the following command:
		`change user /query`
		For more information about the Windows Terminal Server CHANGE USER utility, see http://support.microsoft.com/kb/186504 http://support.microsoft.com/kb/186504.

Preconditions of the DSM Manager Installation

It may be the case that other CA Technologies products are installed on the DSM manager system, which has already installed an MDB.

Before starting a DSM manager installation, make sure that no other product is using the MDB. If another product is using the MDB, the installation process will likely hang.

On Windows, if you want to install CA ITCM after Unicenter Asset Portfolio Management, check whether the process “corasmm.exe” is running. If this is the case, set the Unicenter Asset Portfolio Management notification server and the Unicenter Asset Portfolio Management cache service to manual and restart the computer before installing CA ITCM. When the CA ITCM installation has completed, you should restart and re-enable the two Unicenter Asset Portfolio Management services. This can be done from the service control manager at the location Control Panel, Administrative Tools, Services.

Disk Space Considerations for Manager and MDB Installation

Install the DSM manager on a partition with at least 12 GB of free disk space. The installation itself uses approximately 7.7 GB of disk space and has some additional space requirements for log files. If the MDB is also being installed on this partition, you should allow at least an additional 50 GB for the database (both SQL Server and Oracle) and associated online check point and journal files. A large SQL Server or Oracle database could require up to 100 GB. These figures are independent of your data storage requirements for storing software packages for distribution. For more information, see the "Hardware Specifications and Requirements" chapter in the *CA IT Client Manager Release Notes* that are part of the CA IT Client Manager documentation set (Bookshelf).

A reboot of the system is normally not required after installation, but it may enhance performance by making more system resources available.

Data replication between domain tier and enterprise tier requires a minimum size of the tempdb database. Therefore, it is important to have sufficient space allocated for the tempdb files and transaction log. We recommend that you set the initial file size for the tempdb on the domain tier to 80 MB and on the enterprise tier to 2 GB. Additionally, make sure that the autogrowth property is set to 'unrestricted growth'.

Standalone Manager in a Mixed Database Environment

If you are going to install a standalone domain manager and intend to subsequently link it to an enterprise manager that uses a different MDB database type, you must manually install the relevant database client on the domain manager. This enables the domain manager to connect to the enterprise manager for replication.

For example, if your domain manager uses Microsoft SQL Server and the enterprise manager uses Oracle, you must install the Oracle database client on the domain manager.

Unattended MDB Installation Using a Response File

The MDB installer supports unattended installation from a response file using the setup.bat -r response_file command on Windows and setup.sh -r response_file on Linux/Solaris.

The MDB installer also supports the creation of a response file using the setup.bat -g response_file command on Windows and setup.sh -g response_file on Linux/Solaris.

Instead of generating a response file, you can edit the response file template, install.rsp, and use this template to perform an unattended install.

Encryption and Decryption of Passwords in a Response File

By default, the MDB installers use the Blowfish encryption and decryption utility that is included in the MDB packages: blfs.exe on Windows and blfs on Linux and Solaris. When you run setup with the -g option, the application automatically uses Blowfish to encrypt passwords in the response file.

If you create the response file by editing the included template, install.rsp, run the Blowfish utility from a command or shell window to encrypt the password. Then copy the resulting string to the response file.

For example, if the blfs validation_0101 command on Linux/Solaris returns the encrypted string, 0x530924b11654032a6e0e213281cd8565c3f9ec63b09dc673, you need to copy this string to the response file as follows:

```
# Password of Oracle MDB admin user
ITRM_MDBADMINPWD=0x530924b11654032a6e0e213281cd8565c3f9ec63b09dc673
```

In both cases, when you run setup with the -r option, the application automatically uses the Blowfish utility to decrypt passwords in the response file.

Note: The unencrypted passwords cannot start with 0x (case-sensitive).

The Blowfish algorithm is not FIPS-compliant. You can provide a custom FIPS-compliant utility for encryption or decryption by setting environment variables pointing to the relevant programs. That is, set MDB_ENC_PROG to the full path name of the encryption program and MDB_DEC_PROG to the full path name of the decryption program.

Example: Changing the Encryption or Decryption Programs on Windows

```
set MDB_ENC_PROG=E:\tmp\my_encrypter.exe

set MDB_DEC_PROG=E:\tmp\my_decrypter.exe
```

On Windows, the programs must have a .exe extension in the file names.

Example: Changing the Encryption or Decryption Programs on Solaris or Linux

```
MDB_ENC_PROG=/tmp/my_encrypter
export MDB_ENC_PROG

MDB_DEC_PROG=/tmp/my_decrypter
export MDB_DEC_PROG
```

If you do not set MDB_DEC_PROG, or if the program does not exist, then MDB_DEC_PROG is assumed to be the same as MDB_ENC_PROG. If you do not set MDB_ENC_PROG or if the program does not exist, then the default Blowfish encryption and decryption programs are used.

Preparing to Work with a Microsoft SQL Server MDB

Before you install a DSM manager based on Microsoft SQL Server, the SQL Server must have been installed with the following configuration:

- Mixed mode authentication (that is, Windows authentication and SQL Server authentication) is required
- TCP/IP network protocol is enabled and operational. For information on how to choose and configure network protocols, see the SQL Server documentation.
- The following rule applies to the server collation selected during SQL Server installation:

  You must choose a collation name where a case insensitive variant is supported.

Use the CA ITCM installation wizard and follow the instructions to configure the SQL Server MDB, as follows:

- On the "Configure Manager" page of the wizard, you must enter the mandatory specifications (connection parameters) for the target database system, such as:
  - Management Database Provider (select Microsoft SQL Server)
  - Management Database Server
  - MDB Password

    Note: Because mixed mode authentication is used, this password must conform to the security level of a system login password.
- On the "Configure Microsoft SQL Server MDB" page you can enter the following configuration settings:
  - Compatibility mode

    Note: The Compatibility mode check box must be selected if you are going to install a new MDB 1.5 as shipped with the product and you have planned to later install another CA Technologies product that only supports MDB 1.0.4. If the Compatibility mode check box is not selected, the installation of any follow-up product that does not support MDB 1.5 will fail.

    Default: Compatibility mode is not selected.
  - MDB database name

    Default: mdb
  - MDB instance name.

    Select the instance name from the drop-down list.

    Default: default
  - Database port number

    Default: 1433

During installation, you must enter the port number associated with the Microsoft SQL Server instance for all nondefault instances. The port can be looked up in the SQL Server TCP/IP configuration using SQL Server Configuration Management.

If Microsoft SQL Server is being configured with named instances, the "TCP Dynamic Ports" option is automatically set with the port number (dynamic port configuration). Then, it may happen that the domain or enterprise manager cannot access the database because the port number on the MDB system has changed in the meantime, for example, due to a system restart. To avoid these access failures, we recommend that you change the port setting manually to a static port ID, as follows:

- From the Windows Start menu, open SQL Server Configuration Manager, SQL Server Network Configuration, Protocols for *instance_name*, TCP/IP.
- Right-click and select Properties from the context menu.
- On the TCP/IP Properties dialog select the IP Addresses tab. In the IPAll area, cut the port value in the TCP Dynamic Ports field and paste it into the TCP Port field.

Important! In case you assign a nondefault port number manually, we recommend that you update the reservedPorts list in the registry. Otherwise, it could appear that CAF is started before SQL Server after a reboot; and then, if CAF requests a dynamic port number, it could be that CAF gets the port number that was set for the SQL Server. As a result, the SQL Server will fail upon startup.

Install the DSM Manager: Microsoft SQL Server MDB

After completing the installation of the Microsoft SQL Server MDB, install the DSM enterprise or domain manager.

Follow these steps:

1. Install the Microsoft SQL Client on the computer where you want to install your DSM enterprise or domain manager.

   Note: This step is not necessary if Microsoft SQL Server is already installed on the computer.

2. Install the CA ITCM DSM manager and enter the details of your Microsoft SQL Server MDB in the relevant dialogs.
3. Start CAF.

Remote MDB Installation for Microsoft SQL Server

If you plan to run the DSM manager using a remote Microsoft SQL Server MDB, the manager and the remote MDB computer must have a trusted relationship when running in a Windows environment.

During the installation of a domain or enterprise manager, you can install the MDB on the local host or use an existing remote instance of the MDB.

For a remote configuration, install the database on the remote computer by selecting Install MDB (no CCS functionality).

If you need to use CCS with CA ITCM, you need to install CCS on the MDB host computer, whether local or remote. Use the Install CCS option from the top-level CA ITCM installation dialog. Then install the domain or enterprise manager.

If you use a remote Microsoft SQL Server, install the Microsoft SQL Client Management Tools *before* you install the domain or enterprise manager. Verify that the Microsoft SQL Client Management Tools are not deselected during Microsoft SQL Client installation.
CA ITCM uses the specific user ca_itrm created on the database level to get authenticated for MDB access. You need to specify the same password for the user ca_itrm during "Install MDB" and CA ITCM installation dialogs. The user ca_itrm is created automatically.
When you install multiple domain managers with remote Microsoft SQL Server MDBs, verify that only one MDB exists on each database server instance. This restriction means you must have as many database servers as MDBs.

Note: With a remote Microsoft SQL Server MDB, the name of the server hosting the domain MDB is used as the name of the domain manager. Therefore, the DSM Explorer in the enterprise manager displays the domain manager with the name of its database server.

Preparing to Work with an Oracle MDB

Use the CA ITCM installation wizard to configure the manager to work with an Oracle MDB, as described following. It is crucial that the parameter values specified during these configuration steps must match the parameter values entered during the Oracle MDB installation:

- On the "Configure Manager" page of the wizard you must enter the mandatory specifications (connection parameters) for the target database system, such as:
  - MDB Provider (select Oracle)
  - MDB Server
  - MDB Password
  - Database administrator (sys)

    (For more information, see Database Administrator User on Oracle (see page 123).)
  - Database administrator password
- Click the Database button in the Advanced Manager Configuration area to open another wizard page to specify advanced configuration settings for a custom MDB installation.

- On the "Configure Oracle MDB" page you can enter advanced configuration settings, such as:
  - Compatibility mode

    Note: The Compatibility mode check box must be selected if you are going to install a new MDB 1.5 as shipped with the product and you have planned to later install another CA Technologies product that only supports MDB 1.0.4. If the Compatibility mode check box is not selected, the installation of any follow-up product that does not support MDB 1.5 will fail.

    Default: Compatibility mode is not selected.
  - MDB database name

    Default: orcl
  - Database port number

    Default: 1521
  - MDB administrator password

Prerequisites

This section lists the prerequisites for installing the MDB on Oracle 11g:

- Install Oracle 11g Server on the computer where you are planning to install or upgrade the MDB. This release supports Windows, Solaris, and Linux servers for Oracle 11g MDB.
- Create an Oracle instance using the Oracle Database Configuration Assistant. Consider the following factors while creating the instance:
  - The database instance name (SID) must be the same as the Oracle service name (global name).
  - Appropriate values must be entered in the SGA Size and PGA Size fields on the Memory tab of the Oracle Database Configuration Assistant.

    A minimum of 2 GB is recommended for SGA.
- Install Oracle 11g Client on the computer where you are planning to install or upgrade the CA ITCM DSM manager.

Note: For detailed installation instructions, see the appropriate Installation Guide available in the Oracle Documentation Library.

Database Administrator User on Oracle

The installation of the manager requires an Oracle Administrator user. If you are going to use the Oracle user “SYS”, the Installer will connect “as sysdba”. However, you may also use a different user; in which case the user has to be created as a user who has the same privileges as SYSDBA. This means that the SYSDBA privileges are granted to this user.

The following operations on Oracle require the user to have SYSDBA privileges in order to perform them:

- Start up a database
- Shut down a database
- Back up a database
- Recover a database
- Create a database

How to Install an Oracle MDB (Standalone)

Important! Make note of the values and passwords you enter in the installation wizard steps because you need them later when configuring the DSM manager.

The basic steps for installing the MDB on Oracle 11g in interactive mode are as follows:

1. Create an Oracle instance using the Oracle Database Configuration Assistant if you have not already done so, and do the following:
   - Verify that the database instance name (SID) is the same as the Oracle service name (global name).
   - Enter appropriate values for the instance in the SGA Size and PGA Size fields on the Memory tab of the Oracle Database Configuration Assistant.
2. Run the appropriate script file on the target database server from the MDB directory:

   Valid on Windows

   ```
   setup.bat
   ```

   Valid on Solaris or Linux

   ```
   sh ./setup.sh
   ```

   The MDB Installer is launched and the first wizard page, Choose Setup Language, appears.
3. Accept English as the setup language.

   Note: The only available language for this release is English.

4. Accept the End User License Agreement.
5. (Windows only) Select the database type, Oracle Server, for this procedure.
6. Enter the path of the Oracle installation for the MDB in the ORACLE_HOME field, to define the working runtime Oracle environment.

   For remote MDB installation, enter the ORACLE_HOME value of your local computer.
7. Specify the Oracle database server name and MDB size.
8. Specify MDB user and database administrator credentials.

   Note: The default MDB user name is ca_itrm.
9. Specify advanced Oracle configuration settings, including Oracle service name, Oracle Transparent Network Substrate (TNS) name, port number, tablespace path, and MDB administrator password.
10. Review your database configuration options and confirm the installation by clicking the Install button.

    Installation begins and the MDB schema gets created in the Oracle database.

    Note: The MDB installer on Solaris displays a dialog that shows the Oracle version and operating environment prerequisite checks. With the new MDB installer, this dialog appears only if there are prerequisite failures; otherwise, the installation proceeds.
11. Install DSM manager when installation of the Oracle MDB is complete.

Note: The DSM manager uses EZCONNECT to connect to the Oracle MDB.

More information:

Remote MDB Installation for Oracle (see page 128)
Install the DSM Manager: Oracle MDB (see page 125)
Unattended MDB Installation Using a Response File (see page 117)

Install the DSM Manager: Oracle MDB

Install the DSM enterprise or domain manager.

Follow these steps:

1. Install the Oracle 11g Client on the computer where you want to install your DSM enterprise or domain manager.
2. Install the CA ITCM DSM manager and enter the details of your Oracle MDB in the relevant dialogs.

   Note: When the manager installation requires the name of the MDB Oracle Server, enter the IP address only if the manager and the MDB are on the same computer. Otherwise, enter the host or DNS name.
3. Follow the wizard instructions to complete the manager installation.
4. Perform the following additional steps if the DSM manager is installed on the same computer as the Windows Oracle MDB:
   a. Run the following SQL command as mdbadmin:

   ```
   update ca_n_tier set
           label='<MDB Server host name>',
           db_host_name='<MDB Server host name>',
           db_server='<MDB Server DNS name>'
   where domain_uuid in (select set_val_uuid from ca_settings where set_id=1)
   ```

   b. Verify that the update is committed. If auto-commit is turned off, manually commit the update.
   c. Run the following command from the command prompt:

   ```
   ccnfcmda -cmd setparametervalue -ps /itrm/database/default -pn dbmsserver -v
   <MDB Server DNS name>
   ```
5. Start CAF.

More information:

How to Install an Oracle MDB (Standalone) (see page 123)

Installation of a Remote Oracle MDB

To install a remote oracle MDB, you must first create an oracle instance using the Oracle Database Configuration Assistant on a remote computer running a Sun Solaris operating system

To install the Oracle MDB

1. Log on to the Solaris host as the "root" user and navigate to *DVD_mount*/SolarisProductFiles_MDB/remotemdb.
2. Run sh ./setup.sh
3. Select the Choose Language Setup option.

   Available languages for the installation wizard are English, French, German, and Japanese.
4. Select New Instance and follow the instructions in the wizard.

   Important! Make note of the values and passwords you enter in the following steps because you will need them later when configuring the DSM manager.
5. You must read and accept the End User License Agreement before the installation wizard will continue.
6. For the ORACLE_HOME environment variable, enter the path of the Oracle installation that you want to use for the MDB.

   The installer checks the hardware platform and ORACLE environment. If any tests fail, then installation will not take place. Only if all testing is successful will the user be able to progress through the installation wizard.
7. Select a "product instance name" for the current installation. Usually this is the same name as the ORACLE instance (SID).

   The Product Name Selection drop-down list displays names that are already used. The product instance name must be unique.
8. Enter the password for the MDB user name (ca_itrm).

   The password is set during installation and confirmation is requested. The password should be remembered.
9. Enter the DB Administrator name (default name "sys") and the DB Administrator password. The DB Administrator is a *username* that has been given the SYSDBA privilege in the Oracle instance.

   Note: For more information, see the *MDB Overview*, which is part of the CA ITCM documentation set (Bookshelf).

10. Specify whether to install the compatibility mode.

    Note: The Compatibility mode check box must be selected if you are going to install a new MDB 1.5 as shipped with the product and you have planned to later install another CA Technologies product that only supports MDB 1.0.4. If the Compatibility mode check box is not selected, the installation of any follow-up product that does not support MDB 1.5 will fail.

    Default: Compatibility mode is not selected.

11. In the MDB Database field, enter the SID of the Oracle database instance you want to use for the MDB.

    The value of this field defaults to the product instance name entered on the previous wizard page.

12. Specify the database port number.

    Default: 1521

    Important! The port number you enter here depends on the port number used when the database was created. If a non-default port number was used at the time of database creation, then the same port number must be entered while installing the MDB. Otherwise, do not change the default database port number.

13. Enter the table space path, that is, the directory where Oracle creates the database files. All directories along this path must already exist, except the last one. For example, in the default path preset in the wizard, the directory "mdb" must not exist.

    Default: /opt/CA/SharedComponents/oracle/mdb

14. In the MDB Administrator Password field you must supply the password of the MDBADMIN user.

    The MDBADMIN database user is used to create the MDB schema and is the owner of the schema.

15. At the Install MDB stage in the wizard process, you must confirm the installation by clicking the Install button.

    Only after this confirmation does the MDB schema get created in the Oracle database.

Important! If you are using a remote Oracle MDB, an Oracle 11*g* Client must be available on the manager and on every system where a DSM engine or the DSM Reporter is running. Make sure that the Oracle 11*g* client of type "Administrator" is installed.

More information:

Oracle MDB Maintenance (see page 202)

Remote MDB Installation for Oracle

Note: Remote MDB installation on Oracle database is only supported from Windows.

For a remote installation, the ORACLE_HOME environment variable refers to the local computer (where you may have only an Oracle Client).

For installation and upgrades to a remote Oracle MDB, define a TNS name for the remote computer in the Oracle tnsnames.ora file on the local computer. This action allows the remote Oracle Server to be addressed.

For a local Oracle MDB install, the MDB installer creates the specified tablespace path folder if it does not exist. This step is not possible for a remote install. Therefore, verify that the tablespace folder path that you are going to select during the MDB installation exists on the remote computer. If the tablespace folder does not exist on the remote computer, an error occurs preventing the installation from proceeding.

More information:

How to Install an Oracle MDB (Standalone) (see page 123)

Note on CCS Support for Oracle

CA Common Services (CCS) does not currently support an Oracle MDB.

Therefore, in CA ITCM, a CCS subset is available with a reduced set of functionality that focuses strictly on the needs of CA ITCM, mainly event (calendar) and IPv6 support.

The Installer will automatically choose the appropriate version of CCS for your environment.

Installation and Configuration Considerations for Oracle MDB

The following section describes the installation and configuration considerations for Oracle MDB.

Installing the Solaris Oracle Server

For detailed installation instructions, see the Installation Guide available in the Oracle Documentation Library.

Deleting and Recreating an Oracle Database Instance

Use the Oracle Database Configuration Assistant tool to delete and create an Oracle database instance. While creating an Oracle database instance using this tool, you are prompted to enter the memory size that Oracle might use for that instance. Enter appropriate values in the SGA size and PGA Size fields on the Memory tab.

For example, enter 1198 in the SGA Size field and 399 in the PGA Size field. These suggested values are about 1.2 GB for the data and control information (SGA) and about 0.4 GB for the program area (PGA). These are the minimum recommended values for an installation with up to 10,000 computer assets.

Verify the Oracle Server Installation

You must have the correct Oracle version and patch level installed; otherwise, the DSM manager operations are likely to fail. To verify the Oracle version and patch level, run the following command:

```
goto $ORACLE_HOME/OPatch
call ./opatch lsinventory
```

Configuring the Oracle MDB for Multi-Byte Language Support

When creating an Oracle database instance using the Database Configuration Assistant tool, select Use Unicode (AL32UTF8) option in the Character Sets tab to support multi-byte language.

Modify the Default Password for User ca_itrm

During manager installation or during MDB installation, you can modify the password for the user ca_itrm that is used for MDB access.

To change the ca_itrm password to the preferred one, you must execute a number of steps, depending on the database provider:

- Microsoft SQL Server MDB
- Oracle MDB

Modify Default Password When Microsoft SQL Server Is Used

If you want to modify the default password for the user ca_itrm to the preferred one when Microsoft SQL Server is used as database provider, proceed as follows:

1. Go to the system where Microsoft SQL Server is running.
2. Open Windows Start, Programs, Microsoft SQL Server Management Studio.
3. Select the user ca_itrm user in the Management Studio and change the password.
4. Go to the system where the manager has been installed.
5. Run cadsmcmd setDBCredentials passwd=*new_password.*
6. Run caf stop.
7. Run caf start.

Modify Default Password When Oracle Is Used

If you want to modify the default password for the user ca_itrm to the preferred one when Oracle is used as database provider, proceed as follows:

1. Go to the system where Oracle is running.
2. Open Windows Start, Programs, and launch the appropriate Oracle Database Control.
3. Select the user ca_itrm in the Oracle Database Control and change the password.
4. Go to the system where the manager has been installed.
5. Run cadsmcmd setDBCredentials passwd=*new_password.*
6. Run caf stop.
7. Run caf start.

MDB Installation Log Files

When installing a Microsoft SQL Server MDB on a computer running Windows, the log files can be found at the following locations:

- %TEMP%\ITRM\database\setup.log
- %TEMP%\ITRM\database\mdb_install\install_*xxxx*.log
- *CA ITCM_installation_directory*\database\setup.log

When installing an Oracle MDB on a computer running Sun Solaris, the log files can be found at the following locations:

- /tmp/CAInstaller.ca-cms-mdb-schema.install.log
- *CA ITCM_installation_directory*/database/setup.log
- *CA ITCM_installation_directory*/database/mdb_install/install_*xxxx*.log

On Solaris, there are also log files at the following locations:

- *CA ITCM_installation_directory*/log/mdbinstall.log
- *CA ITCM_installation_directory*/log/mdbupgrade.log

  If the installation fails early, the log files may remain in /tmp/mdbinstall.log.

MDB Upgrades

This release supports the following MDB upgrades:

- Release 12.5 or later DSM manager with Microsoft SQL Server MDB installed either locally or remotely.
- Release12.5 or later DSM manager with Oracle 11g MDB installed remotely on Solaris, Linux or Windows.
- Patched DSM manager and Oracle MDB installed either locally or remotely on Windows, Linux, and Solaris.

  Note: The Oracle 10g Server must be upgraded to Oracle 11g R2 first. Also, upgrade the Oracle Client on the DSM manager to Oracle before launching the DSM manager setup.

If the database server is remote, the MDB is upgraded during a DSM manager upgrade with the current release. For Microsoft SQL Server, no user interaction is required because the database details are retrieved from comstore. For Oracle, set the ORACLE_HOME environment variable and enter the Oracle service name, TNS name, and the mdbadmin and sys passwords.

If existing database sessions are found during the upgrade, each session is displayed with the names of the database user, process ID, and host computer. The database sessions are displayed in two lists in a dialog. The first list is for sessions that must be closed before the upgrade is allowed to proceed. This list includes sessions belonging to database users who are members of roles created by the DSM schema. Representative roles are ams_group, ca_itrm_group, ca_itrm_group_ro (Oracle only), ca_itrm_group_ams, upmuser_group, and mdbadmin (Oracle only). CCS roles (for Microsoft SQL Server only), like emadmin, emuser, uniadmin, uniuser, wvadmin and wvuser, are also included in the first list. (The roles are read from a configuration file on the DVD image.)

The second list displays any remaining sessions belonging to other database users. We recommend that you close these sessions also, but this step is not mandatory. You can proceed with the upgrade even with these outstanding open sessions.

Use the Refresh button in this dialog to refresh the lists as you close open database sessions. The Continue button is enabled only if the first list of database sessions is empty.

Uninstallation

CA ITCM does not support uninstallation of the MDB schema. You can use the data uninstall script during a DSM manager uninstall to remove selected data from the MDB. You can also use Microsoft SQL Server and Oracle functionality to delete and recreate MDB instances.

Special Notes on CA ITCM Installations

The following is a collection of notes and recommendations for special installation scenarios and is intended for experienced users.

Security Policy Settings

The following security policies should be enabled for the user logon used to install DSM manager or the management database (MDB).

- Access this computer from the network
- Act as part of the operating system
- Allow log on through Terminal Services
- Log on as a service

You can enable these policies through the Windows Control Panel, Administrative Tools, Local Security Policy.

CAM and SSA PMUX Restart

Regardless of whether or not you decide to install extended network connectivity (ENC), the CA ITCM installer will internally invoke CA Message Queuing (CAM) and the Secure Socket Adapter Port Multiplexer (SSA PMUX) installer, and this will restart CAM and SSA PMUX if needed.

Note: The SSA PMUX restart applies to Windows only.

For more information about ENC, see the "Extended Network Connectivity (ENC)" chapter.

Software Inventory Availability

Full software inventory is not available directly after a domain manager installation because the software definitions are imported into the MDB via an engine task, which is scheduled by default to run at midnight.

Installation of DSM Manager with a Remote SQL Server MDB Over IPV6

If you are installing the DSM manager (domain or enterprise) with a remote SQL Server MDB over IPv6, perform the following steps before you begin the installation:

1. Set the value of the following registry key to 1 on the manager machine:

   `HKLM\System\CurrentControlSet\Services\smb\Parameters\IPv6EnableOutboundGlobal (REG_DWORD)`

2. Ensure the following:

   - The host name of the MDB machine resolves to a global IPv6 address.
   - Reverse lookup of the IPv6 address resolves to the same MDB host name

3. Ensure that the MDB machine resolves only to reachable IPv6 addresses on the DSM manager machine that is used to reach the MDB machine.

   This means you have to delete any IPv4 DNS record for the MDB machine on the DNS servers that the manager machine uses, as well as any IPv6 DNS records with addresses that the manager machine cannot use to reach the MDB machine. The DNS cache on the DSM manager has to be flushed as appropriate. Otherwise, JDBC fails to connect to the MDB, which consequently affects the installation of CCS, CIC, and MDB Java components.

Installation of Domain Manager Using Remote SQL Server MDB with Named Instance

For successful installation of the domain manager using a remote SQL Server MDB with a named instance, ensure that the SQL Server Browser is running on the remote MDB system. Before you begin the installation, verify that the domain manager is able to connect to the remote MDB and that the Microsoft SQL Browser is functioning correctly by executing the following command on the domain manager system:

```
sqlcmd -E -d mdb -S MDB server name [\instance name] -q "select * from mdb"
```

Remote Control Stand-alone Agent Installation

The remote control (RC) feature of CA ITCM can be configured in a stand-alone mode. In this mode, the RC agent uses local security and configuration policies, rather than policies sent from a central domain manager.

The CA ITCM installation media (DVD) contains a separate installation wizard named setup_rc to install a stand-alone RC agent.

The stand-alone RC agent installation will only enable the following CAF plug-ins:

- pmux
- rchost
- smserver

Setup_rc can be found under:

- WindowsProductFiles_x86\AgentRC
- LinuxProductFiles_x86/rc_agent

Installation on Solaris Intel

Before you begin the installation of CA ITCM on the Solaris (Intel) platform, be sure to install the following patches for the SUNWlibC package:

- 109148-07
- 108436-16

These patches ensure that standard C++ runtime libraries are present.

You can verify the presence of these patches using the following command:

```
showrev –p | grep SUNWlibC
```

This results in output like the following:

```
Patch: 108436-16 Obsoletes: Requires: 109148-07 Incompatibles: Packages: SUNWlibC
```

Note: Client Automation depends on CAPKI, and CAPKI has a dependency on libucb on Solaris Intel. On Solaris intel 11, if libucb is not installed by default, the installation fails.

Follow these steps to install libucb on Solaris intel 11:

1. Run the following command to identify the package.

   pkg search -r /usr/ucblib/libucb.so.1

2. Run the following command to install the package.

   pkg install <package name>

Path Environment Variable for Solaris Intel

The startup of the shell invokes the startup scripts. Note that sh based shells (like bash) invoke /etc/profile and then ~/.profile. However, Solaris 11 Intel, ~/.profile for user root overrides the PATH environment variable.

When the PATH does not contain CA paths, ensure that you source the startup script in the following manner:

- . /etc/profile.CA all or
- source /etc/csh_login.CA all

Accessing the VMware ESX Web Service

To access the VMware ESX Web Service, you must supply the following logon credentials for a user of a VMware ESX host machine:

Hostname

Specifies the name of the ESX host for which asset management inventory is to be collected. An IP address can also be supplied.

Web Service Username

Specifies the name of a VMware ESX user who has the VMware system role of Administrator or Read-only.

Web Service Password

Requires the password for the specified VMware ESX user.

Web Service URL

Indicates the Web Service URL, which takes the following form:

`https://ESXHostFQDNservername/sdk`

ESXHostFQDNservername represents the fully qualified host name of the ESX server. Alternatively, an IP address can be given instead of the host name.

ESX inventory collection is done using the Web Service (SOAP) engine. By default, the Web Service runs on port 443 as a secure web service that can be accessed using SSL over HTTPS.

Remote Control Component Installation on Linux

The remote control (RC) feature of CA ITCM supports Linux. This operating environment supports the RC host component only.

If the stand-alone RC agent is needed on this operating environment, it must be installed from the LinuxProductFiles_x86/rc_agent directory.

Stand-alone agents may not be deployed using the software delivery functionality or the interactive installer.

Remote Control Component Installation on Apple Mac OS X

The remote control feature of CA ITCM supports Apple Mac OS X. This operating environment supports the Remote Control host component only.

Secure Control mode is not supported. All of the other control modes are supported (Stealth View, View, Shared, Classroom and Exclusive).

As with Linux, the Viewer options to disable Host wallpaper and other user experience features have no effect.

Important! After you have installed, re-installed, repaired, or upgraded a Remote Control agent on a Mac OS X platform, CA recommends that you log out of the system and log back in. This ensures that essential DSM processes are started in the correct user context. If this step is omitted, remote control connection attempts will be rejected with the following message, "The host could not open the desktop of the current user."

Share Access for the Boot Server

The Boot Server is always installed as part of a scalability server and Boot Server configuration details are specified on the scalability server configuration pages of the installation wizard.

If you need share access instead of TFTP (which is the default), click the Boot Server button located in the Advanced Server Configuration area of the Configure Scalability Server page and select the "Enable use of Windows network shares" option. The installer will create read-only network shares accessible through the SMB protocol.

For more details on how to switch from TFTP to share access and how to deactivate the PXE server, see the *OS Installation Management Administration Guide*, which is available as part of the CA IT Client Manager documentation set (Bookshelf).

Domain Controller Connection When Installing CCS

If the connection to the domain controller is lost when installing CCS as a domain administrator, the CCS installation will fail when it tries to validate the installing user's rights, sometimes with a return code of 1073741819.

To resolve this, re-establish the connection to the domain controller or run the installation as a local administrator.

Agent and Scalability Servers Move Operations

An agent is configured to connect to only one domain manager at any given time. However, the agent can be reconfigured. The move of an agent can be triggered by the following command:

```
caf setserveraddress new_scalability_server
```

The move of a scalability server can be triggered by the following command:

```
cserver config -h new_domain_manager
cserver register
```

Whenever a calendar is updated on a CA Common Services (CCS) server (located on a DSM manager), the CCS agents (located on DSM scalability servers) need to be updated. Therefore, run the scalability server procedure “Synchronize CCS Calendar” on every downstream scalability server that has a CCS agent installed.

If you move a scalability server from one manager to another, using the command cserver config -h new_manager, the CCS agent (located on that scalability server) is automatically reconfigured to connect to the new manager.

Note: To ensure that CCS values are not changed when re-registering the server, use the cserver command with the "-i" option instead of "-h".

If, however, the server is moved using policy, then this must be done manually; otherwise, the agent will continue to connect to the old CCS server. To change to the CCS server on the new_manager, use the following commands on the scalability server computer:

```
cautenv setlocal CA_CALENDAR_NODE new_manager_address
cautenv setlocal CA_OPR_PROXY new_manager_address
unicntrl stop all
unicntrl start all
```

DSM Manager with CCS WorldView Manager or CCS Including MDB Installation on a Domain Controller

In this installation scenario, DSM manager with CA Common Services (CCS) WorldView manager or 'CCS including MDB' on a domain controller, the following CCS restriction applies:

The CCS WorldView manager cannot be installed on a server designated as a domain controller.

This is due to IPSEC security overwriting the user privileges for the Microsoft COM server when starting the CA Severity Propagation COM object.

This restriction does not allow CA IT Client Manager to install the CCS WorldView manager on a domain controller. Concerned are the DSM manager and the 'CCS including MDB' installations. For a correct installation of the DSM manager, you have the following options on a domain controller:

- Disable CCS (then, no CCS functionality will be available).
- Install MDB and CCS remotely (then, the CCS WorldView manager will be installed on the MDB side).

Installation of Scalability Server on Linux

When a scalability server is installed on Linux using DMDeploy or software delivery with the CA DSM Scalability Server Linux (Intel) ENU package, the CA Common Services software is *not* installed. If CCS is required with a scalability server on Linux, then it must be installed interactively from the DVD.

Installation and Registration of UNIX and Mac OS X Components

These components are not auto-registered in the Software Delivery and Infrastructure Deployment libraries when installing a domain manager.

To make these packages available on a domain manager, import them from the appropriate CD into the Software Package Library and the infrastructure deployment payload area of the manager using the dsmPush tool (the dsmPush.dms file in the DVD's root directory).

Launch the following command:

`dmscript dsmPush.dms copy -I` *`location_of_CD_image`*

To register these packages in the Software Package Library, you can also copy and paste them from the appropriate CD to the Software Library folder in the DSM Explorer.

UNIX Agent Considerations

The UNIX operating environments currently supported by the UNIX agent in CA ITCM are listed in the compatibility matrix available on CA ITCM bookshelf or CA Support. The platforms listed there are also the platforms on which the Packager for Linux and UNIX can run.

Installation Prerequisites for the Agent on Sun Solaris

Before you install the UNIX agent on a Sun Solaris computer, you must ensure that the required minimum kernel configuration parameters are set.

To set or modify the kernel configuration parameters for Solaris 5.10

For Solaris 5.10, the resource control configuration parameter max-shm-memory must be set to 5242880

or higher and the max-sem-ids parameter must be set to 256 or higher.

1. Query the current values of these parameters using the prctl command, for example:

   ```
   prctl –P –n project.max-shm-memory –i project user.root
   ```

   ```
   prctl –P –n project.max-sem-ids –i project user.root
   ```

2. If the resource control configuration parameters need to be updated, use *one* of the following commands:

   - Use prctl to modify resource control configuration parameters, for example:

     ```
     prctl -n project.max-shm-memory -v 5242880 -r -i project user.root
     ```

     ```
     prctl -n project.max-sem-ids -v 256 -r -i project user.root
     ```

     Note: Configuration parameters modified using the prctl command are *not* persistent and you need to run the commands again after the system is restarted.

   - Use projmod to modify resource control configuration parameters, for example:

     ```
     projmod -s -K "project.max-shm-memory=(priv,5242880,deny)" user.root
     ```

     ```
     projmod -s -K "project.max-sem-ids=(priv,256,deny)" user.root
     ```

     Note: Configuration parameters modified using the projmod command are persistent after the system is restarted.

Installation Prerequisites for the Agent on IBM AIX

The latest Runtime Environment libraries from IBM are installed when you install the CA ITCM UNIX agent on an IBM AIX computer running AIX version 5.3 and later.

Software Delivery Download and UNIX Agents

The following consideration applies when the software delivery download method is set to the Internal NOS method.

The Sun Solaris kernel currently does not support mounting Samba shares.

If the scalability server has only NFS mount points configured (that is, it does not use Samba), the Sun Solaris agents will automatically use NFS.

If the scalability server has Samba shares configured, and the NOSLessSwitchAllowed parameter is 1 (True), the Sun Solaris agents will fall back to use the Internal NOSless download method.

If the scalability server has Samba shares configured, and the NOSLessSwitchAllowed parameter is 0 (False), the download will fail, even if the scalability server also has NFS mount points configured.

The current value of the NOSLessSwitchAllowed parameter can be verified by running the command:

```
ccnfcmda -cmd GetParameterValue -ps itrm/usd/agent -pn NOSLessSwitchAllowed
```

The value of the NOSLessSwitchAllowed parameter can be set to 1 by running the command:

```
ccnfcmda -cmd SetParameterValue -ps itrm/usd/agent -pn NOSLessSwitchAllowed -v 1
```

Note: For more detailed information about the ccnfcmda configuration agent command, type <command> /? at the command prompt.

Data Transport Service Installation Note

On Windows, the Data Transport Service (DTS) functionality is not contained in the software delivery (SD) agent plug-in, but in a separate installation package. That means, if you need the DTS functionality, for example, to use the DTS download method for a specific agent, you must deploy the separate DTS installation package to that agent.

On Linux or UNIX, the Data Transport Service functionality is included in the software delivery (SD) plug-in, that is, DTS is installed with the SD agent installation package.

Renaming of Manager and Scalability Server Computers

CA IT Client Manager (CA ITCM) supports renaming of enterprise managers and domain managers through the DSM Explorer using the particular Domain or Enterprise properties dialog. The Name, Contact information, and Description fields can be edited and their values are replicated between domain and enterprise manager.

CA ITCM does not support renaming of scalability server computers.

System Names as Fully Qualified Domain Names

Whenever the CA ITCM Installer asks for a system name to be entered, we strongly recommend that you enter a fully qualified domain name (FQDN) including domain suffix, so that computer systems in other network domains can be reached even if request forward is not configured for all DNS involved.

Installation of CA ITCM When Unicenter NSM r11 Is Preinstalled

If Unicenter NSM r11 is installed before CA IT Client Manager, the following CCS components must be installed by Unicenter NSM before you start the installation of CA IT Client Manager:

Unicenter NSM Components:

- Management Database
  - MDB for Microsoft SQL Server
- WorldView
  - Administrative Client
  - WorldView Manager
- Enterprise Management
  - Administrative Client
  - Event Management
    - Event Agent
    - Event Manager
- Continuous Discovery
  - Continuous Discovery Agent
  - Continuous Discovery Manager

Launch the Unicenter NSM installation, check if all listed components are installed, and install the missing ones.

After the Unicenter NSM installation has finished, you may start the installation of CA IT Client Manager.

Specifying the Port Number for Web Console During Installation

The modification of the SQLServer.PortNo key with the database port number in the wacconfig.properties file is no longer valid with the multi-manager support in the Web Console. The correct port number must be provided during the installation and cannot be modified later.

Note on Adding the Web Console Using the Modify Installation Method

When you are going to add the Web Console using the Modify installation method, you must ensure that you have at least 8 GB of free disk space available!

Disable Virus Protection During Installation and Uninstallation

We recommend that you disable virus protection software before starting any installation or uninstallation of CA IT Client Manager. Interferences can appear during the installation or uninstallation process if virus protection software is enabled.

Disable Remote Sector Server Service During Installation

If you have a Remote Sector Server (RSS) from a prior Unicenter Asset Management release installed on the computer you are going to install CA ITCM on, the RSS service must be stopped before you start the CA ITCM installation. The RSS service must be disabled, as it will try to restart automatically.

Disable the Asset Management Sector Server service from the service control manager. After installation, enable the service again.

Windows XP Network Access - Sharing and Security Model for Local Accounts

If this Windows XP policy is set to "Guest only", anyone trying to authenticate as a local user gets mapped to the Guest account, which is disabled by default. This will cause authentication to fail.

To fix this problem, please refer to the Microsoft documentation at:

www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/506.mspx

Windows Server 2003 Considerations

For Windows NT and Windows 2000 servers, anonymous access, also called NULL sessions, could by default be used to access network resources. File system shares, called NULL session shares, could be configured to accept NULL sessions. This has always been the preferred way for software delivery (SD) agents, running in the LocalSystem account, to access the Software Package Library (SDLIBRARY$ share) on the scalability server.

With the Windows Server 2003, Microsoft raises the security level compared to previous versions of the server operating system. By default, anonymous access and NULL session shares are disabled. The need for anonymous access has been eliminated for computers that belong to the domain by making machine domain accounts true security principals in the Windows security system. In Windows 2000 domains, and later in Windows Server 2003 domains, access rights may be granted to machine accounts as well as user accounts.

On Windows Server 2003, NULL session shares are not used to provide these agents access to the Software Package Library. Instead, SD relies that agents are granted access to the library through their machine domain accounts. This approach, even though more secure and in line with Microsoft's recommendations, does not offer a complete solution for all supported SD agent operating environments.

Please read the article 278259 in Microsoft's Support Knowledge Base about the evolution of anonymous access on Windows operating environments.

MSI Administrative Installs with SDMSILIB on Windows Server 2003

When using MSI administrative installations to deploy packages over the SDMSILIB share, the "sd_sscmd libraryaccess" method is not sufficient for connecting to that share. Agents must be able to access this share even when installations or configurations using software delivery (SD) functionality are not running. Reason is that access requests to the SDMSILIB share may be requested by MSI installations at any time, for example, when performing repair or self healing. Instead, SD relies that agents are granted access to the SDMSILIB share through their machine domain accounts.

Windows 2003 SP1 MSI Library Access - Restrict Anonymous Access to Named Pipes and Shares

By default, anonymous access to network shares on Windows 2003 Service Pack 1 is denied.

For network installations of MSI packages from the SDMSILIB share or general anonymous access to the SDLIBRARY$ share on a computer running Windows 2003 Service Pack 1, the following steps must be performed:

- Set the following security option in the Local Security Policy:
  'Network Access: Restrict anonymous access to Named Pipes and Shares – Disabled'
- Reboot the system in order for the changes to take effect.

SD Agents Connecting SD Scalability Servers

The following applies only when software delivery (SD) agents connect to SD scalability servers running on Windows Server 2003 and where the Local Security Policy "Network Access: Restrict anonymous access to Named Pipes and Shares" is set to Enabled on the manager or scalability server.

SD agents running on computers with Windows XP, or Windows Server 2003, not belonging to any domain, or belonging to a different non-trusted domain than the SD manager on which the Software Package Library share exists, will be refused access as well.

To resolve the access issues for SD agents on Windows XP, or Windows Server 2003, a dedicated user account can be created manually on the scalability server machine and added to the Everyone group. This will grant read-only access to the SDLIBRARY$ shares. The user name and password have to be entered into the common configuration store of each of the domain manager and scalability server running on the new Windows manager platform.

In order to prevent failures, SD agents automatically fall back to internal NOS-less download, if access to the library is denied. This behavior can optionally be switched off by setting NOSLessSwitchAllowed to False in the configuration policy section itrm/usd/agent.

Windows Server 2008 Core Operating Environments

This section describes known issues, workarounds, and solutions that apply to Windows Server 2008 server core operating environments.

Dependency on Graphical User Interface (GUI)

Windows Server 2008 server core provides limited GUI functionality. Due to the dependency on the GUI, the following CA ITCM agent options are not supported:

- Remote Control chat
- Remote Control viewer
- Software catalog
- Systray

Dependency on IE

Windows Server 2008 server core does not support HTML-based installers due to the dependency on IE.

To install the CA ITCM agents, do *one* of the following:

- From the installation media, go to WindowsProductFiles directory and run setup.exe.
- From the DSM Explorer, use DMDeploy to deploy the agent plugins.

Uninstall the Agents

Windows Server 2008 server core does not provide support for Add or Remove Programs. To uninstall the agents, run msiexec from the command line.

For more information about using msiexec, see the Installation Tool msiexec (see page 161) section.

Options Not Supported

Windows Server 2008 server core does not support the following:

- Online help for agents.
- "Force user to log off before job executes" mode of operation for the Logon Shield
- The Logoff option of the Procedure options "Boot Level before execution" and "Boot Level after execution"

Notes on Firewall and Ports

Some operating systems, such as Windows XP and Red Hat, include a firewall feature which may prevent remote connections from being established. These remote connections include the connections from other DSM components, such as scalability servers. In order to allow CA IT Client Manager to work properly, the firewall may have to be reconfigured.

An overview of the ports currently used by CA IT Client Manager and its individual components is provided in the "Ports Used by CA IT Client Manager" (see page 505) appendix.

Compatibility Libraries for Linux

The DSM installer assumes that certain dependent libraries are present. If these libraries are not present, installed components may not work properly.

The following table details the software library prerequisites. These libraries must be present on Linux hosts prior to installing any DSM components.

Linux Distribution/Version	Required RPM Packages
Red Hat 5 Enterprise Linux	glibc 2.3.3-84 compat-libstdc++ 33-3.2.3-61 For 64-bit versions of the OS: ncurses 5.4-1.3 (i386) or ncurses-devel 5.4-13 (i386) zlib 1.1.4-8.1 (i386) or zlib-devel 1.2.1.2-1.2 (i386)
SuSE Linux Enterprise Server 10	glibc 2.3.3-84 compat 2004.4.2-3 libstdc++ 3.2.2-38

Note: To see the latest information about required compatibility libraries and additional system packages, visit the support web site of your Linux supplier.

MSI Prerequisites for the Installer

In all Windows operating environments, the Installer of CA ITCM requires the Microsoft Windows Installer (MSI) engine 2.0. If this version is not available, the installation wizard installs it automatically prior to any installation step. The upgrade to MSI 2.0 does require a system reboot.

On Windows 2003 systems, reboots are very unlikely to happen, as MSI 2.0 should have been installed as part of the operating system.

Component	Windows Platform for Installation	Expected MSI Version	Action Performed by the Installer, if Expected MSI Version Is Not on the Target Computer
GUI	All	2.0	Install/Upgrade to Version 2.0
Manager	All	2.0	Install/Upgrade to Version 2.0
Server	All	2.0	Install/Upgrade to Version 2.0
Agent	2003	2.0	Install/Upgrade to Version 2.0

Note: If agents are installed using software delivery or infrastructure deployment functionality, you must ensure that the Microsoft Windows Installer is already installed on the target computers. If necessary, you can download the Microsoft Windows Installer from the Microsoft website (www.microsoft.com).

Sharing the MDB between CA Service Desk Manager and CA ITCM

If you are planning to share the same MDB between CA Service Desk Manager and CA ITCM, you must first install CA Service Desk Manager and then install CA ITCM.

Administrative Installation on Windows

This is a manual installation option that applies to Windows operating environments only. An administrative installation provides the Microsoft Windows Installer function to uncompress the content of the installation image and copy the decompressed image to a network share.

Installation Directories on Windows

The structure of the installation directories in Windows environments and the rules and restrictions that apply to them are described as follows:

Default base path

`C:\Program Files\CA\DSM`

You can change this default base path when prompted.

Shared components path

Shared components are installed in different directories. By default, the Windows Installer creates directories for each of the shared components under the base path:

`C:\Program Files\CA\SC`

You can change this default base path when prompted.

PATH environment variable

During installation, the PATH environment variable is extended with

basepath`\bin`

However, in the following case, the PATH environment variable may not be automatically updated during installation:

When you are installing through a Terminal Server session, the PATH variable change becomes effective only after one of the following actions has been completed:

- Log off and log in again into the system
- Reboot the system

This behavior is caused by the Microsoft operating system, and therefore cannot be changed.

As a result of this, on some Windows systems the application framework (CAF) command line interface cannot be used until changes to the PATH variable are sensed.

The maximum length of the PATH variable is determined by the Windows operating environment used. During installation the actual length of the PATH variable is checked. If the length does not allow you to add additional directory names, the installation process is stopped.

Installation Directories on Linux and UNIX

The structure of the installation directories of CA ITCM in Linux and UNIX environments, and the rules and restrictions that apply to them, are described as follows:

Default base path

The default CA ITCM installation directory is:
`/opt/CA/DSM`

The CA ITCM installation directory is also referenced by the environment variable $CA_ITRM_BASEDIR.

You can change this default base path when prompted.

Shared components path

Shared components are installed in different directories. The Installer creates directories for each of the shared components by default under the base path:
`/opt/CA/SharedComponents`

The common components location is also referenced by the environment variable $CASHCOMP, which is set up by the Installer.

Note: $CASHCOMP is shared by all CA products on a computer. If this value has been set (by installing another CA product previously), it will not be possible to change it in the CA ITCM installation. The installer will honor the existing settings.

PATH environment variable

You can specify whether you want the system-wide PATH environment variable to be updated or not at the end of the installation. If you do not, you can still set up the path manually after installation, along with other environment variables required for correct operation of CA ITCM. To do this in a Bourne/Korn/bash shell, run the command:

```
# . $CA_ITRM_BASEDIR/scripts/dsmenv
```

To set up the environment in the C shell, run the command:

```
# source $CA_ITRM_BASEDIR/scripts/dsmenvcsh
```

Install Alert Collector

You can set the role in which Alert Collector must run at the time of deployment. Configure Alert Collector in one of the following roles:

Persist Alerts into MDB

Configures the alert collector to persist alerts into MDB.

Persist Alerts into MDB and Take Configured Actions

Configures the collector to persist the alerts into MDB and take configured actions such as sending mails, raising SNMP trap, writing to Windows/CCS event log.

Persist Alerts, Take Configured Actions, and Forward

Configures the collector to persist the alerts into MDB, take configured actions, and forward alerts to another alert collector.

Forward

Configures the collector to forward the alerts to another alert collector.

Install the alert collector on EM, DM or a standalone machine connecting to the manager MDB on DM/EM. Also, you may install on a standalone machine in *Forward Alerts* role.

The following section explains the roles you can select based on the configurations:

On Enterprise Manager or Standalone Server Connecting to EM

Select *Persist Alerts into MDB*. For EM, the other roles are not supported.

On Domain Manager or Standalone server connecting to DM

Select *Persist alerts into MDB and take configured actions* or *Persist alerts into MDB, take configured actions and forward alerts*. Select the latter role when the DM is linked to an EM to forward alerts to the EM. Select other roles when you have to persist into the MDB or forward to alert collector on EM.

Stand-alone Server – not connecting to either DM or EM

Select *Forward* to send alerts to another alert collector. For example, in an ENC environment, install the alert collector on the ENC server which resides in the DMZ so that the alerts are forwarded to the alert collector on the DM.

By default, you can install the alert collector directly on the DM, the EM (if one exists) or on separate server machines connected to the MDBs on the managers. To handle the increasing load, perform the following steps:

- Introduce additional alert collector servers, each forwarding to the alert collector on the DM.
- Increase the number of worker processes for the DSM_WebService_HM application pool on IIS.

Restrictions for Computer, User, and Directory Names

Computer, user, and directory names must be valid for the operating system that CA ITCM is being installed on and also adhere to the restrictions specified in the following sections:

- Computer Name Restrictions (see page 152)
- User Name Restrictions (see page 153)
- Directory Name Restrictions (see page 153)

Computer Name Restrictions

Computer names must contain the following ASCII characters only:

- alphanumeric
- hyphen -

Computer names must not start with a hyphen.

Important! To support localized hostnames, that means, hostnames in non-US English (non-ENU) language locales, it is required that the underlying Domain Name System (DNS) infrastructure supports UTF-8 character encoding in DNS.

User Name Restrictions

User names must contain the following ASCII characters only:

- alphanumeric
- at @
- pound #
- dollar $
- underscore _

User names must not start with @, #, $, or a digit.

Directory Name Restrictions

A directory name must start with either:

- an ASCII letter, that is, a-z and A-Z
- a digit 0-9
- an underscore _

It can continue with:

- ASCII letters
- digits
- hyphen -
- underscore _
- period .
- tilde ~

Generally, CA Technologies recommends that path names not be distinguished by case.

Windows specific notes:

- Absolute directory names must start with a drive specification (a drive letter immediately followed by a colon), followed by a backward slash \, and then followed by a relative directory path. No UNC paths are allowed.
- Round brackets (and) can be used after the first character of a directory name, but when installing a manager, round brackets (and), and hyphen - are not allowed within the directory name.
- Spaces are allowed after the first character of a directory name.
- Uppercase letters are not distinct from lowercase letters (for example, A is the same as a).
- On Windows, it is not possible to install a manager with a local or remote MDB by using a UNC path name for the image location. If the image location is on a remote system, it must be made accessible as a Windows share. Also, the path name must not contain a @.

Linux and UNIX specific notes:

- Absolute directory paths must start with a forward slash / and continue with a relative directory path. A relative directory path contains a number of directory names separated by forward slashes.
- Uppercase letters are distinct from lowercase letters (for example, A is not the same as a).
- White space (for example, space and tab characters) is not permitted in installation directory paths.

Interactive Installation Using the Installation Wizard

The CA ITCM installation wizard manages the entire installation of all software components and some prerequisites. If any prerequisites are missing, the Installer will post error messages.

Disk Space Check Before Installation

The setup program will estimate the amount of disk space required to install the components you select. Installation only continues if there is enough disk space available.

However, substantial amounts of additional disk space are normally required for data storage.

Interactive Installation of Individual Components

To install one or more individual components on an existing CA ITCM installation

1. Run the installation wizard and select the Install CA ITCM option.

   If an existing installation is detected, the Select Install Option dialog displays.

   Select the Modify install option and follow the instructions in the installation wizard.

2. In the Select Components and Features dialog, which shows all available features, select the features you want to install.

   Note: The features that are already installed are selected. When you unselect an existing feature, this feature will be removed.

3. Follow the instructions in the subsequent dialogs of the installation wizard and enter the required information for installation and configuration.

Installation Summary

During installation the Installer collects information on all steps performed after the setup program was called. An installation summary provides a list of the components the user has selected for installation. This summary is presented to the user before installation commences.

On Windows, after installation has completed, the installation summary is also available as a text file called DSMSummary.txt. The installation summary text file is stored under the directory specified by the %temp% environment variable.

On Linux and UNIX, the installation summary is stored in the main installation log file, which by default is

/opt/CA/installer/log/ca-dsm.install.log

Installation Rollback

If the installation of one of the components called by the setup program fails, or cannot be completed, a rollback is performed for this package and any other package that have been installed as part of the installation session to restore the system to a consistent state.

Copy of Installation Packages

The setup program optimizes disk space usage by copying only those packages from the installation media (DVD) to the local system or the Software Package Library that are actually needed for the functionality selected. Consider the following two cases:

- If infrastructure deployment functionality has been selected for installation, the installation packages for agents and servers are copied from the installation media to the local system.
- If software delivery manager functionality is being installed, all installation packages, including DSM Explorer and manager are copied into the AUTOREG folder of the Software Package Library.

In those cases, only packages that are needed for the selected functionality are copied to the local system and Software Package Library. If all functionality has been selected, all packages are copied. If only software delivery functionality has been selected, only packages needed for software delivery are copied.

CCS Considerations

The DSM manager setup automatically chooses the appropriate variant of CA Common Services (CCS), either Micro-CCS or full CCS. The application installs Micro-CCS with the DSM manager if its MDB resides on Oracle. Full CCS is installed with a Microsoft SQL Server MDB.

When you upgrade the DSM manager, the DSM manager setup attempts to upgrade either full CCS or Micro-CCS appropriately.

The Install CCS option is still available from the top level of the CA ITCM installation wizard. It installs full CCS on the local computer. This option requires Microsoft SQL Server on the latter with the MDB preinstalled.

In this release, however, the Install CCS including MDB option has been removed from the top level of the CA ITCM installation wizard.

Interactive Installation of CA IT Client Manager on Windows

We recommend that you first run the Check Prerequisites option to make sure that relevant prerequisite software is present before you start the installation. See CCS Considerations here.

To install CA ITCM interactively you must perform the following steps:

- Log on to the system as administrator.
- Mount the installation DVD or execute the setup command to open the installation wizard.
- Follow the instructions in the installation wizard and enter the required information for installation and configuration. The installation wizard provides you with helpful explanations and hints on the installation screens.
- The first dialog of the installation wizard lets you select the language that is used during installation.

The installation wizard provides the following options on its welcome screen:

Install CA ITCM

Lets you choose the product functionalities to install, provided you have accepted the license agreement.

Install MDB

Lets you install the management database (MDB) on a dedicated host without any of the CA Common Services (CCS) components. This MDB will be accessed remotely by all components which require it. This installation option prevents the manager from using CCS functionality.

Install CCS

Launches an interactive CCS installation.

Install CCS including MDB

Launches the CCS installation including the management database (MDB). You must select this option, if you want to use the DSM manager together with CCS functionality.

Check Prerequisites

Checks the host environment to determine if the product installation can successfully occur. The application will inform you, if any external prerequisites are missing. You must install the required software before the CA ITCM installation can proceed.

View Documents

Provides a list of documentation files available in the PDF format that you can read with the free Acrobat Reader.

Contact Us

Provides the official postal, web, and email addresses of CA Technologies, as well as the company's phone and fax numbers.

Interactive Installation on Linux and UNIX

The process for interactively installing CA IT Client Manager on Linux or UNIX is as follows:

1. Log on to the Linux or UNIX computer as user root.
2. Mount the installation DVD, then change to the root of the DVD and run the script:
   ```
   # sh ./setup.sh
   ```
   The installation wizard launches. Make sure that you have the details of the directories where to install the components.
3. Follow the instructions in the installation wizard and enter the required information for installation and configuration.

The first dialog lets you select the language that is used during installation.

The subsequent welcome dialog provides the following options:

Install DSM

Lets you choose the product functionalities to install, provided you have accepted the license agreement.

View Documents

Provides a list of documentation files available in the PDF format that you can read with the free Acrobat Reader.

Contact Us

Provides the official postal, web, and email addresses of CA Technologies, as well as the company's phone and fax numbers.

When you select the Install DSM option, the installation wizard first navigates you to the End User License Agreement (EULA) dialog. After you accept the license agreement, you can select any combination of the following functionalities to install:

- Asset Management
- Remote Control
- Software Delivery

You may install any or all features and functions even if you have not yet purchased a license for the product, and run the functionality for a trial period.

The subsequent dialog of the installation wizard asks you to choose the installation method.

Note: By default, the installation wizard on Linux and UNIX is a Java graphical user interface (GUI). If it is not possible to display a graphical user interface, for example, when you are installing from a character based console, the installation wizard has a VT100-style (character based) user interface.

Installation of CA ITCM Using the Command Line in Windows

The following sections provide information about tools, installation packages, and installation options that can be used to perform and control the CA ITCM installation on Windows using the command line.

Installation Packages for Windows

CA IT Client Manager is structured as a set of MSI packages to ensure effective network distribution and installation and to reduce network traffic for agent deployment.

The Master Setup contains all Installer dialogs, gathers information needed to call the other packages in silent mode, and manages rollback where needed. All other packages install the files and resources needed for the specific component.

Third-party products that are internal prerequisites for DSM components are automatically installed from separate MSI packages.

The MSI installation packages are stored on the installation media at the following location (where *component* stands for Manager, Explorer, and so on):

`...\WindowsProductFiles_x86\`*component*

Installation Packages for Windows

The following table provides an overview of the installation packages available for CA IT Client Manager, their file names, and their names displayed by the Windows Add or Remove Programs applet in the Windows Control Panel.

The installation packages can be found in the WindowsProductFiles_x86 folder of the CA IT Client Manager installation DVD.

Package	File Name	Name in the Windows Add or Remove Programs List
Master Setup	setup.exe	CA IT Client Manager

Package	File Name	Name in the Windows Add or Remove Programs List
Explorer	Explorer.msi	CA DSM Explorer
Manager	Manager.msi	CA DSM Manager
Server	Server.msi	CA DSM Scalability Server
Base Agent	AgtBHW.msi	CA DSM Agent + Basic Inventory plugin
AM Agent	AgtAM.msi	CA DSM Agent + Asset Management plugin
DTS Agent	AgtDTS.msi	CA DSM Agent + Data Transport plugin
RC Agent	AgtRC.msi	CA DSM Agent + Remote Control plugin
SD Agent	AgtSD.msi	CA DSM Agent + Software Delivery plugin
Documentation	Documentation.msi	CA DSM Documentation
DMPrimer	dmsetup.exe	CA DSM DMPrimer
ENC Server	ServerENC.msi	CA ENC Server
RVI	RVI.msi	CA DSM Remote Virtualization Inventory

Third-Party Installation Packages

The following table provides an overview of third-party installation packages required by individual DSM components, their file names, and a description of their purpose. For information about third-party product versions and releases, see TPLAs available on CA ITCM bookshelf.

Package	File Name	Description
AMS 12.8	setupwin32.exe	CA Technologies component for Asset Maintenance System. Required for Web Services.
CCS r11.2	setup.exe	CA Technologies component for CA Common Services. Required for manager installations.
MDAC	mdac_typ.exe	Microsoft Data Access package. Required for manager database access.
Apache Tomcat 7.0.40		Apache Tomcat installation. Required for Web Console.
CA SSA 3.2.0	CA Secure Socket Adapter_NoEtpki.msi	CA Secure Socket Adapter.
CAPKI 4.3.0	Setup.exe	CA PKI libraries

Installation of CA IT Client Manager Using setup.exe

To install or configure CA IT Client Manager from the command line, you must start the installation by running setup.exe from the WindowsProductFiles_x86 directory of the installation media (DVD).

The following options can be set when executing the setup.exe program:

/a

Starts an administrative installation, which will decompress all DSM components and files to a network share.

Note: This parameter works with setup only under the product files directory, not with setup at the root directory of the installation media.

/V"/l*v x:\DSMSetupxxx.log"

Specifies the log file path. Log file names are static; they cannot be changed.

Installation Tool msiexec

The MSI installation packages support a command line interface. This can be used when deploying DSM functionality to remote systems through alternative methods, such as custom built DVD or CD, or when building CA ITCM functionality into host deployment images.

The Microsoft Windows Installer (MSI) installs software from package files which have the file extension of .msi.

Msiexec.exe is the executable command which can be used to install MSI packages from the command line. Msiexec is a very flexible tool with many command line options. You can find the detailed descriptions of the msiexec options and parameters in the Microsoft Online Help.

All MSI packages support general options. As well, some MSI packages support package specific options. These two sets of options can be used to control the exact manner in which a specific application is installed.

An example of an msiexec command using general options (/i, -l*v, /qn) and the Manager package specific installation option ADDLOCAL is the following:

```
msiexec /i "x:\WindowsProductFiles_x86\Manager\Manager.msi" -l*v
"c:\DSMSetupMgr.log" ADDLOCAL=Manager,MgrDC,MgrAM ALLUSERS=1 /qn
```

The general options and package specific options are described under "General Options for msiexec" (see page 162) and "Package specific MSI Properties" (see page 164).

Note: Agent package specific options are those installation parameters used during interactive deployment to specify the "additional Windows install options" on the Agent Configuration page of the Deployment wizard. On that page, you can enter multiple install options, separated by spaces, in order to override existing options.

Important! If you are installing DSM components directly using the MSI command line msiexec, you should always set the MSI installation property ALLUSERS to the value 1 (meaning: “Installs for all users but the user requires administrative access privileges on the computer”) to allow later upgrade, uninstall, or re-install through Software Delivery or Deployment functionality out of a DSM manager. If you do not set the parameter like this or leave it empty, the component is registered for the particular user installing it at the first time and cannot be maintained by using manager functions.

Note on specifying system names:

Whenever the CA ITCM Installer asks for a system name to be entered, we strongly recommend that you enter a fully qualified domain name (FQDN) including domain suffix, so that computer systems in other network domains can be reached even if request forward is not configured for all DNS involved.

General Options for msiexec

All MSI packages support the following general options:

/i ***msi install package***

Installs or configures CA ITCM.

/q n|b|r|f|+|–

Sets the user interface level.

Option (Combination)	User Interface Level
q	No user interface.
qn	No user interface.
qb	Basic user interface. Use qb! to hide the Cancel button.
qr	Reduced user interface with no modal dialog box displayed at the end of the installation.

Option (Combination)	User Interface Level
qf	Full user interface and any authored FatalError, UserExit, or Exit modal dialog boxes at the end.
qn+	No user interface except for a modal dialog box displayed at the end.
qb+	Basic user interface with a modal dialog box displayed at the end. The modal box is not displayed if the user cancels the installation. Use qb+! or qb!+ to hide the Cancel button.
qb–	Basic user interface with no modal dialog boxes. Note that /qb+– is not a supported user interface level. Use qb–! or qb!– to hide the Cancel button.

Note: The ! option is available with Microsoft Windows Installer 2.0 and works only with basic user interface. It is not valid with full user interface.

/l [i|w|e|a|r|u|c|m|o|p|v|x|+|!|*] *Logfile*

Writes logging information into a log file at the specified path. Flags indicate which information to log. If no flags are specified, the default is iwearmo.

Flag	Information to log
i	Status messages
w	Nonfatal warnings
e	All error messages
a	Start up of actions
r	Action-specific records
u	User requests
c	Initial user interface parameters
m	Out-of-memory or fatal exit information
o	Out-of-disk-space messages
p	Terminal properties
v	Verbose output
x	Extra debugging information. Only available on Windows Server 2003
+	Append to existing file
!	Flush each line to the log

Flag	Information to log
*	Wild card. Log all information except for the v and x options. To include the v and x options, specify /l*vx

Package-specific MSI Properties

The MSI installation packages for the following DSM components and plug-ins support package-specific installation properties:

- DSM Explorer
- Basic Inventory Agent
- Asset Management Agent
- Data Transport Service Agent
- Remote Control Agent
- Software Delivery Agent
- Scalability Server
- Manager
- ENC Gateway Server

Note: You must pass the package-specific MSI properties as user parameters in your software job. For more information about user parameters, see the Jobs Tab topic in the Software Delivery section of *DSM Explorer Help*.

Prerequisites for Installing MSI Packages

Before installing any of the MSI packages, it is necessary to install the ETPKI libraries and the CA Secure Socket Adapter. For the required versions of these prerequisites, see the Third-Party Installation Packages (see page 160) section. Before installing the Asset Management MSI package, it is necessary to install the Systems Performance LiteAgent.

- **Installing the CAPKI libraries:**

  The setup for CAPKI is located on the CA ITCM installation media (CD/DVD) in the WindowsProductFiles_x86\CAPKI directory.

  To install the CAPKI libraries, use the following command line:

  ```
  setup install caller=CADSMCAPKI
  ```

- **Installing the CA Secure Socket Adapter:**

  The CA Secure Socket Adapter can be installed using the Secure Socket Adapter installer, which is located in the WindowsProductFiles_x86\SSA directory on the CA IT Client Manager installation media (CD/DVD).

  To install the CA Secure Socket Adapter, use the following command line:

  ```
  msiexec.exe
  /i"D:\WindowsProductFiles_x86\SSA\CASockAdapterSetupWin32NoEtpki.msi" /l*v
  "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\DSMSetupSSA.log" /qb-!
  ```

- **Installing the Systems Performance LiteAgent:**

  The Systems Performance LiteAgent can be installed using the Systems Performance LiteAgent installer, which is located in the WindowsProductFiles_x86\PMLA directory on the CA ITCM installation media (CD/DVD). The Systems Performance LiteAgent DSM Client also needs to be installed.

  To install the Systems Performance LiteAgent, use the following command line:

  ```
  msiexec.exe /i"D:\WindowsProductFiles_x86\PMLA\CA_SysPerf_LiteAgent.msi" /l*v
  "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\DSMSetupPMLiteAgent.log" /qb-!
  ```

  To install the Systems Performance LiteAgent DSM Client, use the following command line:

  ```
  msiexec.exe /i"<Network
  drive>\WindowsProductFiles_x86\PMLA_Client\CA_SysPerf_LiteAgent_UAM.msi" /l*v
  "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\DSMSetupPMLiteAgentClient.log" /qb-!
  ```

MSI Properties for the Explorer Package

The MSI install package for the DSM Explorer (Explorer.msi) supports the following package-specific properties:

ADDLOCAL

Specific features that can be selected for installation.

Value	Description
Explorer	Explorer common components (mandatory for the Explorer installation)
ExpAM	Asset Management plug-in
ExpRC	Remote Control common plug-in
ExpSD	Software Delivery common plug-in
ExpSDB	Boot Manager plug-in
ExpSDM	Software Delivery Manager Client API
ExpRP	Reporter plug-in
ALL	Selects all the features above.

ADMINCONSOLE_MANAGER

Manager system the DSM Explorer should connect to.

Value: System name or IP address

MSI Properties for the Basic Inventory Agent Package

The MSI install package for the basic inventory agent plug-in (AgtBHW.msi) and ENC Client supports the following package-specific properties:

AGENT_SERVER

Scalability server the agent should connect to.

Value: System name or IP address

AGENT_DEFAULTGROUPS

A group or a list of management groups created at the manager where the agent automatically registers.

Value: A comma-separated list of group names

Example: Grp1/subgroup1,Group2,...

ENC_CLIENT_ENABLED

Specifies whether the ENC Client should be enabled when the basic hardware inventory is installed. By default, the client files are copied to the computer but are not running. This simplifies the installer and allows a simple configuration job to enable the client at a later date, if required.

Value: 0 (leave inactive), 1 (make active)

Note: The following parameters do *not* need to be specified if the ENC Client is not being enabled.

ENC_SVR_ADDR

The ENC Gateway Server to which this client should connect.

Value: FQN of the server

ENC_SVR_TCP_PORT

TCP port on the ENC Gateway Server to connect to.

Default: 443

ENC_SVR_HTTP_PORT

HTTP port on the ENC Gateway Server to connect to.

Default: 80

ENC_HTTP_PROXY_ADDR

Address of a HTTP internet proxy that the ENC Client must connect to in order to connect outside the local network.

ENC_HTTP_PROXY_PORT

Port number on the proxy to connect to.

Default: 8080

ENC_PROXY_ORDER

The set of connection types to be attempted by the ENC Client. If omitted, a default order is used.

Value: This is a space separated list of zero or more of the following keywords: socket, socks4Anon, socks5Auth, socks5Anon, httpConnect, http, and httpProxy.

ENC_SOCKS_ADDR

Address of a SOCKS internet proxy that the ENC Client must connect to in order to connect outside the local network.

Value: FQN or IP address of the server

ENC_SOCKS_PORT

Port number on the proxy to connect to.

Default: 1080

ENC_SOCKS_USER

Name of the user to authenticate when connecting to a SOCKS server.

Example: socksuser

ENC_SOCKS_PW

Plain text password of the user specified through ENC_SOCKS_USER.

ENC_HTTP_PROXY_USER

Name of the user to authenticate when connecting to a HTTP server.

Example: httpuser

ENC_HTTP_PROXY_PW

Plain text password of the user specified through ENC_HTTP_PROXY_USER.

Note: For more information about ENC properties, see the *encUtilCmd Command Reference*. Also, see the ENC Gateway Policy Group topic in the Configuration Policy section of the *DSM Explorer Help*.

MSI Properties for the Asset Management Agent Package

The MSI install package for the Asset Management agent plug-in (AgtAM.msi) supports the following package-specific properties:

AGENT_SERVER

Scalability server the agent should connect to.

Value: System name or IP address

AGENT_DEFAULTGROUPS

A group or a list of management groups created at the manager where the agent automatically registers.

Value: A comma-separated list of group names

Example: Grp1/subgroup1,Group2,...

MSI Properties for the Data Transport Service Agent Package

The MSI install package for the Data Transport Service (DTS) agent plug-in (AgtDTS.msi) supports the following package-specific properties.

SC_DSMPROP

Shortcut to the agent property dialog.

Value	Description
1	A shortcut to the agent property dialog will be introduced into the Start menu.
0	No shortcut is created.

ADDLOCAL

Specific features that can be selected for installation.

Value	Description
Agent	Agent common parts (mandatory for any agent installation)
AgtDTS	Data Transport Service agent common parts (mandatory for the DTS agent installation)
ALL	Selects all the features above.

AGENT_DEFAULTGROUPS

A group or a list of management groups created at the manager where the agent automatically registers.

Value: A comma-separated list of group names

Example: Grp1/subgroup1,Group2,...

MSI Properties for the Remote Control Agent Package

The MSI install package for the Remote Control agent plug-in (AgtRC.msi) supports the following package-specific properties:

SC_DSMPROP

Shortcut to the agent property dialog.

Value	Description
1	A shortcut to the agent property dialog will be introduced into the Start menu.
0	No shortcut is created.

ADDLOCAL

Specific features that can be selected for installation.

Value	Description
Agent	Agent common parts (mandatory for any agent installation)
AgtRC	Remote Control agent common parts (mandatory for the Remote Control agent installation)
AgtRCA	Remote Control Host
AgtRCV	Remote Control Viewer
AgtRCP	Remote Control Replayer
ALL	Selects all of the features above.

AGENT_SERVER

Scalability server the agent should connect to.

Value: System name or IP address

RC_AGENT_STANDALONE

Value	Description
0	Remote Control agent is centrally managed
1	Remote Control agent is stand-alone

AGENT_DEFAULTGROUPS

A group or a list of management groups created at the manager where the agent automatically registers.

Value: A comma-separated list of group names

Example: Grp1/subgroup1,Group2,...

MSI Properties for the Software Delivery Agent Package

The MSI install package for the Software Delivery agent plug-in (AgtSD.msi) supports the following package-specific properties:

SC_DSMPROP

Shortcut to the agent property dialog.

Value	Description
1	A shortcut to the agent property dialog will be introduced into the Start menu.
0	No shortcut is created.

ADDLOCAL

Specific features that can be selected for installation.

Value	Description
Agent	Agent common components (mandatory for any agent installation)

Value	Description
AgtSD	Software Delivery agent common components (mandatory for the Software Delivery agent installation)
AgtSDA	Software Delivery components (mandatory for the SD Catalog)
AgtSDC	Software Delivery Catalog components
ALL	Selects all of the features above.

AGENT_SERVER

Scalability server the agent should connect to.

Value: System name or IP address

AGENT_DEFAULTGROUPS

A group or a list of management groups created at the manager where the agent automatically registers.

Value: A comma-separated list of group names

Example: Grp1/subgroup1,Group2,...

MSI Properties for the Scalability Server Package

The MSI install package for Scalability Server (Server.msi) supports the following package-specific properties:

FIPS_MODE

Defines the FIPS mode set by the CA ITCM installer.

Value	Description
1	FIPS-preferred
2	FIPS-only

ADDLOCAL

Specific features that can be selected for installation.

Value	Description
Server	Scalability server common components (mandatory for any server installation)
SrvAM	Asset Management scalability server plug-in
SrvSD	Software Delivery scalability server plug-in
SrvRC	Remote Control scalability server plug-in
ALL	Selects all of the features above.

SRV_SDBPATH

Directory path where the scalability server database should be installed.

SERVER_PATH

Directory path where scalability server-specific data should be installed.

SERVER_MANAGER

Manager system the scalability server should connect to.

Value: System name or IP address

SERVER_ENGINE

Engine system the scalability server should connect to. If this parameter is not specified, the system engine is used by default.

Value: Engine name

BS_OS_PATH

Directory path where the OS images and other Boot Server-specific data are stored. The path must end with the string \SDBS\var.

Example: f:\Program Files\CA\DSM\Server\SDBS\var

CREATESDMSISHARE

Share to access MSI packages registered to the Software Delivery manager.

Value	Description
1	Creates a share to access the MSI packages.

Value	Description
0	Does not create a share SERVER_ENGINE.

CREATESDLIBSHARE

Share to access packages registered to the Software Package Library.

Value	Description
1	Creates a share to access the packages.
0	Does not create a share.

BOOTSERVER_ENABLED

Determines whether to enable the Boot Server service.

Value	Description
0	Do not enable the Boot Server service.
1	Enable the Boot Server service.

BOOTSERVER_DISABLESHARES

Share to access packages registered to the Boot Server.

Value	Description
0	Creates a share to access the packages.
1	Does not create a share.

MSI Properties for the Manager Package

The MSI install package for manager (Manager.msi) supports the following package-specific properties:

ADDLOCAL

Specific features that can be selected for installation.

Value	Description
Manager	Manager common components (mandatory for any manager installation)
MgrInf	Manager common infrastructure (mandatory for any manager installation)
MgrDC	Engine plug-in (mandatory for any manager installation)
MgrAM	Asset Management manager plug-in
MgrRC	Remote Control manager plug-in
MgrSD	Software Delivery manager plug-in
MgrDTS	Data Transport Service manager plug-in (mandatory for any Software Delivery manager installation)
MgrDM	Deployment manager plug-in
MgrIP	Image Prepare manager plug-in
ALL	Select all of the features above.

DMSOFTLIBDIR

Directory path where the packages for DMDeploy should be installed.

DMKEYLOCATION

Directory path for the Deployment Manager key file.

SDLIBRARY

Directory path where the Software Package Library should be installed.

MANAGER_ROLE

Role of the manager.

Value	Description
0 = Enterprise	The manager works as an enterprise manager.

Value	Description
1 = Domain Member	The manager works as a domain manager within an enterprise.
2 = Standalone Manager	The manager works as a standalone domain manager.

ENTERPRISE_NAME

Enterprise manager system the domain manager should connect to if the Domain Member role (value = 1) was defined. Otherwise, this property is empty.

Value: System name or IP address

WAC_MANAGER

Web Console manager system for a standalone Web Console installation.

Value: System name or IP address

ENGINE_MANAGER

Engine manager system for a standalone Engine installation.

Value: System name or IP address

DSM_TOMCAT_PORT

TCP/IP port where the handler listens for requests.

Default: 8090

DSM_TOMCAT_SHUT

TCP/IP port where the handler listens for shutdown requests.

Default: 8095

DSM_TOMCAT_AJP

Port where the worker listens for Ajp13 requests in order to forward requests to out-of-process workers using the Ajpv13 protocol.

Default: 8020

DB

Type of the database used.

Value: SQLServer or Oracle

DBSERVER

Name of the system where the database resides.

Value: System name or IP address

DBUSERNAME

Windows user name for database access.

DBPASSWORD

Password for DBUSERNAME.

DBVUSER

Vnode on the database system, if the database is Ingres and if a remote database system is used.

DBVPWD

Password for DBVUSER.

DBSW

Flags whether the Software Signatures for software detection should be inserted (included) into the Management Database or not (excluded).

Value	Description
excl_sw	Do not insert software signatures.
incl_sw	Insert software signatures.

FAILOVER_ENABLED

Flags whether recovery support is enabled or disabled.

Value	Description
0	Recovery support is disabled.
1	Recovery support is enabled.

FAILOVER_STATUS

Flags whether this manager is the active or passive node in a clustered environment.

Value	Description
0	This manager is a passive manager.
1	This manager is the active manager.

FAILOVER_CLUSTER_NAME

Cluster name of the manager.

MSI Properties for the ENC Gateway Server Package

The MSI install package for the ENC Gateway Server supports the following package-specific properties:

AGENT_SERVER

Scalability server the agent should connect to.

Value: System name or IP address

ENC_CLIENT_ENABLED

Specifies whether the ENC Client should be enabled when the ENC Gateway server is installed.

Value: 0 (leave inactive), 1 (make active)

ENC_SERVER_TYPE

Specifies the roles for the ENC Gateway server. This should be one or more of the following values listed in the table following, separated by spaces. An ENC Gateway server can operate in one or more roles. If a manager is specified, a server is automatically configured as well. The ENC Client is also automatically configured to register with this server.

If an ENC Gateway server only is configured, the client registers with this one too.

In the above two cases, the configuration parameters for the client are not required, except for ENC_CLIENT_ENABLED.

If only a router is configured, then both the client and router must register with another ENC Gateway server. This is done by setting the ENC_SVR_ADDR parameter.

Value	Description
ENC_SRS	Configure to operate as an ENC Gateway registration server.

Value	Description
ENC_ROUTER	Configure to operate as an ENC Gateway router.
ENC_MRS	Configure to operate as an ENC Gateway registration manager.

ENC_SVR_ADDR

If installing an ENC Gateway router, this should be the ENC Gateway server that it will register with.

If installing an ENC Gateway registration server, this should be the ENC Gateway registration manager that it will register with.

Value: FQN of the ENC Gateway server or manager to register with.

Note: If installing an ENC Gateway manager, then this is configured automatically.

ENC_SVR_TCP_PORT

TCP port on the ENC Gateway manager to connect to.

Default: 443

Note: If installing an ENC Gateway manager, then this is configured automatically.

ENC_SVR_HTTP_PORT

HTTP port on the ENC Gateway manager that the ENC Gateway registration server or router will connect to.

Default: 80

Note: If installing an ENC Gateway registration manager, then this is configured automatically. This needs only be set for Gateway servers or routers.

Note: For more information about ENC properties, see the *encUtilCmd Command Reference*. Also, see the ENC Gateway Policy Group topic in the Configuration Policy section of the *DSM Explorer Help*.

Additional Properties for msiexec

The following properties are common to all of the CA Technologies provided MSI installation packages:

CA

Installation directory on the target system.

Example: C:\Program Files\CA

CONFIGDATA_LOCATION

Installation directory for the package's configuration data including the configuration store (comstore).

Default: Product installation directory.

Example: C:\Program Files\CA\DSM

SHAREDCOMPONENTS

Installation directory for the package's shared components.

Example: C:\Program Files\CA\SC

Note: **Once a package has been installed, the values of these common properties are fixed for any other packages subsequently installed.**

For each MSI installation package you can additionally use the following properties:

DSM_LANGUAGE

Specifies the language of the CA IT Client Manager installation. Possible values are: enu (English (U. S.)), deu (German), fra (French), and jpn (Japanese).

The files for all supported language versions of CA IT Client Manager will be installed, but the language specified by DSM_LANGUAGE is used as the language for the actual installation.

Default: Empty (NULL). This causes the Installer to use the system default locale. If the system default locale is not one of the supported languages, enu (English (U. S.)) is used.

Note: DSM_LANGUAGE does not specify the language of the installation wizard dialogs.

REBOOT

Value	Description
REALLYSUPPRESS	If a reboot is necessary, it will suppress it in any case and require a manual execution.

ALLUSERS

Value	Description
0	Installs for a particular user.
1	Installs for all users but the user requires administrative access privileges on the computer.
2	Installs for all users if the user has administrative access; otherwise, it installs for a particular user.

Note: If you are installing DSM components directly using the MSI command line, you should always set ALLUSERS=1 to allow later upgrading, uninstalling, or reinstalling through Software Delivery or Deployment functionality out of a manager. If you do not set the parameter like this or leave it empty, the component is registered for the particular user installing it the first time and cannot be maintained by using manager functions.

ARPSYSTEMCOMPONENT

Setting the property prevents the application from being displayed in the Add or Remove Programs list of the Windows Control Panel. This property has no effect on operating environments earlier than Windows 2000 and Windows XP.

CAF_INSTALL_SERVICE

Value	Description
0 | 1	Should be 1 for the first MSI package you install on the system. For all others it can be 0.

CAF_START_SERVICE

Value	Description
0 | 1	Should be 1 for the last MSI package you install on the system. For all others it should be 0.

FIPS_MODE

Value	Description
1	Installs CA ITCM in FIPS-preferred mode (Default)
2	Installs CA ITCM in FIPS-only mode

Options for msiexec for Uninstall, Repair, and Administrative Installation

You can also use the MSI command line interface to initiate uninstall, repair, or administrative installation tasks:

/x msi_install_package | productcode

Uninstalls a product.

/f [p|o|e|d|c|a|u|m|s|v] msi_install_package | productcode

Repairs a product. This option ignores any property values entered at the command line. The default argument list for this option is “omus”. This option shares the same argument list as the REINSTALLMODE property.

Option	Description
p	Reinstalls only if file is missing.
o	Reinstalls if file is missing or an older version is installed.
e	Reinstalls if file is missing or an equal or older version is installed.
d	Reinstalls if file is missing or a different version is installed.
c	Reinstalls if file is missing or the stored checksum does not match the calculated value. Repairs only files that have msidbFileAttributesChecksum in the Attributes column of the File table.
a	Forces all files to be reinstalled.
u	Rewrites all required user-specific registry entries.
m	Rewrites all required computer-specific registry entries.
s	Overwrites all existing shortcuts.
v	Runs from source and re-caches the local package. Do not use the v reinstall option for the first installation of an application or feature.

/a msi_install_package

Administrative install option. Installs a product to a network share from where it can be installed to the net.

Example of Combining msiexec Options and Properties

The following example shows how you can combine msiexec options and properties.

```
msiexec.exe
/i"N:\DSM_11_2_9999_0_DVD\WindowsProductFiles_x86\Manager\Manager.msi"
/l*v "G:\DOCUME~1\KSYST0~1.TAN\LOCALS~1\Temp\DSMSetupManager.log"
ADDLOCAL=Manager,MgrAM,MgrRC,MgrSD,MgrDC,MgrDTS,MgrDM,MgrIP
REBOOT=REALLYSUPPRESS ALLUSERS=1
CA="G:\Program Files\CA\DSM\"
CAF_INSTALL_SERVICE="1" CAF_START_SERVICE="0"
/qb-! DMSOFTLIBDIR="G:\Program Files\CA\DSM"
SDLIBRARY="G:\Program Files\CA\DSM\SD\ASM\LIBRARY"
ENTERPRISE_NAME="KSYST01U"
MANAGER_ROLE="2" DB="SQLServer"
DBSERVER="KSYST01U" DBUSERNAME="ca_itrm" DBPASSWORD=XXX DBSW="excl_sw"
```

Installation of CA ITCM Using the Command Line in Linux or UNIX

You install CA ITCM on Linux or UNIX using the installdsm script, which is in the distribution directory under LinuxProductFiles_x86/component.

Note: CADSMCMD is provided for Linux only and not other UNIX derivatives. For more information, see the *CLI Reference Guide*.

For convenience and for consistency with the Windows installation, there is a script file called setup.sh in the root directory of the installation DVD. That script calls /LinuxProductFiles_x86/manager/installdsm.

By default, the installer for Linux and UNIX runs in an interactive mode. If CA ITCM is already installed on the system, the installer will give the option to Upgrade/Repair, Modify, or Uninstall.

The installation media also contains a template response file, install.rsp. This file can be used to create unattended installations.

installdsm script-Install CA ITCM on Linux or UNIX

The installdsm script has the following format:

```
installdsm [-f | -r responsefile [/Rname=value…] | -g responsefile ]
```

-f

Forces installation without backup of a possibly existing older product version.

-r *responsefile* [/R*name*=*value* ...]

Performs an unattended installation using the values specified in the response file. The -r option causes installdsm to check that the response file is not empty and contains a valid set of label-value pairs. The /R specification overrides any parameters specified in the response file. Supply a separate /R specification for each parameter that you want to override, for example:

```
installdsm -r rsp.txt \
/RITRM_AUTOSTART_INSTALL=1 \
/RITRM_AUTOSTART_REBOOT=1
```

There is no check for the validity of the parameter names or values, or whether the named parameters are in the response file.

The default list of parameter settings is supplied as a sample response file install.rsp in each of the Linux and UNIX packages.

Each time you use the installer for an interactive installation or to generate a response file for an unattended installation, you can edit the parameter values. After the installation script prompts you for the options, the installer copies the files into place and runs the configuration actions.

-g *responsefile*

Generates a response file. The script displays the dialogs as for an interactive installation, but at the end of the dialog sequence writes all the property values you specify to the named response file.

Response File Setting in Linux and UNIX

An unattended installation of CA ITCM is driven by a response file. The response file is a text file that contains parameter values that control installation and configuration. The response file is generated before the installation, either manually or by using the installdsm script with the -g option. During installation, the response file is read-only.

The CA ITCM installation includes standard response files that you can use to perform an unattended installation. The folder for each component contains an install.rsp file. This sample response file provides a full installation of the component.

Modifying Installation Property Values

The response file contains parameter values (properties) that control installation and initial configuration.

Most CA ITCM parameters have the prefix CA_ITRM, or CA_DSM, or ITRM_ or DSM_, or a prefix that indicates the component. Other parameters may be used by other CA products.

You can override the parameter values in the response file by using installdsm with the /R specification. This lets you modify the default installation behavior when running remote installations using the Infrastructure Deployment wizard or Software Delivery packages.

When you manually edit a response file, be careful with property values that are usually derived from other property values (mostly locations of directories and subdirectories). Do not hard-code a property value that was previously derived from another in order to not break any derivation relationship.

Example

SDLIBRARY (the location of the Software Delivery library) is by default derived from CA_DSM_CONFIGDATA (the location of CA ITCM configuration data), which itself comes from CA_ITRM_BASEDIR (the main CA ITCM location). These relationships are maintained in the supplied install.rsp response file. In a response file, if CA_DSM_CONFIGDATA is hard-coded as CA_DSM_CONFIGDATA=/data/CA/ConfigDataLocation and SDLIBRARY is hard-coded as SDLIBRARY=/data/CA/SDLibrary, the derivation relationships among CA_ITRM_BASEDIR, CA_DSM_CONFIGDATA, and SDLIBRARY are broken.

Note: Agent package-specific options are those installation parameters used during interactive deployment to specify the "additional UNIX install options" on the Agent Configuration page of the Infrastructure Deployment wizard. On that page, you can enter multiple install options, separated by spaces, to override existing options.

Basic Installation Properties

CA_ITRM_BASEDIR

Specifies the product installation directory. Only DSM components are stored in this directory, while components shared with other CA Technologies products are stored in a directory pointed to by the $CASHCOMP environment variable. All DSM components must use the same value for $CA_ITRM_BASEDIR. Therefore, if you are deploying DSM agents using the Infrastructure Deployment wizard or command line from a domain manager, you must specify the required value for CA_ITRM_BASEDIR in the arguments to the DMPrimer component, which is typically the first DSM component to be installed on a computer. See Pass Options to the DMPrimer Installation (see page 235) for further details.

Default: /opt/CA/DSM

CA_DSM_CONFIGDATA

Specifies the directory into which configuration data is installed.

Default: $CA_ITRM_BASEDIR

CASHCOMP

Specifies the parent directory for common components and link directories. If this variable has been set by other currently installed components, it will not be changed. The $CALIB and $CABIN environment variables are derived from CASHCOMP. All CA Technologies software components must use the same value for $CASHCOMP on a given computer. Therefore, if you are deploying DSM agents using the Infrastructure Deployment wizard or command line from a domain manager, you must specify your required value for CASHCOMP in the arguments to the DMPrimer installation, which is typically the first DSM component to be installed on a computer. See Pass Options to the DMPrimer Installation (see page 235) for further details.

Default: /opt/CA/SharedComponents

DSM_ALLOW_SOFT_PREREQS

Specifies whether installation should continue even if a software prerequisite check fails. Specify 1 to force installation even if required software prerequisites are not present.

Important! Disabling the prerequisites check may result in a nonfunctional installation of CA IT Client Manager!

Default: 0 (no)

DSM_LANGUAGE

Specifies the language of the installation. Possible values are enu (English (U. S.)), deu (German), fra (French), and jpn (Japanese). Even if the property value is not enu, the files for the enu installation are always installed in addition to the files for the specified language.

Default: Empty (NULL). This causes the Installer to use the system default locale. If the system default locale is not one of the supported languages, enu (English (U. S.)) is used.

Note: DSM_LANGUAGE does not specify the language of the installation wizard dialogs.

ITRM_AUTOSTART_INSTALL

Specifies whether to start DSM daemons after installation. Specify 0 to cause the DSM daemons to not be started after installation.

Default: 1 (yes)

ITRM_AUTOSTART_REBOOT

Specifies whether to start DSM daemons when the host is rebooted. Specify 0 to cause the DSM daemons to not be autostarted.

Default: 1 (yes)

ITRM_INST_CMDLINE

Specifies whether to install the software delivery and automated deployment (DMSweep) command line utilities. Specify 0 to not install these utilities.

Default: 1 (yes)

ITRM_SETUP_SYS_PROFILE

Specifies whether to modify the system profile (/etc/profile or equivalent) to set up the DSM environment for all login users. Specify 0 to leave the system profile unmodified.

Default: 1 (yes)

FIPS_MODE

Specifies the FIPS mode of CA ITCM. Specify 1 for FIPS-preferred mode and 2 for FIPS-only mode.

Default: 1 (FIPS-preferred)

Agent General Properties

ITRM_INST_AGENT

Specifies whether to install any DSM agents. If this is not set, no agent features are installed unless other features depend on them. Specify 0 to not deploy any agent features unless required by other settings.

Default: 1 (yes)

ITRM_SERVER

Specifies the host name of the scalability server that the DSM agent will connect to. This parameter is used only if $ITRM_INST_AGENT is set to 1.

Default: *Local host name*

ITRM_AGENT_DEFAULTGROUPS

Specifies which management groups the agent should join, in a comma-separated list without any spaces.

Default: Null (which implies that the agent will join no groups)

Scalability Server General Properties (Linux only)

ITRM_INST_SERVER

Specifies whether to install a DSM scalability server. If not set, no scalability server features are installed. This parameter is ignored for agent-only packages. Specify 0 to not install a scalability server.

Default: 1 (yes)

ITRM_MANAGER

Specifies the host name of the domain manager that the DSM scalability server reports to. This parameter is used only if $ITRM_INST_SERVER is set to 1.

Default: *Local host name*

Scalability Server Properties (Linux only)

ITRM_ENGINE

Specifies the name of the engine the scalability server uses. An empty value specifies the system engine.

Default: Null

ITRM_PATH_COMMON_SERVER_DB

Specifies the path of the scalability server database directory.

Default: $CA_DSM_CONFIGDATA/Server/serverdb

Asset Management Agent Properties

ITRM_INST_AM_AGENT

Specifies whether to install the asset management (AM) agent. Specify 0 to not install this agent.

Default: 1 (yes)

ITRM_AMAGENT_CMDFILE_USER

Specifies the user ID under which the AM agent executes a command file.

Default: root

ITRM_AMAGENT_EXTUTILITY_USER

Specifies the user ID under which the AM agent executes a utility.

Default: root

ITRM_AMAGENT_DMSCRIPT_USER

Specifies the user ID under which the AM agent executes a DMScript.

Default: root

ITRM_AMAGENT_USER_INVENTORY

Specifies whether to install the user inventory module. Specify 0 to not install the user inventory module.

Default: 1 (yes)

ITRM_AMAGENT_WITHCRONINFO

Specifies whether to show crontab information. Specify 0 to not show information.

Default: 1 (yes)

ITRM_AMAGENT_WITHUSERINFO

Specifies whether to show user information. Specify 0 to not show information.

Default: 1 (yes)

ITRM_AMAGENT_PRIO_LEVEL

Increments asset management process priority. The priority range is from –20 to 19.

Default: 0

ITRM_AMAGENT_EXACTINTERVAL

Specifies whether the AM agent should run at intervals (value = 1) or at fixed times (value = 0).

Default: 1

ITRM_AMAGENT_RANDOM

Specifies whether the AM agent should run during a specific interval (value = 0) or a randomly chosen interval (value = 1). This parameter is significant only if $ITRM_AMAGENT_EXACTINTERVAL=1.

Default: 0

ITRM_AMAGENT_WEEKLY

Specifies that the AM agent should run every n weeks. This parameter is significant only if $ITRM_AMAGENT_EXACTINTERVAL=1.

Default: 0

ITRM_AMAGENT_DAILY

Specifies that the AM agent should run every n days. This parameter is significant only if $ITRM_AMAGENT_EXACTINTERVAL=1.

Default: 1

ITRM_AMAGENT_HOURLY

Specifies that the AM agent should run every n hours. This parameter is significant only if $ITRM_AMAGENT_EXACTINTERVAL=1.

Default: 0

ITRM_AMAGENT_EXMONDAY

Specifies that the AM agent should not run on Mondays, if value = 1. This parameter is significant only if $ITRM_AMAGENT_EXACTINTERVAL=0.

Default: 0 (agent runs on Mondays)

ITRM_AMAGENT_EXTUESDAY

Specifies that the AM agent should not run on Tuesdays, if value = 1. This parameter is significant only if $ITRM_AMAGENT_EXACTINTERVAL=0.

Default: 0 (agent runs on Tuesdays)

ITRM_AMAGENT_EXWEDNESDAY

Specifies that the AM agent should not run on Wednesdays, if value = 1. This parameter is significant only if $ITRM_AMAGENT_EXACTINTERVAL=0.

Default: 0 (agent runs on Wednesdays)

ITRM_AMAGENT_EXTHURSDAY

Specifies that the AM agent should not run on Thursdays, if value = 1. This parameter is significant only if $ITRM_AMAGENT_EXACTINTERVAL=0.

Default: 0 (agent runs on Thursdays)

ITRM_AMAGENT_EXFRIDAY

Specifies that the AM agent should not run on Fridays, if value = 1. This parameter is significant only if $ITRM_AMAGENT_EXACTINTERVAL=0.

Default: 0 (agent runs on Fridays)

ITRM_AMAGENT_EXSATURDAY

Specifies that the AM agent should not run on Saturdays, if value = 1. This parameter is significant only if $ITRM_AMAGENT_EXACTINTERVAL=0.

Default: 0 (agent runs on Saturdays)

ITRM_AMAGENT_EXSUNDAY

Specifies that the AM agent should not run on Sundays, if value = 1. This parameter is significant only if $ITRM_AMAGENT_EXACTINTERVAL=0.

Default: 0 (agent runs on Sundays)

ITRM_AMAGENT_EXECUTETIME

Specifies that the AM agent should start running at this time during the day. The time has the format hh:mm (Hour:Minute). This parameter is significant only if $ITRM_AMAGENT_EXACTINTERVAL=0.

Default: 00:00 (midnight)

Asset Management General Properties

ITRM_INST_AM

Specifies whether to install the asset management (AM) component. If not set, no AM features are installed. Specify 0 to not install any AM features.

Default: 1 (yes)

Asset Management Software Usage Scalability Server Properties (Linux only)

ITRM_INST_AM_METER_SERVER

Specifies whether to install the asset management (AM) software usage scalability server. Specify 0 to not install the software usage scalability server.

Default: 1 (yes)

Asset Management Sector Server Properties (Linux only)

ITRM_INST_AM_SECTOR_SERVER

Specifies whether to install the asset management (AM) sector server. Specify 0 to not install the sector server.

Default: 1 (yes)

DMPrimer Properties

ITRM_INST_DMPRIMER

Specifies whether to install the DMPrimer. Specify 0 to not install the DMPrimer.

Default: 1 (yes)

Data Transport Service General Properties (Solaris only)

DTS_PPP_USER

(Used on Solaris only) Specifies whether to create a PPP user. This parameter is ignored if either of the protocols asppp or Solstice PPP is not detected. Specify 1 to create a PPP user.

Default: 0 (no)

RC General Properties (Linux/Mac OS X only)

ITRM_INST_RC

Specifies whether to install any Remote Control components. If not set, no Remote Control features are installed. Specify 0 to not install any Remote Control components.

Default: 1 (yes)

Remote Control Agent Properties (Linux/Mac OS X only)

ITRM_INST_RC_AGENT

Specifies whether to install the Remote Control agent. Specify 0 to not install the agent.

Default: 1 (yes)

ITRM_RC_AGENT_STANDALONE

Specifies whether the Remote Control agent is centrally managed (value = 0) or standalone (value = 1).

Default: 0

ITRM_RC_AGENT_IN_MGMT_GROUPS

Specifies whether a managed agent will appear in management groups.

Default: 1 (yes)

Remote Control Scalability Server Properties (Linux only)

ITRM_INST_RC_SERVER

Specifies whether to install the Remote Control scalability server component. Specify 0 to not install a Remote Control scalability server.

Default: 1 (yes)

Software Delivery General Properties

ITRM_INST_SD

Specifies whether to install any software delivery (SD) components. If not set, no SD features will be installed. Specify 0 to not install any SD components.

Default: 1 (yes)

Software Delivery Agent Properties

ITRM_INST_SD_AGENT

Specifies whether to install the software delivery (SD) agent. Specify 0 to not install the agent.

Default: 1 (yes)

CA_DSM_REPLACE_PRE_R11_SD_AGENT

Specifies whether to replace (that is, remove) the pre-r11 SD agent or allow co-existence. Only relevant if a pre-r11 SD agent is already installed on the system. Specify 1 to cause older agents to be removed.

Default: 0 (co-existence)

SD Boot Server Properties (Linux only)

FIPS_MODE

Defines the FIPS mode set by the CA ITCM installer. Valid values are 1 (FIPS-preferred) and 2 (FIPS-only).

ITRM_INST_SD_BOOTSERVER

Specifies whether to install the software delivery (SD) boot server. Usually, scalability servers and boot servers are installed on the same host. Specify 0 to not install a boot server.

Default: 1 (yes)

ITRM_BOOTSERVER_OS_INSTALL_PATH

Specifies the location of the OSIM OS images library.

Default: $ITRM_PATH_COMMON_SERVER_DB/SDBS/var

BOOTSERVER_ENABLED

Determines whether to enable the Boot Server service. Specify 0 to disable the service.

Default: 1 (yes)

BOOTSERVER_DISABLESHARES

Specifies whether to disable SMB shares. Specify 0 to enable SMB shares.

Default: 1 (yes)

SD Scalability Server Properties (Linux only)

ITRM_INST_SD_STAGSERVER

Specifies whether to install the software delivery (SD) scalability server component. Usually, scalability servers and boot servers are installed on the same host. Specify 0 to not install an SD scalability server.

Default: 1 (yes)

SDLIBRARY

Specifies the location of the Software Package Library.

Default: $CA_DSM_CONFIGDATA/sd/asm/library

ITRM_SD_EXPORT_NFS_SHARE

Specifies whether to export $SDLIBRARY as an NFS share. Specify 1 to export $SDLIBRARY.

Default: 0 (no)

ITRM_SD_EXPORT_SAMBA_SHARE

Specifies whether to export $SDLIBRARY as a SAMBA share. Specify 1 to export this as a SAMBA share.

Default: 0 (no)

DSM_SD_INSTALL_CCS_CALENDAR

Specifies whether to install CCS calendaring (event management). Available only if the CCS distribution is available or already installed. Specify 1 to install CCS calendaring.

Default: 0 (no)

Web Console Properties (Linux only)

ITRM_INST_WEBGUI

Specifies whether to install the Web Console. Specify 1 to install the Web Console.

Default: 0 (no)

Web Services Properties (Linux only)

ITRM_INST_WEBSERVICES

Specifies whether to install web services. Specify 1 to install web services.

Default: 0 (no)

WAC_MANAGER

Specifies the manager that web services will connect to.

Default: *Local host name*

DSM_TOMCAT_PORT

Specifies the TCP/IP port where the handler listens for requests.

Default: 8090

DSM_TOMCAT_SHUT

Specifies the TCP/IP port where the handler listens for shutdown requests.

Default: 8095

DSM_TOMCAT_AJP

Specifies the port where the worker process listens for Ajp13 requests in order to forward requests to out-of-process workers using the Ajpv13 protocol.

Default: 8020

ITRM_AMS_WEBPORT

Specifies the Asset Maintenance System web port.

Default: 8080

PIF Packager Properties

ITRM_INST_PACKAGER

Specifies whether to install the PIF Product Software Development Kit (SDK). The SDK can be installed on its own, that is, independently of CA ITCM. Specify 0 to not install the SDK.

Default: 1 (yes)

Documentation Properties (Linux only)

ITRM_INST_DOC

Specifies whether to install documentation. Specify 0 to not install the documentation set.

Default: 1 (yes)

Installation Log Files

Any activity of the Installer in CA IT Client Manager is logged in files that are automatically created by the Installer.

CA Technologies provides a log file collection tool called dsminfo, which helps you by picking up any available information you need to analyze a problem you may have with CA ITCM.

The dsminfo tool is available at CA Online Support and can be downloaded from the following location: http://support.ca.com.

Installation Log Files on Windows

The Installer creates the following types of log files on Windows:

DSMSetupxxx.log

Created by the Microsoft Windows Installer (MSI) and stored under the directory specified by the %temp% environment variable. This log file is created when using the manager, scalability server, DSM Explorer, and agents. Each MSI package creates a separate log file.

TRC_*xxx*.log

Created by internal processes and stored under the directory specified by the %temp% environment variable. These files document the configuration of the installed components, for example, configuration of CAF, manager, or database.

In the log file names, the string *xxx* is replaced with the name of the component the log information belongs to, for example, DSMSetupManager.log.

Installation Log Files on Linux and UNIX

The initial installation log file on Linux and UNIX is called ca-dsm.install.log. If you modify the installation, the log file is called ca-dsm.reinstall.log. When you remove the product, the log file is ca-dsm.deinstall.log.

On Linux and UNIX the installation log files are stored in the following directories:

- /tmp
- /opt/CA/installer/log

Version Information About Installed DSM Components

The Installer provides version information about installed components and features of CA IT Client Manager. This information can also be accessed using the dsmver command.

Version information is shown in the format M.m.b.r, where M = major release number, m = minor release number, b = build number, r = revision/patch number. For example, version 12.0.01234.1 is major release 12, minor release 0, build 1234, revision 1.

To display the installed components and features and their versions, type the dsmver command at the command line.

The dsmver command has the following format:

```
dsmver
```

The output format of the version information is as shown in the following example:

```
Desktop and Server Management
-----------------------------------------
Explorer - Asset Management         12.0.1234.1
Explorer - Remote Control           12.0.1234.1
Explorer - Software Delivery        12.0.1234.1
Manager - Engine                    12.0.1234.1
Manager - Asset Management          12.0.1234.1
Manager - Data Transport            12.0.1234.1
Server
. . . . .
```

Chapter 4: Post-Installation Tasks

This chapter provides information about modifying, repairing, upgrading, and uninstalling an existing installation.

This section contains the following topics:

Changing the Product Language After Installation

The following list provides some relevant information about changing the product language of CA IT Client Manager after installation:

- There are alternative techniques for changing the product language after installation:
  - Changing the language of already installed DSM components is supported for the components Explorer, scalability server, and agents. On the agent host, run the ccnfcmda command as follows:

    ```
    ccnfcmda -cmd SetParameterValue -ps itrm/common/localization
    -pn language -v lang
    ```

    The value of *lang* specifies the desired language. Possible values are enu (English (U.S.)), deu (German), fra (French), and jpn (Japanese); for agents additionally chs (Simplified Chinese), esn (Spanish), and kor (Korean).

    Note: For more detailed information about the ccnfcmda configuration agent command, type <command> /? at the command prompt.
  - Create a query-based policy to run the ccnfcmda command as described above.
- Changing the language for the manager is not possible after manager installation

- When configuring the product language of CA IT Client Manager, make sure that the language package for the specified language has been installed because there is no check for availability. If no language package for the specified product language has been installed, CA IT Client Manager falls back to English (U.S.).
- When the language is reconfigured, you must stop and restart CA IT Client Manager using caf stop and caf start, respectively, so that it can take over the new value.

More information:

Multi-Language Installation (see page 107)

Maintaining the MDB

The following tasks provide information about maintaining and synchronizing the management database.

Microsoft SQL Server MDB Maintenance

Microsoft SQL Server (SQL Server) database tables should be optimized every time the database has been updated with significant amounts of data.

To help you with the administration of the management database (MDB) on SQL Server, CA IT Client Manager supplies the DsmMSSqlOpt.bat maintenance script that administrators can apply regularly.

The DsmMSSqlOpt.bat script helps you optimizing the database tables by performing maintenance tasks such as defragmenting the index and updating statistics. The script affects only tables that are owned by CA IT Client Manager.

The DsmMSSqlOpt.bat maintenance script is automatically installed during CA IT Client Manager installation to the following location:

```
%Program Files$\CA\DSM\database\mdb_install\mssql\DsmMsSqlOpt.bat
```

The DsmMSSqlOpt.bat maintenance script is also available on the CA IT Client Manager installation media (DVD) at the following location:

```
Maintenance\Windows\mssql\DsmMsSqlOpt.bat
```

The DsmMSSqlOpt.bat maintenance script can be executed with certain options as follows:

```
DsmMsSqlOpt.bat [-pagecount=n] [-maxfrag=m] [ -usereindex] [ {local | ServerName}
[MDBName] ]
```

-pagecount

Specifies the maximum number *n* of pages of tables or indexes. Tables or indexes with more than the specified number of pages will be defragmented. *n* is a numerical value.

Default: 1000

-maxfrag

Specifies a degree *m* of fragmentation. Tables with the specified degree of fragmentation will be defragmented. *m* is a numerical value.

Default: 10

-usereindex

Specifies that indexes are rebuilt instead of defragmented. By default, the DsmMsSqlOpt script performs defragmentation of indexes.

If you have a DSM enterprise manager in addition to domain managers, remember that the maintenance script needs to be executed against the databases on both tiers. We recommend that you run the script at least once after the first 1,000 computer assets have been registered in the domain database. Subsequently, the script should be run every time an additional 5,000 computer assets have been registered. On the enterprise, maintenance should run every time 5,000 computer assets have been replicated from the associated domain managers.

The DsmMsSqlOpt.bat script must be run locally on the computer where the MDB is installed. The script offers two options: it can be used to rebuild indexes or defragment indexes. Before running the script with the rebuild index option, we recommended that you shut down all manager components that access the MDB. The DSM components should be restarted after the script has finished.

When the script is called with the option to defragment indexes, DSM components may be kept up and running. However, operations initiated by the script are resource-intensive and may have a negative impact on performance. Also, consider that for large databases, defragmentation of indexes may take several hours to complete.

Therefore, you may want to schedule MDB maintenance tasks at times when there is little or no workload on the MDB. For example, the script could be scheduled to launch once a week overnight, or over the weekend.

Important Notes on SQL Server MDB Maintenance

Following are some notes on Microsoft SQL Server MDB maintenance:

- The %TEMP% variable must be set to an appropriate working directory before launching the DsmMsSqlOpt.bat script.
- It is good practice to rebuild indexes with a fragmentation degree over 30% as the first maintenance step because rebuilding indexes runs much faster than defragmentation. To achieve this, you must launch the DsmMsSqlOpt script with the options -usereindex and -maxfrag=30, for example:
  ```
  DsmMsSqlOpt.bat -maxfrag=30 -usereindex
  ```
- After the initial step, all tables with a fragmentation over 10% should be defragmented. This can be done by calling the DsmMsSqlOpt script with the option -maxfrag=10, for example:
  ```
  DsmMsSqlOpt.bat -maxfrag=10
  ```

Oracle MDB Maintenance

To solve performance problems with the Oracle MDB, do one of the following:

- From an Oracle SQL tool on the Solaris Oracle server computer run the command:

  ```
  EXEC DBMS_STATS.gather_schema_stats(ownname =>'MDBADMIN', cascade =>true,
  method_opt=>'FOR ALL COLUMNS SIZE AUTO');
  ```

- Login to the Solaris computer using the Oracle user credentials, and from the command shell run the command as shown in the following example:

  ```
  echo "EXEC DBMS_STATS.gather_schema_stats (ownname => 'MDBADMIN', cascade
  =>true, method_opt=>'FOR ALL COLUMNS SIZE AUTO');"|sqlplus sys/<pwd>@<instance>
  as sysdba
  ```

  In this example, <*pwd*> is the password of the current Oracle instance and <*instance*> is the name of the current Oracle instance (SID).

More information:

Installation of a Remote Oracle MDB (see page 126)

Objects Synchronized to the Target MDB

Objects that are synchronized to both SQL Server and Oracle based target MDBs include the following types:

- **Primary Asset and User Information**
  - Discovered computers
  - Discovered users
  - Discovered computer users (relations between computers and users)
- **Hardware Inventory**
  - Computers, general inventory
- **Software Inventory**
  - Software signatures
  - Computers, software inventory (both signature and heuristic based software inventory)

Creating the Synchronization Task

The synchronization of DSM assets and inventory data with an SQL Server or Oracle-based target MDB is initiated by an engine task that runs at a scheduled time. You create this task and define the scheduling for the task through the DSM Explorer GUI.

The engine task that performs the synchronization of DSM assets and inventory data with an existing MDB on Microsoft SQL Server is created, configured, assigned, scheduled, and run in the same way as any other DSM engine tasks. Follow Control Panel, Engines, All Engines on the DSM Explorer, right-click the engine that should perform the synchronization task, and select Add New Task on the context menu. The Create New Task wizard opens and guides you through the creation of the synchronization task.

On the Create New Task wizard you perform the following main steps:

- On the first wizard page, select the task type Database Synchronization from the Task type drop-down list.
- On the second wizard page, enter an appropriate name and description for the database synchronization task to reflect the purpose and type of the task).

- On the third wizard page, specify the target database type and the credentials for the target MDB, as described in the Synchronization Task Configuration Options (see page 204) section. You can test your settings immediately by clicking the Test Connection button. Before you leave this page, the wizard checks if the target MDB exists and meets the required conditions.
- On the fourth wizard page, click the Set Scheduling button if you want to modify the preset scheduling for the synchronization task, which is "Generally scheduled to run always". Click Finish to use the preset scheduling and terminate the wizard.

Synchronization Task Configuration Options

During the creation of the synchronization task you must specify the credentials (connection properties) for the target MDB on one of the Create New Task wizard pages.

- **SQL Server based target MDB:**

  For an SQL Server based target MDB the required credentials include:

  - Server type of the target MDB (Value: MS SQL Server)
  - Name of the computer that hosts the target MDB
  - Database Server Instance, portnumber (Default: <none>)
  - Database name
  - User name on the target MDB

    The user name is fixed as ca_itrm and cannot be changed.
  - Password on the target MDB

    Important! Here you must enter the password that you specified using the CA_ITRM password parameter in the CA ITCM setup when upgrading the SQL Server MDB for synchronization.

- **Oracle based target MDB:**

  For an Oracle based target MDB the required credentials include:

  - Server type of the target MDB (Value: Oracle)
  - Name of the computer that hosts the target MDB
  - Server ID of the target MDB (Default: orcl)
  - Port number for the target Oracle MDB (Default: 1521)
  - User name on the target MDB

    The user name is fixed as ca_itrm and cannot be changed.
  - Password on the target MDB

    Important! Here you must enter the password that you specified using the CA_ITRM password parameter in the CA ITCM MDB installer when upgrading the Oracle MDB on Solaris for synchronization.

You can immediately test the settings you made by clicking the Test Connection button on the same wizard page. The manager then tries to open a connection to the target MDB. The result of this action is displayed next to the Test Connection button, for example, Connection succeeded.

You can configure the scheduling for the synchronization task by clicking the Set Scheduling button on the Scheduling page of the Create New Task wizard. The default setting is "Generally scheduled to run always".

Options and Restrictions of the Synchronization

You have the following options to perform the synchronization task:

- Synchronization of data from the MDB on the DSM domain manager to the target MDB.
- Synchronization of data from the MDB on the DSM enterprise manager to the target MDB. This includes synchronization of data from all domain managers reporting to the enterprise manager.

There are the following restrictions with the synchronization:

- You should not synchronize data from a DSM domain manager MDB when the associated enterprise manager already synchronizes with the same target MDB. If you do so, this will cause unnecessary data load on the network.
- You should not synchronize data from a DSM enterprise manager MDB when one of its associated domain managers already synchronizes with the same target MDB. If you do so, this will cause unnecessary data load on the network.

Removing Synchronization

If you want to remove the synchronization between the Microsoft SQL Server source MDB and the target MDB, you must delete the synchronization task.

You start the removal of the synchronization task from the All Engine Tasks directory on the DSM Explorer GUI while the synchronization task is linked to an engine. Right-click the engine task and select Delete from the context menu. You will be asked to confirm the removal of the selected item.

However, the synchronization task is not removed immediately. The Delete Task dialog notifies you that the engine needs to run one more time before the synchronization task is removed.

On the Delete Task dialog you can also select that you want the engine to clean up the target MDB regarding synchronized objects. If you do not select this option, the engine cleans up only the source MDB. If you select this option, the status of the synchronization task changes to "Pending for Engine to perform clean-up of database". After the clean-up task has been performed by the engine the next time it is scheduled, the engine unlinks and removes the synchronization task.

Uninstallation of DSM Manager and MDB

When uninstalling the DSM manager, the MDB is not uninstalled and remains on the system.

The MDB is used by different CA Technologies products that may be installed locally together with the MDB or that may be using it remotely. Uninstalling one of these CA Technologies products does not necessarily mean that the MDB is no longer used.

We recommend that uninstalling the MDB and the selected MDB provider should only be done by an authorized administrator after having carefully considered all implications of local or remote usage by other CA Technologies products.

A Microsoft SQL Server MDB can be removed using the Microsoft SQL Enterprise Manager, where you can select the MDB database and delete it. Another tool that can be used to delete an MS SQL Server MDB is SQL Server Management Studio.

To remove an Oracle MDB, use the setup program and select "uninstall" to remove the PIF product part of the MDB schema. Then logging in as 'oracle', you can use the Oracle dbca administration tool to delete the database tables. Finally, any remaining files in the ../opt/CA/SharedComponents/oracle/mdb folder can be removed manually by logging in as 'root'.

Note: For more information about removing an Oracle MDB, see the *MDB Overview* (which is part of the CA ITCM documentation set (Bookshelf)) or the appropriate Oracle documentation.

If you uninstall a DSM manager, you must manually remove the ca_itrm user from the Microsoft SQL Server, as well as the ca_itrm_ams account if present. If the ca_itrm user remains in the Microsoft SQL Server, a new installation of CA ITCM using this SQL Server may not be possible. If CCS has been used and is also uninstalled, the nsmadmin and hostname\TNDUsers accounts will also need to be deleted from SQL Server.

If you uninstall a DSM manager, the corresponding data contained in the MDB is not removed by default.

The CA ITCM installation wizard provides the feature to remove data from the MDB.

If, for any reason, you do not choose this way to remove data from the MDB, you must run the script data_uninstall (see page 208) to clean up the MDB. This script supports Microsoft SQL Server and Oracle. The appropriate versions of the script, data_uninstall.bat (for SQL Server) and data_uninstall.sh (for Oracle), are available at the following locations on the CA ITCM installation DVD:

- *dvdroot*\Maintenance\Windows\mssql\
- *dvdroot*\Maintenance\Windows\oracle\

Copy all files from the respective subdirectory to your local manager system and run the data_uninstall script with appropriate parameters from the command prompt.

Following is a list of scenarios and business cases that explain the use of the data_uninstall script:

Drop Manager forever

If CA ITCM was the only application, you may remove the MDB manually.

Otherwise, run the data_uninstall script and set the flags for -pdata d and -data d.

Clean up Manager to start from scratch

If CA ITCM was the only application, you may remove the MDB manually.

Otherwise, run the data_uninstall script and set the flags -pdata d and -cdata d.

If you want to remove the registered assets as well, you should set the argument -asset d.

Remove Manager but keep all data

In this case, at least some data must be removed referring to file system objects. Therefore, run the data_uninstall script and set the -sdonly flag. This will remove the references to related software delivery file system objects, including Operating System Installation Management (OSIM) and boot information.

data_uninstall Command—Delete Data from the Database

Use the data_uninstall command to delete data from the database or check the database for products and domains registered. The data_uninstall command supports Microsoft SQL Server and Oracle.

This command has different formats:

```
data_uninstall -server server_name
    -instance instance_name:port_number
    -database database_name
    -asset {k | d }
    -pdata {k | d }
    -cdata {k | d }
    -user
    -pwd
```

Deletes data from the database depending on the k or d flags (k = keep the data, d = delete the data) given as arguments. (You will get this usage if you run the command without any arguments.)

```
data_uninstall -server server_name
    -instance instance_name:port_number
    -database database_name
    -check
```

Prints the number of products registered in the MDB as well as the number of domains registered in the database.

```
data_uninstall -server server_name
    -instance instance_name:port_number
    -database database_name
    -sdonly
```

Deletes only software delivery data depending on the object in the file system. This command also deletes all MDB references to OSIM and boot images.

-server *server_name*

Specifies the name of the local RDBMS system.

Important! The name of the database server plus the name of the database instance must have a maximum overall length of 29 characters.

-instance *instance_name*:*port_number*

Identifies the database instance, for example, a Microsoft SQL Server instance name. The specification of the port number is mandatory, except in case of the Microsoft SQL Server default instance. In case of the Microsoft SQL Server default instance, you must use double quotes to define an empty name like -instance "".

-database *database_name*

In the case of SQL Server, specifies the name of the database, for example, mdb.

In the case of Oracle, specifies the SID.

-asset {k|d}

Specifies if asset data should be unregistered. Use -asset k to keep assets and -asset d to unregister assets.

-pdata {k|d}

Specifies if product-specific data should be deleted. Use -pdata k to keep the data and -pdata d to delete the data.

-cdata {k|d}

Specifies if CA ITCM common data should be deleted. Use -cdata k to keep the data and -cdata d to delete common data.

-user *user_name*

Specifies the user name to connect to the database, for example, ca_itrm.

-pwd *password*

Specifies the password of the user specified through -user.

-check

Checks if CA Technologies products are still registered in the database and which domains are registered.

-sdonly

Deletes only software delivery data that relates to objects in the file system, including OSIM and boot data.

Example: Check products and domains

This example only checks if CA Technologies products are still registered in the MDB database and lists all domains registered.

```
data_uninstall -server myMachine
    -instance ""
    -database mdb
    -check
```

Example: Delete data except assets

This example deletes all CA ITCM data from the MDB database but does not deregister the assets.

```
data_uninstall -server myMachine
    -instance ""
    -database mdb
    -check
    -asset k
    -pdata d
    -cdata d
    -user ca_itrm
    -pwd myPassword
```

The data_uninstall Log File

After running the data_uninstall script, a log file with the name data_uninstall.log can be found In the Temporary folder, as follows:

- Windows:
  `%TEMP%`
- Linux:
  `/tmp`

Installation of SQL Bridge

The SQL Bridge synchronization feature is installed in your application environment as part of the DSM manager installation. This means that on the source side of the SQL Bridge no special installation steps are required. However, perform some upgrade steps on the target side of the SQL Bridge for the appropriate MDB.

Upgrade the Target Side with Microsoft SQL Server MDB 1.0.4

Microsoft SQL Server MDB 1.0.4 is used with Unicenter Asset Portfolio Management r11.3 on Windows.

To upgrade the target Microsoft SQL Server MDB

1. Run *Install MDB* setup from the installation DVD.

   This procedure applies MDB patches not yet available on the target MDB and create the ca_itrm database user.

2. To take full advantage of the synchronization feature, download and install the test fix T5D6008 for Windows, which is available at CA Support online. Follow detailed installation instructions provided with the test fix. T5D6008 includes fixes that are applicable for Unicenter Asset Portfolio Management r11.3 on Windows.

Upgrade the Target Side with Microsoft SQL Server MDB 1.5

Microsoft SQL Server MDB 1.5 is used along with CA Service Desk Manager r12 on Windows.

To upgrade the target Microsoft SQL Server MDB, run the “Install MDB” setup from the CA ITCM installation DVD.

This procedure will apply the latest MDB schema updates for DSM on the target MDB and create the ca_itrm database user.

Installation of Oracle Bridge

The Oracle Bridge synchronization feature is installed in your application environment as part of the DSM manager installation. This means that on the source side of the Oracle Bridge no special installation steps are required. However, you need to perform some upgrade steps on the target side of the Oracle Bridge for the MDB.

Upgrade the Target Side with Oracle MDB 1.5 on Solaris

Oracle MDB 1.5 is used along with CA Service Desk Manager r12 on Windows.

To upgrade the target Oracle MDB

1. Run the “Oracle MDB Installer on Solaris" setup, which is available on the CA ITCM Release 12.8 installation DVD.

   This procedure will apply the latest MDB schema updates for DSM on the target MDB and create the ca_itrm database user.

2. In the AMS.Properties file for CA Service Desk Manager add the new configuration parameter:

   ```
   dsm_oracle_ddl=1
   ```

Example

The following example shows how the AMS.Properties file should look:

```
# ca_itrm_ams user password to connect to DSM Domain Database.
dsm_domain_db_password=
# Table Owner for DSM on-the-fly created tables.
# This property should never need to be set unless the tables
# were not created by ca_itrm.
dsm_dbowner=
# If we are running r11.2 or later and want to support
# Oracle Bridging, set the value of dsm_oracle_ddl to 1
dsm_oracle_ddl=1
```

How to Enable a Docking Device on Windows

Occasionally, mobile device users need to exchange or synchronize the information between their mobile device and a computer. Typically, the mobile device, for example, a Personal Digital Assistant (PDA), is connected through a "cradle" or "docking device" that is connected to the serial port or USB port of the computer or directly to the computer through an infrared or Bluetooth interface.

To enable data exchange between the mobile device and the computer using the docking device, you must perform the following installation and configuration steps:

- Install the synchronization software.
  - For Windows CE devices (PocketPC and Windows Mobile):

    Install Microsoft ActiveSync (which is shipped with the PocketPC or Windows Mobile device) on a target computer and connect the device to this computer.

    Note: The Microsoft ActiveSync component needs to be installed before enabling docking device support on a host PC. Also, the Microsoft ActiveSync component must be made aware of the changes to the PATH environment variable which is done during the installation of CA ITCM. This is accomplished by logging off and then on again after the installation of CA ITCM.
  - For Palm OS devices:

    Install the HotSync software (Palm Desktop, which is shipped with the Palm OS device) on a target computer and connect the Palm OS device to this computer.
- Install a Software Delivery or Asset Management agent on the target computer.
- On the manager activate the proxy device for CA ITCM, as follows:
  - Create a new configuration policy, for example, my_dockingdevice_policy, and set the value of the 'DSM/common components/docking_devices' parameter to True.
  - For Software Delivery additionally, set the value of the 'DSM/Agent/Common agent/software delivery docking device' parameter to Palm+WinCE.
  - Apply the policy to the target computer.
- For Windows CE devices, reconnect the mobile device to the target computer (disconnect and connect again).

  For Palm OS devices, synchronize the Palm OS device with its host PC.
- Run "caf register all" on the target computer, or wait up to 24 hours for automatic registration.

How to Run Agents from Source on Windows

CA ITCM allows the Windows Asset Management, Software Delivery, and Remote Control agent components to be executed from an MSI administrative network share installation point. This specific functionality is called *run-from-source*. If an agent has been installed in run-from-source mode, the program executable is loaded and executed from that administrative network share installation point. Configuration files, log files, and so on, are stored on the local disk.

The common CAM and CAWIN components currently must always be installed locally.

After installing an agent in run-from-source mode, the agent system must be rebooted.

To set up an environment to install agents in run-from-source mode

1. Create an MSI administrative installation point.

   Use the interactive installation wizard to go to the WindowsProductFiles_x86 folder and call setup.exe /a. This creates an installation point for the complete product and all of its components.

   If you want to perform the agent installation silently or to install an agent component only, go to one of the agent folders under WindowsProductFiles_x86 and execute the following command:

   ```
   msiexec /a msipackagename /qn /v*l %temp%\ITRMAdminAgt.log"
   ```

   Note: If you want to use the msiexec command for several agent packages, make sure that you use the same root folder for all the agents.

2. Create a network share for the administrative installation point you just created (unless you already have one). You must configure this as a null session share.

3. Install the MSI package from the administrative network share installation point.

   At the target computer where you would like to install the agent in run-from-source mode, you can execute the following command:

   ```
   msiexec /i \\servernode\adminshare\msipackagename ADDSOURCE=ALL
   AGENT_SERVER=servername CAF_START_SERVICE=0 /qn /v*l %temp%\DSMSetupRFS.log
   ```

   This installs the agent silently.

You can also set up an environment to install agents in run-from-source mode using the custom installation option in the installation wizard. Start the installation wizard using an UNC path, *server node**MSI admin share*\setup.exe, follow the custom installation dialog boxes, and configure each agent you want to run from source.

Note: If the administrative network share is hosted by a Windows 2003 Server, you may need to add the agent's machine account to the Windows 2003 Server's Administrators group.

How to Run CA ITCM Services under User Accounts on Windows

While the application framework (CAF) runs under the local system account, occasionally a CA ITCM service such as the Software Delivery agent needs to run under an administrator account. CAF provides this through the following caf command options:

setcreds

The caf setcreds command sets the credentials for a CA ITCM service. Only the asset management agent and software delivery agent are supported. You can use this command directly on the console in an asset or software job sent to many computers. Beware, however, of embedding plain text passwords in a job.

savecreds, loadcreds

The caf savecreds command lets you store a set of credentials for different computers and services in an encrypted file. This file can be transmitted to many computers and applied using the caf loadcreds command. This file lets you specify different administrator passwords for different computers as each entry in the file is specific to a computer. The caf loadcreds command applies only those entries for the local computer it is run on.

Run CA ITCM Services as Administrator

On Windows, a CAF feature lets you run a CA ITCM plug-in or service under specific user credentials. However, only users in the administrators group are supported; other types of users will not work.

To run a plug-in or service, for example, the sdagent service

1. Open a command prompt window.
2. Set the credentials for sdagent using the command:
   `caf setcreds sdagent user administrator password` *xxx*
3. Test that it works by issuing the following command:
   `caf start sdagent`

   The sdagent program (sd_jexec.exe) should appear in the Task Manager running as administrator.

How to Introduce Your Own X.509 Certificates into the Install Image

CA IT Client Manager uses X.509 certificates for authentication between its client processes and any service that requires authentication. For example, X.509 is used when the software delivery component connects to its parent scalability server

A CA IT Client Manager installation comes with a set of default standard certificates signed by a CA root certificate. The public root certificate is installed on every node within the enterprise.

We strongly recommend that each enterprise create and deploy its own root certificate, Basic Host Identity (BHI) certificates, and application-specific certificates.

For details on creating end user-specific certificates see CA IT Client Manager Security Features (see page 375).

To create new certificates using the cacertutil tool, you must install at least one component (Explorer, Asset Management agent, and so on). The cacertutil tool is in the bin folder under the DSM installation directory.

After having created your own specific certificates, replace the default standard certificates inside the install image with your new certificates before starting any installation or deployment of DSM components.

After replacing the certificates within the install image, installation or deployment can start as usual.

Default Certificates for Windows

The default certificates for Windows are in the following folders. Each of these folders has a subfolder structure, Program Files\CA\DSM\bin that contains the relevant certificates.

- AgentBHW
- AgentAM
- AgentRC
- AgentSD
- AllAgents
- Server
- Manager
- Explorer

Default Certificates for Linux and UNIX

The default certificates for Linux and UNIX are in subdirectories called certificates under the following package directories:

- agent
- am_agent
- basichwinv
- rc_agent (Linux only)
- sd_agent
- server (Linux only)

Customize X.509 Certificates Using cfcert.ini

The cfcert.ini file controls the certificates installed by CA ITCM. The cfcert.ini file contains several sections that correspond to each application group in the installation. The default cfcert.ini file is as follows:

```
[CAF]
files=itrm_dsm_r11_root.der,basic_id.p12

[Configuration]
files=ccsm.p12

[Manager]
files=itrm_dsm_r11_cmdir_eng.p12

[Registration]
files=registration.p12

[USD.Agent]
files=itrm_dsm_r11_sd_catalog.p12

[USD.Manager]
files=itrm_dsm_r11_agent_mover.p12,itrm_dsm_r11_sd_catalog.p12



[Files]
itrm_dsm_r11_root.der=cacertutil import -i:itrm_dsm_r11_root.der -it:x509v3
basic_id.p12=cacertutil import -i:basic_id.p12
-ip:enc:uAa8VNL4DKZlUUtFk5INPnr2RCLGb4h0 -h -t:dsmcommon
ccsm.p12=cacertutil import -i:ccsm.p12 -t:csm
-ip:enc:IWhun2x3ys7y1FM8Byk2LMs56Rr8KmXQ
itrm_dsm_r11_cmdir_eng.p12=cacertutil import -i:itrm_dsm_r11_cmdir_eng.p12
-ip:enc:gYuzGzNcIYzWjHA6w542pW68E8FobJhv -t:dsm_cmdir_eng
itrm_dsm_r11_sd_catalog.p12=cacertutil import -i:itrm_dsm_r11_sd_catalog.p12
-ip:enc:wdyZd4DXpx6j5otwKY0jSaOOVLLi0txQruDVOslGOlNIMZw96c85Cw -t:dsmsdcat
itrm_dsm_r11_agent_mover.p12=cacertutil import -i:itrm_dsm_r11_agent_mover.p12
-ip:enc:sytOQtZteLopAt1CX0jIJUJcpqBWrb7G7VegY7F7udogc1c5kLIylw -t:dsmagtmv
registration.p12=cacertutil import -i:registration.p12
-ip:enc:z5jLhmvfkaAF4DLMDp3TWuC7nG8yh3dfvmN668thfrU -t:dsm_csvr_reg
babld.p12=cacertutil import -i:babld.p12 -ip:enc:TrdWglmuNCdeOAfj2j3vMwywVbGnlIvX
-t:babld_server
dsmpwchgent.p12=cacertutil import -i:dsmpwchgent.p12
-ip:enc:QWF8vknD5aZsU1j5RLzgt1NQgF5DcXj4v1vS4ewDzOA -t:ent_access
dsmpwchgdom.p12=cacertutil import -i:dsmpwchgdom.p12
-ip:enc:sqb9qO2SGjbYqzIvwM7HEbx0M6UJk8Dc82EvUoDeJmE -t:dom_access
dsmpwchgrep.p12=cacertutil import -i:dsmpwchgrep.p12
-ip:enc:x901eho57IZ19zg6g97rQetHjA1461na7nhBmJl7mcc -t:rep_access
```

```
[Tags]
dsmcommon=x509cert://DSM r11/CN=Generic Host Identity,O=Computer Associates,C=US
csm=x509cert://dsm r11/CN=Configuration and State Management,O=Computer
Associates,C=US
dsm_cmdir_eng=x509cert://dsm r11/cn=dsm directory synchronisation,o=computer
associates,c=us
dsmsdcat=x509cert://dsm r11/CN=DSM r11 Software Delivery Catalog,O=Computer
Associates,C=US
dsmagtmv=x509cert://dsm r11/CN=DSM r11 Agent Mover,O=Computer Associates,C=US
dsm_csvr_reg=x509cert://dsm r11/CN=DSM Common Server Registration,O=Computer
Associates,C=US
babld_server=x509cert://dsm r11/cn=babld server,o=computer associates,c=us
ent_access=x509cert://dsm r11/CN=Enterprise Access,O=Computer Associates,C=US
dom_access=x509cert://dsm r11/CN=Domain Access,O=Computer Associates,C=US
rep_access=x509cert://dsm r11/CN=Reporter Access,O=Computer Associates,C=US
```

Each section of the cfcert.ini file declares the certificates that are required to be installed by the associated installer. The installer reads the “files=” entry from its associated section in cfcert.ini and installs each certificate listed in turn by using the command located in the [Files] section of the cfcert.ini file.

For example, the common application framework (CAF) installer finds that it needs to install the certificates itrm_r11_dsm_root.der and basic_id.p12. In the [Files] section, the CAF installer finds the cacertutil commands associated to these certificates in the first two lines, and executes these commands.

The [Tags] section allows you to create new certificates that do not use the standard certificate URIs. When installing a DSM manager node the installation components will read this section and set up security profiles for the named URIs. The tags and URIs listed previously are the CA ITCM defaults and will be used if not present in the cfcert.ini file.

By convention, the file names listed in the “files=” entry in each section of cfcert.ini are the same as the names of the underlying certificate file. This allows for easier maintenance of the cfcert.ini initialization file.

To replace the default certificates with your own, change each individual section and the [Files] section to reflect the new certificate names and passwords.

Important! Ensure that the new certificates are imported using the correct tag names. The tags are specified by the -t: switch. For more information and a list of available certificates, see Installation of Application-Specific Certificates (see page 383) and Current Certificates (see page 531).

Modify or Repair an Installation

To modify or repair an existing installation of CA ITCM, run the setup program. The available options are as follows:

Modify

Allows you to add or remove components.

Note: Be aware that you always specify the end state of the modify process. If you have a manager installed and want to add a DSM Explorer, make sure you have checked manager and DSM Explorer because this would be your desired end state.

Repair

Allows you to repair an existing installation. The Repair function checks files, registry keys, and shortcuts of the original install and reinstalls them if they are deleted or corrupted.

Modify an Installation

Modifying an existing installation of CA ITCM means to install new features or remove currently installed features.

To modify an installation

1. Run the setup program and select the Install CA ITCM option.

   The Installer detects whether an installation already exists and displays the Select install option dialog.

2. Select Modify.

   The Select Product Functionality dialog appears.

3. Make your selections and click Next.

   The Select Features dialog appears, displaying all available features. The installed features are already selected.

4. Select the features to install and unselect features to remove.

5. Follow the instructions in the installation wizard.

After the operation has successfully finished, you can restart the CAF service immediately or specify to restart the service later.

How to Change the Manager Role

Changing the role of a DSM manager from domain manager to enterprise manager or from enterprise manager to domain manager cannot be done by using the Modify function. To change from one manager role to the other, proceed as follows:

- Use the Modify function to uninstall the manager.
- Uninstall the database provider and the Management Database (MDB).

  Important! Before uninstalling the database provider, see Uninstallation of Manager and Management Database (see page 206).
- Use the Modify function to install the manager with its new role.

Repair an Installation

Repairing an existing installation of CA ITCM fixes missing or corrupt files, shortcuts, and registry entries of the previous setup.

To repair an installation

1. Run the setup program and select the Install CA ITCM option.

   The Installer detects whether an installation already exists and displays the Select install option dialog.
2. Select Repair.
3. Follow the instructions in the installation wizard.

The Repair function does not replace files or any settings that were created or made during the use of CA ITCM.

Upgrade an Installation

To upgrade an installation means to reinstall features or components to higher version or build numbers without uninstalling the older ones. All current settings are kept and the database is not overwritten.

You can perform an upgrade using one of the following alternatives:

Using the installation wizard

Run the setup program and it will inform you that a previous version has been detected and an upgrade will be done.

Using the DSM Explorer and distributing packages for upgrade

Within the DSM Explorer the preregistered software delivery packages can be used to distribute the components. Software delivery functionality will automatically run an upgrade if an older version exists on the target computer.

Using the deployment wizard

Within the DSM Explorer, the Infrastructure Deployment wizard can be used to distribute and install packages to the target computers. For target computers where a previous version is already installed, it is necessary to require an upgrade from within the Deployment: Agent Configuration wizard page. In the input field, Additional Windows install options, the following settings must be entered to request an upgrade on the target computer:

```
REINSTALL=ALL REINSTALLMODE=vomus
```

Calling the MSI Packages Directly

When using the MSI packages directly, you must add the following parameters to the command line:

```
REINSTALL=ALL, REINSTALLMODE=vomus
```

Example

```
msiexec.exe /i"N:\DSM_12_0_1234_1_DVD\WindowsProductFiles_x86\AgentSD\agtsd.msi"

REINSTALL=ALL
REINSTALLMODE=vomus /l*v "%temp%\ITRMupdateSDagent.log"
```

Uninstallation of CA ITCM

The methods to uninstall CA ITCM or parts of the CA ITCM installation are provided in the following sections:

- Uninstallation of CA ITCM on Windows (see page 223)
- Uninstallation of CA ITCM on Linux and UNIX (see page 225)

Uninstallation of CA ITCM on Windows

To uninstall CA ITCM or parts of it, you can use *one* of the following options:

- Use the Add/Remove Programs function from the Windows Control Panel.

  This function lets you remove the complete CA ITCM or single components of it. Select the appropriate item from the list of installed software and click the Change/Remove button.

- Use the CA ITCM installation wizard.

  Execute setup.exe. The installation wizard starts and provides the installation wizard that guides you through an interactive uninstall. Choose Install CA ITCM. One of the subsequent dialog boxes offers the Remove, Modify, and Repair options.

  Selecting the Remove option removes the complete CA ITCM installation from the system where setup.exe was executed.

  Selecting the Modify option provides a list of all components and features managed by the Installer. Features currently installed on the local system are checked. Clear the ticks (the hook disappears) from those components or features you want to uninstall. The specified features will be uninstalled when you finish the dialog, but the CA ITCM installation is not removed.

- Execute msiexec /x with an appropriate product code at the command line.

  The component to remove is specified by its product code (see page 223). Using the option /qn in the msiexec command you can specify uninstallation in silent mode.

On Windows, the uninstallation using the setup program uninstalls all CA ITCM products and language packs. Uninstalling single MSI packages using Add/Remove Programs from the Windows Control Panel or using the msiexec command line tool does not uninstall any other MSI package.

Note: After uninstalling on Windows, some files, folders, and registry keys will remain. Remove the DSM directory manually after the uninstallation is complete.

Product Codes in CA ITCM

The installable components of CA ITCM are identified by an individual product code, as follows:

Basic Inventory Agent (ENU and multi-language):

{501C99B9–1644–4FC2–833B–E675572F8929}

Asset Management Agent (ENU and multi-language):

{624FA386-3A39-4EBF-9CB9-C2B484D78B29}

Data Transport Service Agent (ENU and multi-language):

{C0C44BF2–E5E0–4C02–B9D3–33C691F060EA}

Remote Control Agent (ENU and multi-language):

{84288555–A79E–4ABD–BA53–219C4D2CA20B}

Software Delivery Agent (ENU and multi-language):

{62ADA55C–1B98–431F–8618–CDF3CE4CFEEC}

Agent language package DEU:

{6B511A0E-4D3C-4128-91BE-77740420FD36}

Agent language package FRA:

{9DA41BF7-B1B1-46FD-9525-DEDCCACFE816}

Agent language package JPN:

{A4DA5EED-B13B-4A5E-A8A1-748DE46A2607}

Agent language package ESN:

{94163038-B65E-45BE-A70C-DC319C43CFF2}

Agent language package KOR:

{2C300042-2857-4E6B-BC05-920CA9953D2C}

Agent language package CHS:

{2D3B15F5-BBA3-4D9E-B7AB-DC2A8BD6EAD8}

Documentation:

{A56A74D1–E994–4447–A2C7–678C62457FA5}

Explorer:

{42C0EC64–A6E7–4FBD–A5B6–1A6AD94A2D87}

Manager:

{E981CCC3–7C44–4D04–BD38–C7A501469B37}

MasterSetup:

{C163EC47–55B6–4B06–9D03–2A720548BE86}

Scalability Server:

{9654079C-BA1E-4628-8403-C7272FF1BD3E}

DMPrimer:

{A312C331-2E7A-42E1-9F31-902920C402EE}

Example for Uninstallation Using msiexec and Product Code

The following example removes the asset management agent in silent mode and writes removal information into a log file, rmvamagt.log, in the logs folder on drive c.

```
msiexec /x {A302890B-3180-455B-A958-6DDFAE9F4B00} /l*v "c:\logs\rmvamagt.log" /qn
```

Uninstallation of CA ITCM on Linux and UNIX

You can uninstall CA ITCM or parts of it on Linux or UNIX using one of the following options:

./setup.sh

Run setup.sh from the installation DVD and select Uninstall in the setup dialog.

lsm -e *prodname* [-s]

Run this lsm command version from the CA ITCM command line. In the lsm command the product or component is specified by *prodname*. The option -s specifies unattended (silent) uninstallation mode.

The following example uninstalls the complete CA ITCM in unattended (silent) mode:

```
lsm -e ca-dsm -s
```

The following example uninstalls the DMPrimer:

```
lsm -e ca-dsm-dmprimer-standalone
```

The product or component names that can be used as values for the variable *prodname* in the Linux/UNIX Installer (lsm) command are shown in the following table:

Product/Component Name	Description
ca-dsm	CA IT Client Manager
ca-dsm-dmprimer-standalone	DMPrimer (only installed when using the infrastructure deployment component of CA ITCM)
ca-dsm-SMPackager	Software Packager for Linux and UNIX

General Notes on Agent Uninstallation

The uninstallation of the agent base package for any agent also uninstalls any associated language packages.

The uninstallation of a language package does not affect the agent base package, so language packages can be removed at any time you want.

When a stand-alone language package is uninstalled and the current language in the configuration store (comstore) is set to that language, then the value of the configuration parameter, itrm/common/localization/language, in the comstore is changed to enu. Otherwise, the parameter value is not altered.

A language package deregisters itself with Software Delivery and Infrastructure Deployment on uninstallation.

Using Software Delivery to Uninstall Windows Agent DSM Packages

DSM packages can be split into two classes: base packages and custom packages. Custom packages "contain" base packages and base packages are the "atoms." Base packages are registered when installed or discovered and are listed as "installed software." When a custom package is delivered and installed using Software Delivery, an installation record is created for the custom package. However, this custom package installation record is not created for a manual installation or installation using infrastructure deployment.

When using Software Delivery to uninstall DSM packages, only the base packages should be uninstalled. The order in which the base packages should be uninstalled is important. First, uninstall the agent language packages, then the DCS add-on, then Asset Management and/or Remote Control. Obviously, the software delivery agent needs to be uninstalled last. One way of implementing this would be to create an software delivery uninstall job container with a job for each stage. When the base packages have been uninstalled, the installation records for the custom packages should be removed using DSM Explorer.

Note that plug-ins like Secure Socket Adapter and DMPrimer are not removed. To remove these plug-ins, uninstall any remaining DSM components on the target computer manually using Add/Remove programs.

Chapter 5: Infrastructure Deployment

The following introduces the infrastructure deployment phases, the deployment management concepts, and the ways to deploy interactively, through the command line, or triggered by continuous discovery. Additionally, some special deployment aspects, prerequisites, and tools are considered.

This section contains the following topics:

Infrastructure Deployment Introduction

Deployment Management (DM) is the infrastructure deployment solution within CA IT Client Manager. DM simplifies the infrastructure deployment of software components to a large number of target computers within a heterogeneous enterprise and eliminates the need for an administrator to manually log on, transfer installation images, run the installation process, and monitor the results of the installation on each target computer in turn.

DM provides the following benefits:

- Automatic infrastructure deployment to a range of target operating environments.
- Synchronous deployment, that is, initiating a deployment concludes with the deployed component installed and running without further human interaction. Where this is not possible, asynchronous deployment is offered, which may require a user to log on or reboot before installation is completed.
- Enhanced logging and reporting functionality. DM monitors the progress of a deployment and displays appropriate status information.
- Security features that meet the needs of current enterprise installations. Suitable authentication and encryption technologies are used to ensure that no sensitive data is accessible to third parties during network transmission or in persistent storage.
- A deployment manager, which will separate the bulk of the deployment workload from the deployment client interfaces. Multiple deployment managers can deploy to a single target computer, if necessary.
- Automatic deployment to newly discovered systems. The administrator can define rules to deploy certain software to certain systems whenever a computer appears in the network for the first time.

Typical CA ITCM Infrastructure Deployment Phases

Infrastructure deployment is comprised of the following main phases:

- Interactive manager installation at the headquarters
- Defining scalability servers for this manager and deploying the scalability servers, using the deployment wizard
- Deploying agents connected to the scalability servers, using the deployment wizard
- Automatic deployment to newly discovered systems

Deployment Management Concepts

When a deployment operation is requested, the manager first tries to send down a relatively small "primer" package to the target computer.

The primer package is pushed out using one of a variety of methods, depending on the target operating system and what software is installed.

It is not always possible to remotely push out the primer, for example, when the network security settings prevent it. However, in such cases, you can manually install the primer on the target computers.

Once the primer is installed, it is used to transfer the actual deployment package data to the target computer and run the installation. All subsequent deployments to the same target computer can use the existing primer installation.

The deployment manager controls all the deployment operations and handles job status.

The deployment clients (deployment wizard and dmsweep command line interface) use an API to communicate with the deployment manager. They are installed along with the DSM Explorer and can therefore be run on a computer other than the manager, if required.

To reduce network usage when deploying large numbers of agents, you can “stage” deployment packages at scalability servers.

Protocols for Transferring Packages Using Scalability Server

DMDeploy uses the following protocols to transfer packages to target computers when you deploy using a scalability server:

Windows Network Share

Uses this mechanism if the scalability server and the target computer are on Windows.

SSH/SFTP

Uses this mechanism if either the scalability server or the target machine is on Linux or Unix.

Telnet/FTP

Uses this mechanism if either the scalability server or the target machine is on Linux or Unix.

For more information about these transfer mechanisms, see Prerequisites for Automatically Deploying CA ITCM Infrastructure (see page 245).

Using Scalability Servers in Context of Infrastructure Deployment

To reduce network usage when deploying large numbers of agents, you can “stage” deployment packages at scalability servers. To make deployment payload packages available at a scalability server, deploy the payload to the scalability server but specify the “stage package at scalability server” option. To subsequently deploy packages stored at the scalability server, check the “Transfer Packages from Scalability Server” option when selecting the deployment payload.

Using a scalability server with infrastructure deployment has implications for network configuration. Typically, a scalability server would be used to deploy agents to target computers that are located "close" on the enterprise network, that is, those that use relatively fast network speed between the scalability server and agent computers.

There are many administration tasks to perform and remember when using scalability servers with infrastructure deployment, including the following:

- To deploy to Windows target computers using a Linux scalability server with Telnet/FTP transfer mechanism, you must enable Telnet on Windows target computers. On computers running Windows 2003, Windows XP, or newer operating systems, the Telnet service can be enabled and started using the Administration Tools, Services dialog from the Windows Control Panel.

- To deploy to Linux or UNIX target computers using a scalability server with Telnet/FTP transfer mechanism, an FTP server must be enabled on the scalability server. Also, the target computer needs a Telnet server running because the manager uses Telnet to the target computer and FTP to the scalability server to pull the package across.

  In addition to the above, if your scalability server is running on a Windows machine, you will need to perform the following configuration task on the scalability server to set up an alternative FTP site for use by Infrastructure Deployment. A separate FTP site is required to avoid security issues with other FTP areas when sharing the staging location where CA ITCM agent packages will be stored:

  - Open the Control Panel, Administration Tools and select Internet Information Services (IIS) manager.
  - Right-click the FTP Sites node and select New, FTP Site to run the FTP Site Creation Wizard.
  - Run the wizard and enter ITCM FTP Site as the description for the new site. Select the default values given in the wizard until you get to the FTP Site Home Directory wizard page. On this page you will have to specify the DMPrimer install location directory, as this is where ITCM Infrastructure Deployment agent packages will be staged. If you already have a DMPrimer installed, then use the Browse button to locate the directory. By default the DMPrimer will be installed in Program Files\CA\DSM\DMPrimer. Having selected the FTP Site directory, continue through the wizard, selecting the default options, and click the Finish button.

  One point to note is that when using the Windows Scalability Server to deploy to Linux targets, the CA ITCM FTP Site must be started. You should ensure that any other FTP Site, such as the Default FTP Site, has been stopped; otherwise, the deployment will fail.

- When using FTP on a scalability server, you must be careful when specifying the user credentials needed to connect to it. When staging a package to the scalability server/FTP server, you must specify credentials of a user who has privilege to write to the scalability server. When deploying a package from a scalability server/FTP server, the anonymous user is typically used to access the packages.

- If deployment through Telnet/FTP is required, then FTP server details are provided during the manager installation and the DMPrimer packages are uploaded to the specified server. Normally, the FTP server is located on the same computer as a scalability server.

  If more than one FTP server is to be used against a single Infrastructure Deployment manager, for instance, if there are multiple scalability servers with an FTP server running on each computer, then you must take some manual configuration steps before deployment will use an alternative FTP server that was not configured at installation time.

  To change the FTP details, you must run the 'dmdeploy ftpinfo' command with the details of the new FTP server, and copy the primer packages and dmkeydat.cer file to the corresponding location on the FTP server. The deployment manager will then use this FTP server for deployment through Telnet/FTP. These steps are covered in the Changing FTP Server Details for Use with Infrastructure Deployment (see page 248) section.

- If you are using a scalability server on Windows for infrastructure deployment, note that Windows has a limit on simultaneous connections. Some jobs may fail when the connection limit is reached. In this case, you receive a message *Failed to obtain package at this time. Connection limit on scalability server reached. Please retry.* Use the configuration parameter 'Deployment Thread Limit' to control the number of concurrent deployments run by the Infrastructure Deployment manager. The default value of the configuration parameter is 10 and can be changed if you deploy through a scalability server running on Windows.
- In a pure IPv6 environment deployment fails, if the Telnet versions used do not support the IPv6 protocol.
- In a pure IPv6 environment deployment to Linux or UNIX target computers fails, if the FTP versions used do not support the IPv6 protocol.

More information:

Protocols for Transferring Packages Using Scalability Server (see page 229)

Auditing of Scalability Servers with Infrastructure Deployment Content

Infrastructure Deployment lets users audit the scalability servers in their network that contain deployment content and get a list of deployment packages that exist on each scalability server.

The list of infrastructure deployment packages available on a scalability server is displayed when the scalability server is selected during navigation through the deployment wizard. Scalability Server contents can also be displayed using the "dmsweep sspack" command.

Deployment Management Process

When executing Deployment Management (DM), perform the following primary steps of the deployment process:

1. From the administrator computer, the infrastructure deployment client component (deployment wizard or dmsweep command) issues a request to the DM manager (DMDeploy) to install an agent on a list of one or more target computers. The deployment manager may be running on a computer that is remote from the client. The list of targets can consist of explicit machine names or IPv4 addresses, or may be obtained from a "container" source such as a Windows domain, an LDAP directory, or a CA ITCM query.

   For deployment to succeed to each target computer, it is important to ensure that its name, whether entered explicitly or obtained from a container, is suitable for resolving to the address of the target as seen on the deployment manager computer. If, for example, the list of targets retrieved from a directory is not fully qualified with network domain names, deployment may not be able to proceed in certain network configurations.

2. A check is made to see if the DMPrimer is already installed on the target computer. If not, DMPrimer will be installed first on the target computer. The DM manager tries to deliver the DMPrimer installation package. The delivery method used depends on the target operating environment and the security that has been enabled on it. After the DMPrimer image is copied across to the target computer, its installation is initiated.

   As some operating systems do not have a method for remote invocation of the DMPrimer installation, you may have to establish the installer to be installed on a significant operating system event, such as a reboot. This is termed an asynchronous installation, because the message to indicate completion of the installation is received asynchronously at an unspecified future time. Alternatively, the DMPrimer installation can be performed manually.

3. The DMPrimer installer installs itself and the CA Message Queuing (CAM) component on the target computer. During installation, the FIPS mode of the DMPrimer on the target computer depends on the FIPS mode of the manager. The manager passes the FIPS mode as an installation parameter. This parameter is also updated in the dmprimer.cfg file, which is part of the DMprimer installation.

   However, on start, DMPrimer reads the FIPS mode from the agent configuration policy on the target computer. If successful, the primer updates the dmprimer.cfg file with the FIPS mode of the agent and initializes in that mode. If there are no agents installed on the target, the DMPrimer initializes in the mode specified in the dmprimer.cfg file.

   Note: On most operating systems, the DMPrimer installation needs to run with elevated privileges.

4. Once the DMPrimer is installed and DMDeploy has received the "installation complete" signal from the target computer, package deployment can be initiated. A DMDeploy manager that has previously installed a DMPrimer and has authenticated with it can deploy packages without needing to resupply user names or passwords. This is done through authentication using public and private keys. You can force the deployment manager to retransfer and install the DMPrimer even if a version is already present. To do so, set the "AlwaysDeployPrimer" configuration policy using the DSM Explorer.

For details on using the deployment manager through the DSM Explorer, see the online help for Deployment wizard.

Flexible Specification of Deployment Targets

To provide flexibility when specifying deployment targets, a target credentials file has been introduced. With the target credentials file, an administrator can create and maintain lists of individual target systems or groups of target systems along with their connection credentials.

The target credentials file allows users to plan their deployments "offline" before initiating the actual deployment jobs. You can specify deployment to different "areas" of a network by creating families of credential files, for example, files relating to different company departments.

You can use the target credentials file with both the dmsweep command (using the /targetcred option) and the Infrastructure Deployment wizard.

Pass Options to the DMPrimer Installation

You can specify options for the DMPrimer installation. This lets you, for example, install DMPrimer into nonstandard locations. This is a common requirement because all subsequent installations of CA ITCM components on a given computer must use the location settings first set by the installation of DMPrimer. Therefore, if you need to use nondefault installation locations for the CA ITCM software, you must set the DMPrimer installation location using the options described below when you initially deploy to a particular target computer.

You can enter the install options through both the dmsweep command line (using the /primerargs option) and the deployment wizard (using the "Show Advanced Options" area of the Agent Configuration page).

To install the DMPrimer into a nonstandard location, you must pass the following arguments to the DMPrimer installation:

- For deployment to Windows target computers:

  `CA=x:\NewProductPath`

  `CASHCOMP=x:\NewSharedArea`

For deployment to Linux or UNIX target computers:

`/RCA_ITRM_BASEDIR=/opt/NewProductPath /RCASHCOMP=/opt/NewSharedArea`

By default, DMPrimer installations use the same FIPS mode as the manager. You can override the default value using the following parameter:

Windows target computers:

```
FIPS_MODE=1 //(FIPS-preferred)
FIPS_MODE=2 //(FIPS-only)
```

Linux or UNIX target computers:

```
/RITCM_FIPS_MODE=1 //(FIPS-preferred)
/RITCM_FIPS_MODE=2 //(FIPS-only)
```

Note on Adding Windows Install Options

When you are passing additional Windows install options containing one or more spaces to a deployment job, using the Agent Configuration page of the Infrastructure Deployment wizard, the parameter values must be quoted properly. For each additional Windows install option, the value must be enclosed in double quotes, for example:

```
CA="C:\Program Files\mydir" CASHCOMP="C:\Program Files\mydir\sharedComps"
```

On the command line, using dmsweep, the individual parameters must be separated by commas and protected with double quotes, as in the following example:

```
/pri "CA=\"C:\Program Files\CA\test\" CASHCOMP=\"C:\Program Files\CA\test\""
```

Notes on Infrastructure Deployment Using IPv6 Addresses

If you are going to deploy CA IT Client Manager infrastructure using IPv6, you should peruse the following notes:

- In order to use Infrastructure Deployment in an IPv6 environment, the following conditions must be met first:

  1. The following registry key needs to be set to 1 on the DSM manager:

     HKLM\System\CurrentControlSet\Services\smb\Parameters\IPv6EnableOutboundGlobal (REG_DWORD)

  2. Apply two hotfix updates on the Scalability Server:

     - http://support.microsoft.com/kb/947369/en-us
     - http://support.microsoft.com/kb/950092/en-us

  3. The host name of the target machine must resolve to a global IPv6 address.

     Also ensure that a reverse lookup of the IPv6 address resolves to the same host name.

  4. The Infrastructure Deployment configuration policy option, Use host names, must be set to True.

  Note: If you intend using Infrastructure Deployment to deploy software via a scalability server to any Windows 2003 machine in an IPv6 environment, then you will also need to carry out Steps 1–3 above on the intended Windows 2003 target.

  If these conditions are not met in an IPv6 only network, then the DMPrimer package must be manually installed. For more information, see the Manual Installation of the Infrastructure Deployment Primer Software (see page 237) section.

- Both Infrastructure Deployment and Continuous Discovery support deployment only to IPv4 address ranges.

Manual Installation of the Infrastructure Deployment Primer Software

Even if automatic deployment to target computers is not possible for any reason, you can still deploy infrastructure software if you manually install the primer software on the target computer. This can be done by physically installing the primer package or running the installation through login scripts.

And installing the primer software itself, install a security key that is generated by the deployment manager you want to use to deploy infrastructure to your target computers.

The DMprimer installer provides you an option to specify the FIPS mode for the primer. If you want to modify the FIPS mode after installation, update the FIPS_MODE setting in the dmprimer.cfg file. However, on start, DMPrimer reads the FIPS mode from the agent configuration policy on the target computer. If successful, the primer updates the dmprimer.cfg file with the FIPS mode of the agent and initializes in that mode. If there are no agents installed on the target, the DMPrimer initializes in the mode specified in the dmprimer.cfg file.

Deployment Primer Installation on Windows

The installation of the deployment primer on a target computer running Windows requires the following actions:

- Make the CA ITCM installation media (DVD) available on the target computer, or manually copy the primer setup file to the target computer.

  The primer setup file is stored on the installation media as follows:
  `\WindowsProductFiles_x86\DMPrimer\dmsetup.exe`
- Run dmsetup.exe on the target computer to install the primer.

Deployment Primer Installation on Linux or UNIX

The installation of the deployment primer on a Linux or UNIX target computer requires the following actions:

- Make the CA ITCM installation media (DVD) available on the target computer, or manually copy the primer installation image to the target computer.

  The primer installation image is stored on the installation media in the following directory:
  `/LinuxProductFiles_x86/dmprimer`
- Change to the directory containing the primer installation image on the target computer and run the following installation command to install the primer:
  `# sh installdmp`

Provide the Deployment Management Certificate to a Primer Installation

The deployment manager generates a certificate that needs to be transferred to the target computer before the primer on the target computer will accept deployment packages. The deployment certificate file is called dmkeydat.cer.

The location of the certificate is configurable at installation time. You may configure a different file location if you want to store the certificate in a more secure area or in a location shared between two managers providing a failover solution. In the latter case, sharing the certificate enables deployment managers to communicate with DMPrimer components delivered from either manager without the need to resupply authentication credentials.

On Windows, the deployment certificate is stored in the following directory:
`\Program Files\CA\DSM\DMDeploy`

The certificate must be copied to the primer installation folder on the target computer, which by default is as follows:
`\Program Files\CA\DSM\DMPrimer`

On Linux and UNIX, the deployment certificate is stored in the following directory:
`/opt/CA/DSM/DMDeploy`

The certificate must be copied to the primer installation folder on the target computer, which by default is as follows:
`/opt/CA/DSM/dmprimer/bin`

Deployment of Agent Packages

To reduce the amount of data transferred through the network during deployment of CA ITCM agents, CA ITCM provides agent packages that support English language only and packages that contain agents for all supported languages (multi-language agent packages).

On the product installation DVD the different agent packages are located under the product files folders, for example, WindowsProductFiles_x86.

The English-only packages are marked with the suffix _ENU. The multi-language agent packages have no specific suffix.

In the Software Package Library, ENU packages are suffixed with “(English only Edition)”; multi-language agent packages do not have a special identifier.

In the Infrastructure Deployment wizard, ENU packages are marked with “(English only Edition) ENU”; multi-language agent packages have the suffix NLS(ENU,DEU,FRA,JPN).

During installation, you choose if you want to get the English-only packages or the multi-language agent packages or both into the Software Delivery Library and the infrastructure deployment package folder.

If you select just one kind of package, for example, English language agent packages and at a later point decide to add the multi-language agent packages as well, you must run the dsmPush command to push the agent package of your choice.

Multi-language agent deployments to target computers do not have a fixed language specified. Instead, the installation is carried out in the system language of the target computer. To specify an explicit installation language when deploying to target computers, enter the DSM_LANGUAGE option in the "Please enter any additional... install options" field within the Infrastructure Deployment wizard. The option must be specified as follows (*lang* specifies the installation language on the target computer and is one of the strings enu, deu, fra, jpn, chs, esn, or kor):

DSM_LANGUAGE=*lang* (on Windows)

/RDSM_LANGUAGE=*lang* (on Linux and UNIX)

If you do not provide a language setting, the system default locale is used, provided such a language package is available. If the system default locale is not one of the supported languages, the installer falls back to enu (English (U.S.)).

You may also provide the language parameter when deploying packages to target computers using the dmsweep command line. Specify the language to be used for the CA ITCM operation using the pparams option.

Example: Deploy a German Windows Agent Using the Command Line

In this example, the German Windows agent is package number 3.

```
dmsweep deploy /ip targetcomputer /pn 3 /pparams servername,/DSM_LANGUAGE=deu
```

Note: For more information about additional install options (also called properties), like DSM_LANGUAGE, and their values, see the sections about installation of CA ITCM using the command line in the "Installation of CA ITCM" chapter.

By default, all agent packages are installed in the same FIPS mode as the manager. You can override the default value using the following parameter:

Windows target computers:

```
FIPS_MODE=1 //(FIPS-preferred)
FIPS_MODE=2 //(FIPS-only)
```

Linux or UNIX target computers:

```
/RITCM_FIPS_MODE=1 //(FIPS-preferred)
/RITCM_FIPS_MODE=2 //(FIPS-only)
```

Deployment to Windows Vista and Windows 2008 Computers

If the firewall of a target computer running the Windows Vista or Windows 2008 operating system is "off" and deployment to the computer fails, create or set the following registry variable so that it has a value of 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
        System\LocalAccountTokenFilterPolicy
```

This is required because User Account Control (UAC) in Windows Vista or Windows 2008 does not automatically grant administrative rights to local users. This occurs even though the local users are members of the Administrators group.

Note: Setting this value will result in remote UAC access token filtering being disabled.

Setting this value is worth doing, if the user has a local administrator account on the computer running Windows Vista or Windows 2008. Domain administrators will not benefit from this change.

If the firewall of a target computer running Windows Vista or Windows 2008 is "on" (enabled), the following ports should be opened in addition to file sharing ports, to enable deployment to that computer:

- UDP ports:

4104	CAM
137, 138	File and printer sharing, and so on

- TCP Ports:

135	dmdeploy
139, 445	File and printer sharing, and so on

If deployment still fails, the following Outbound Rules in the firewall for Windows Vista or Windows 2008 should be fully enabled:

- Remote Assistance
- Network Discovery
- File and Printer Sharing
- Core Networking

If after opening the ports and enabling the Outbound Rules, the deployment scan still returns "No Response", consider setting the "Do not ping target during scan" configuration option to True. You can find this option in the configuration policy in the Manager\Infrastructure Deployment section. This marks the target as "Machine Responding" during a scan and lets deployment continue. Although this does not guarantee that deployment will succeed, it is merely a method to bypass any problems that may occur with the initial contacting of the target computer.

Deployment Using the DSM Explorer

The Infrastructure Deployment wizard helps administrators deploy agents or scalability servers within their enterprise.

The wizard guides you step-by-step through the process of creating a deployment job. You can choose from two job types: Deploy Software to Target Computers and Stage Packages at Scalability Server. You select the package to deploy from a list and specify whether it should be deployed to a specific computer or all computers in a specific domain, within an IPv4 address range, or within a directory. The wizard then scans the target computers to find out if deployment is possible on all targets and if credentials are required for deployment.

The wizard provides you with on-screen descriptions for each step and a separate help system.

After the deployment job starts, you can monitor and control the job through the Deployment Job Status function in the Control Panel. For more information, see the Monitor and Control Agent Deployment Jobs section in the *DSM Explorer Help*.

Note: During the installation of agent plugin packages on non-global zone computers on Solaris, you may see the following status message in the Deployment Job Status pane: "SSH failed to install dmprimer." To resolve this problem, update the agent's IP address and name in the hosts file (/etc/hosts).

Deployment Using the Command Line

The dmsweep utility lets you automate deployment activities and interactively perform many of the same tasks as can be done in the DSM Explorer.

Authorization to install the DMPrimer agent through dmsweep, in Windows NT environments, is provided in Deployment Management as follows. The dmsweep utility connects to the deployment manager using standard security mechanisms. As the user of dmsweep, you must have been granted the ability to perform deployments as the manager by a system administrator (operating system-level privileged administrators are granted deployment privilege by default). You can specify target computer credentials using the /tu (user name) and /tp (password) arguments.

Deployment Triggered by Continuous Discovery

The feature to deploy software whenever new systems are discovered is based on the CA Common Services Continuous Discovery feature. The CA Common Services Distributed Intelligence Agent (DIA) is used to retrieve events each time a new system is detected. The Continuous Discovery feature is switched on after the user has created at least one policy to describe which package is supposed to be deployed to which target computer dependent on the IPv4 address and operating system of the machine. The policies can be defined in the Continuous Discovery Deployment Policy wizard, which is similar to the Infrastructure Deployment wizard.

The discovery process is as follows:

- A system connects to the network for the first time.
- The Continuous Discovery service detects the new hardware and, using its heuristics, classifies it and creates a managed object representing the system in the WorldView repository.
- In response to the new data arriving in the database, a trigger is executed that registers the event in a special (dedicated) event table.
- The CA ITCM discovery application that has subscribed for those events is notified.
- The discovery application checks the continuous discovery policies if the detected system is targeted to receive new software and calls the deployment interface that is similar to the way DMSweep works.

Note: For the Continuous Discovery feature, configure Microsoft SQL Server with the default port 1433 on the domain manager.

Deployment Packages

Deployment packages of the following types are provided:

- CA DSM Agent + Basic Inventory plugin
- CA DSM Agent + Asset Management plugin
- CA DSM Agent + Remote Control plugin
- CA DSM Agent + Software Delivery plugin
- CA DSM Agent + AM, RC, SD plugin(s)

  This package is a combined package that includes agent plug-ins for Basic Inventory, Asset Management, Remote Control, and Software Delivery.

  For Linux, this package additionally includes the CA Data Transport agent plug-in.
- CA DSM Scalability Server

  This package is a combined package that contains the scalability server and agent plug-ins for Basic Inventory, Asset Management, Remote Control, Software Delivery, and CA Data Transport.

  Note: When the CA DSM Scalability Server deployment package is deployed using DMDeploy, the scalability server plug-in and *all* agent plug-ins are installed. However, when this package is deployed using the software delivery functionality, only the scalability server plug-in and the Software Delivery and CA Data Transport agent plug-ins are installed.

  Note: For information about CA DSM Scalability Server Linux (Intel) deployment package, see Installation of Scalability Server on Linux (see page 138).
- To deploy device compliance scanner (DCS), the following deployment packages are provided:

  Windows

  - CA DSM Agent AM DCS plugin (English only Edition)
  - CA DSM Agent AM DCS plugin
- To deploy Remote Virtualization Inventory, the following deployment packages are provided:

  Windows

  - CA DSM Agent AM RVI plugin (English only Edition)
  - CA DSM Agent AM RVI plugin

  AIX

  - CA DSM Agent AM RVI plugin AIX(RS/6000) (ENU)

  HP-UX

  - CA DSM Agent AM RVI plugin HP-UX(800) (ENU)

Linux

- CA DSM Agent AM RVI plugin Linux(intel) (ENU)

Solaris Sparc

- CA DSM Agent AM RVI plugin Solaris-Sparc (ENU)

Note: No CA ITCM documentation is installed with deployed client packages.

The deployment packages are present on a manager computer only if the manager feature for deployment is installed on the local system (which is the default).

You can change the preset location for the deployment packages during the interview phase of the installation process.

Important! Although you can specify additional MSI command line properties for the Windows versions of the deployment packages, give special consideration to the Windows versions of the "CA DSM Agent + AM, RC, SD plugin(s)" and "CA DSM Scalability Server" packages. For these combined MSI packages, you must not specify package-specific MSI feature list properties such as ADDLOCAL; otherwise, the deployment of the package will fail. If you need to list specific features for a package, we recommended that you do this for the dedicated agent deployment package in question.

The dsmpush Tool

The dsmpush tool (script) lets you import or "push" installation packages from the installation DVD into the domain manager. The dsmpush tool is used to import packages suitable for use by either Infrastructure Deployment or software delivery functionality.

Normally, the packages are already pushed onto a manager computer during setup, but this push is optional. If you need to push the packages again, to add more packages, or to update the packages, you can use the dsmpush tool.

The dsmpush tool provides a check and a copy function. The check function validates and lists existing deployment packages in the manager. The copy function imports a set of packages for specified products and operating environments into the Infrastructure Deployment library on the local system or into the software delivery library.

With every run the dsmpush tool provides log information in the log file TRC_Inst_dsmPush.*ddmmyyyhhmmss*.log; *ddmmyyyhhmmss* is the time stamp of the particular log file.

For the description of the dsmpush check and copy functions and their parameters, see the *CLI Reference Guide*.

Prerequisites for Automatically Deploying CA ITCM Infrastructure

The Infrastructure Deployment component lets you remotely install agent and scalability server software to target computers that are not running CA ITCM software. This can only be done using the facilities offered by the underlying operating systems on source and target computers, and is subject to any restrictions imposed by an enterprise network configuration.

The initial step when deploying infrastructure software is to remotely install a small “primer” application, the DMPrimer, onto the target computer. This DMPrimer software is responsible for subsequent transfer of infrastructure software component installation images, and the invocation of their installation. When delivering the DMPrimer to the target computers, the deployment manager must supply user credentials that are valid on the target.

The DMPrimer is transferred to the target system using one of the following mechanisms. If the target computer's operating system is known to the deployment manager, an appropriate transfer mechanism is selected. If the target operating system cannot be determined, each of the following mechanisms is attempted in turn.

- **Opening a network share**

  The deployment manager tries to connect to a Windows network share on the target system. By default, the share name used is ADMIN$, however, this can be altered by means of the "defaultTargetShare" configuration policy. This mechanism is available only from deployment managers running on a Windows-based platform and will only succeed on some Windows targets. Windows variants such as Windows XP Home do not support this deployment mechanism.

- **Opening a network connection to the target computer using the SSH protocol, and transferring the primer installation package using SFTP**

  This mechanism works on any computer running an SSH server, however, it is mainly useful when targeting Linux or UNIX computers.

  Note: When deploying to Solaris systems, CA recommends that you use either SunSSH v1.1 (or higher) or the latest version of OpenSSH.See the following website for additional details about patches applicable for Solaris platforms and versions: http://opensolaris.org/os/community/security/projects/SSH.

  If you are running a firewall on the target computer, ensure that the SSH port (22) is enabled to permit connection from the deployment manager. You should also check that the SSH server on the target computer is configured to use an RSA key along with the 3DES cipher for encryption and the HMAC-SHA1 message authentication code (MAC). Most SSH servers will support this configuration by default, but if they do not then you should consult your SSH server documentation for instructions on how to add this.

  To successfully deploy to a UNIX or Linux agent, configure the /etc/ssh/sshd_config configuration file of your recent SSH implementation as follows:

  - Set "PasswordAuthentication" to Yes
  - Set "PermitRootLogin" to Yes
  - Verify that SFTP subsystem is enabled

  When deploying to some IBM AIX systems that are running both an IPv4 and IPv6 stack, using an IPv6 address, the target computer SSH server may be listening only on port 22 for IPv4. This would cause the deployment to fail. To correct this, edit the sshd_config configuration file and set the ListenAddress to "::".

  When deploying to Solaris 11, follow these steps:

  - Comment out the following:

    ```
    CONSOLE=/dev/console
    ```

  - Line in the following:

    ```
    /etc/default/login.
    ```

    ```
    vi /etc/default/login
    ```

    ```
    #CONSOLE=/dev/console
    ```

  - Remove the following from the root entry in /etc/user_attr:

    ```
    ;type=role
    ```

    or use the command:

    ```
    rolemod -K type=normal root
    ```

  - Restart the ssh Service

Note: If you want the SSH communication between the deployment manager and the target computer to be FIPS-compliant, you must verify that the SSH server running on the target is also using FIPS-compliant cryptographic module, apart from setting FIPS-only mode on the deployment manager.

- **Opening a network connection to the target computer using the Telnet protocol and transferring the primer installation using FTP**

  This mechanism is mainly useful when targeting UNIX systems that do not support SSH. Use of Telnet/FTP is becoming less widespread because of inherent security weaknesses in these protocols, and is being superseded by SSH/SFTP.

  When using this connection method, Telnet commands are executed on target computers that pull the DMPrimer installation image from an FTP server located in the manager.

Important! Some modern operating systems do not encourage, and sometimes actively prohibit, the remote installation of software. If you try to deploy CA ITCM software to these systems, you will usually see the deployment fail with a status of “No primer transport”. In such cases, installation of CA ITCM software components may be performed in other ways, for example, installation off physical distribution media such as DVD.

Alternatively, you can install the DMPrimer software manually. This will allow deployment of the CA ITCM infrastructure without having to rely on facilities offered by the underlying operating systems.

To determine whether automatic deployment is possible in your environment, you can perform some simple checks by running the following standard operating system operations:

- For delivery of the DMPrimer image using Windows shares, you must be able to map a share (default: ADMIN$) from your deployment manager host computer to each deployment target computer using the target user credentials supplied in the deployment request.
- For delivery of the DMPrimer image using SSH, you must be able to connect using SSH from the deployment manager to the deployment target computers.
- For delivery of the DMPrimer using Telnet, you must be able to connect using a Telnet client to your deployment target computers using the root/Administrator credentials supplied in the deployment request. You must also be able to perform an FTP fetch operation from manager target computers, connecting to FTP as the anonymous user.

Changing FTP Server Details for Use with Infrastructure Deployment

The optional details relating to the FTP server used to store infrastructure deployment packages can be altered after installation is complete, for example, if you want to relocate FTP packages on a different server.

To alter the optional details on a Windows target computer, run the following command:

`\Program Files\CA\DSM\bin\dmdeploy.exe ftpinfo` *`FTP_server FTP_user FTP_password`*

FTP_server

Specifies the address of the computer hosting the FTP server.

FTP_user

Specifies the user to connect to FTP as.

FTP_password

Specifies the password associated to the FTP user.

Windows XP Settings to Enable Agent Deployment

To enable deployment of agents to target computers that run firewall software, for example, Windows Firewall in Windows XP Professional SP2, you must perform the following actions manually:

1. Change Security Policy "Network Access: Sharing and security model for local accounts" from 'Guest only - local users authenticate as Guest' to 'Classic - local users authenticate as themselves' (applies to Windows XP).

   The Classic model allows fine control over access to resources and prevents network logons that use local accounts from being mapped to the Guest account, which normally has only "Read Only" access to a given resource.

   For more information see the web page “Network access: Sharing and security model for local accounts” of the Windows Product Documentation.

2. Configure the following firewall settings.

   - Allow File and Printer Sharing
   - Open UDP Port 4104
   - Open TCP Port 135

Chapter 6: Upgrading and Migration Considerations

This section contains the following topics:

Supported Upgrade Paths

CA ITCM Release 12.8 supports upgrades from the following products and versions:

- For manager components, the upgrade is supported from:
  - CA ITCM 12.5
  - CA ITCM 12.5 SP1
  - CA ITCM 12.5 SP1 C1
- For scalability server and agent components, the upgrade is supported from:
  - CA ITCM 12.5
  - CA ITCM 12.5 SP1
  - CA ITCM 12.5 SP1 Feature Pack 1
  - CA ITCM 12.5 SP1 Kubuntu
  - CA ITCM 12.5 SP1 C1

General Considerations

All upgrades must be performed on a like-for-like language basis. For example, you can upgrade a French to the French language version of CA ITCM, but not to the English language version.

CA ITCM Components Upgrade Considerations

When you are upgrading CA ITCM components, the following are the considerations:

- The new signatures pushed down by the CA ITCM Release 12.8 scalability server for detecting virtual application images are specially tagged, such that they are ignored by legacy agents. Therefore, only Release 12.5 agents processes the signatures and inventory virtual applications correctly.

MDB Considerations

The following are the MDB considerations:

- CA ITCM Release 12.8 does not support Microsoft SQL Server 2005 as the MDB. Upgrade the database management system to Microsoft SQL Server 2008 or higher before upgrading to CA ITCM Release 12.8.

Upgrade Considerations

When you upgrade to Release 12.8:

- CA ITCM upgrades the components that are installed with the previous release only. To install the current release components or additional components, run the installer with the modify option and select the components for installation. For example, Automated Migration and Alert Collector.
- When WAC is configured with SSL before the upgrade, verify that you import the certificates to the JRE 1.7 certificate store once the upgrade is complete. For more details, see the Enable SSL for Web Console and Web Services topic in Web Console Help.
- When CA Asset Management or CA Remote Control agents on Windows are upgraded through a Software Delivery job, the Software Delivery Agent package is added automatically to this job. Software Delivery agent is upgraded first, followed by the requested Agents.
- When you upgrade OSIM IPS components, ensure that a customized template.ini is backed up before the latest template.ini is placed in the OSIM installation directory. Extract any custom changes from the backup of template.ini and apply them to the new template.ini. In future releases, CA ITCM contains extensible-tool updates to support the customization of the boiler template.ini.
- For the plug-ins to work properly, upgrade all DSM plug-ins to the current release.

Upgrade Information

Note: When you upgrade from CA ITCMr12.5 SP1 or r12.5 SP1 C1, CCS is not upgraded. The current release contains additional CCS patches that are required to support Windows Server 2012 and SQL Server 2012. If you plan to upgrade the Manager machines to Windows Server 2012 or SQL Server 2012, contact CA technical support for the list of patches to be applied.

While you upgrade from R 12.5, R12.5 SP1, and R12.5 SP1C1 *to CA ITCM Release 12.8, do not run caf kill all before upgrade. Run caf stop, when required.*

FIPS Considerations

The following are the FIPS considerations:

- When you upgrade existing CA ITCM components, you cannot specify the FIPS mode; upgrades always force FIPS-preferred mode.
- All the upgraded components use FIPS-preferred mode until you explicitly switch them to FIPS-only mode. You can switch to the FIPS-only mode when you have upgraded all the components in the CA ITCM infrastructure to the current release. For more information about switching the FIPS modes, see the Security Features section.
- After upgrading the domain manager and the Image Prepare System (IPS), you can use IPS to upgrade existing OS and boot images to make them comply with the FIPS standards. You can then register and apply the migrated images to the boot servers. For more information about upgrading, registering, and applying the OS images, see the *OS Installation Management Administration Guide*.

More information:

How to Switch to FIPS-Only Mode (see page 418)
How to Switch to FIPS-Preferred Mode (see page 419)

Upgrade Considerations for OSIM

While upgrading ITCM from R12.5 SP1 FP1 CentOS patch (R055831) or R12.5 SP1 FP1 C1 to CA ITCM Release 12.8, perform the following steps:

- Update the existing Linux-Based (LinuxPE) boot image.
- Update the existing RHEL5.x and RHEL6.x LinuxPE-based OS images.
- Update any existing OS images (earlier supported with WinPE and Dosx) which is now supported with LinuxPE. After you update the existing OS image, ensure that the value of InstallDrive boot parameter is sda, sdb.
- Change the value manually to the one supported by the OS images.

Note: Specify the InstallDrive boot parameter about the use of local disk for the OS installation. The default value is empty and first available local disk is used for OS Installation.

You can add a disk in the following ways:

- Add the disks from the DSM explorer like *sde, sdf* for more than four (4) disks.
- Modify the file OS.def under the OSIM IPS (CA\DSM\osimips\os-template\camenu) folder.

See the new definition for the InstallDrive boot parameter for LinuxPE-based OS images:

```
[InstallDrive]

Type=MapListExt

Trans=yes

MaxLength=128

Comment=Disk to install the OS like sda or sdb or sdc.

item=sda

item=sdb

item=sdc

item=sdd
```

For more information, see OS Installation Management Administration Guide.

Upgrading Process

Upgrading CA ITCM can be a lengthy process, and may be affected by many external factors such as lack of system resources and unexpected power loss. Before commencing any upgrade, particularly of manager and scalability server components, it is recommended that a full backup of your existing installation be performed to guard against loss of data.

The order in which you carry out the upgrade of components is of importance. This release of CA ITCM supports a strict top-down upgrade strategy. You should review the steps within the phases below in full before proceeding.

- Phase 1: Upgrade the DSM enterprise manager
- Phase 2: Upgrade the DSM domain manager
- Phase 3: Upgrade the DSM scalability servers
- Phase 4: Upgrade the DSM agents

After each upgrade phase the configuration is fully functional, that is, the upgraded components can communicate with components not yet upgraded.

Note: When using the CA ITCM installation DVD to upgrade CA ITCM software previously installed on a computer be aware that all CA ITCM components installed on that computer will be upgraded.

Note: If you try to upgrade your existing installation from a different installation source or media, for example, DVD reader, than that was used for the original Unicenter DSM installation, the upgrade installation may fail with MSI error code 1602. To avoid this failure, we recommend that you configure your installation to use the same source or media that has been used for the original installation.

Important Notes on Upgrading

- Changing language of an existing installation on upgrade is not possible. If you specify a different language identifier, for example, in the response file for an unattended upgrade, the upgrade is aborted.
- After you upgrade the DSM domain manager, from the DSM Explorer, navigate to Control Panel, Configuration, Configuration Policy, PolicyName, DSM, Manager, Infrastructure Deployment, and ensure that the value of the parameter "Always deploy primer" is set to False.

  When the parameter value is set to False, the manager upgrades the DMprimer of only those target computers whose DMprimer version is lower than that of the manager. If you set the parameter to True, the manager upgrades the DMprimer of target computers regardless of the DMprimer version.
- Certificates are not updated during the upgrade process; this is to protect any existing custom certificates which may already be in place on the computer. If a master image has been updated to use new custom certificates, they are copied to the 'bin' folder during installation, but are not applied to the certificate store.

  Custom certificates must be applied during initial installations or applied manually after an upgrade process. The commands necessary to import new certificates are detailed in the Authentication (see page 375) section in the Security Features chapter.

More information:

How to Switch to FIPS-Only Mode (see page 418)
How to Switch to FIPS-Preferred Mode (see page 419)

Phase 1: Upgrade the DSM Enterprise Manager

In phase 1 of the upgrade process you upgrade the DSM enterprise manager. Enterprise managers are usually installed only in very large or very distributed companies. If you have not previously installed a DSM enterprise manager, jump to upgrade phase 2.

To upgrade the enterprise manager, perform the following steps:

1. Close down all services and applications that may have a connection to the DSM enterprise MDB.

   In a pure CA ITCM implementation this would include the DSM enterprise manager itself, remote engines for both enterprises and domains, and running instances of the DSM Reporter. If other CA applications or third-party products are installed on your network that share the MDB and hence may have an outstanding connection to it, these will need to be shut down as well.

2. Upgrade the MDB using the DVD (if appropriate).

   If the MDB is installed on a computer remote from the DSM enterprise manager, upgrade the MDB using the CA ITCM DVD. Select either “Install MDB” or “Install CCS including MDB”.

3. Upgrade the DSM enterprise manager itself using the DVD.

4. Upgrade all remote DSM enterprise engines using the DVD (if appropriate).

   If you have previously installed any enterprise level engines on remote computers, upgrade them now using the CA ITCM DVD.

5. Upgrade any remote DSM Explorers or DSM Reporters using the DVD or software delivery package (if appropriate).

   Any standalone instances of DSM Explorer, DSM Reporter, Web Services, or Web Console that are used to connect to the DSM enterprise manager and that have not been upgraded as a result of the preceding steps should be upgraded now. Instances that are installed on computers that also include a DSM scalability server or DSM agent should be upgraded after Phase 3 and Phase 4 respectively.

Note: CA ITCM Release 12.8 is compatible only with CA Asset Intelligence Release 12.8 or CA Patch Manager Release 12.8. When you upgrade to CA ITCM Release 12.8, you must also upgrade CA Asset Intelligence or CA Patch Manager to Release 12.8.

Note: When you upgrade from CA ITCMr12.5 SP1 or r12.5 SP1 C1, CCS is not upgraded. The current release contains additional CCS patches that are required to support Windows Server 2012 and SQL Server 2012. If you plan to upgrade the Manager machines to Windows Server 2012 or SQL Server 2012, contact CA technical support for the list of patches to be applied.

While you upgrade from R 12.5, R12.5 SP1, and R12.5 SP1C1 *to CA ITCM Release 12.8, do not run caf kill all before upgrade. Run caf stop, when required.*

Phase 2: Upgrade the DSM Domain Manager

In phase 2 of the CA ITCM upgrading process you upgrade the DSM domain manager.

To upgrade the DSM domain manager, perform the following steps:

1. Close down all services and applications that may have a connection to the DSM domain MDB.

   In a pure CA ITCM implementation this would include the DSM domain manager itself, remote engines for both enterprise and domain , and running instances of the DSM Reporter (for this domain as well as for the parent enterprise manager). If other CA applications or third-party products are installed on your network that share the MDB and hence may have an outstanding connection to it, these will need to be shut down as well.

2. Upgrade the MDB using the CA ITCM installation DVD (if appropriate).

   If the MDB is installed on a machine remote from the DSM domain manager, upgrade the MDB using the installation DVD. Select either “Install MDB” or “Install CCS including MDB”.

3. Upgrade the DSM domain manager itself using the installation DVD.

4. Upgrade all remote DSM domain Engines using the installation DVD (if appropriate).

   If you have previously installed any DSM domain level engines on remote computers, upgrade them now using the installation DVD.

5. Upgrade any remote DSM Explorers or DSM Reporters using the installation DVD or software delivery package (if appropriate).

   Any standalone instances of DSM Explorer, DSM Reporter, Web Services, or Web Console that are used to connect to the DSM domain manager and that have not been upgraded as a result of the preceding steps should be upgraded now. Instances that are installed on computers that also include a DSM scalability server or DSM agent should be upgraded after Phase 3 and Phase 4 respectively.

Note: CA ITCM Release 12.8 is compatible only with CA Asset Intelligence Release 12.8 or CA Patch Manager Release 12.8. When you upgrade to CA ITCM Release 12.8, you must also upgrade CA Asset Intelligence or CA Patch Manager to Release 12.8.

Note: When you upgrade from CA ITCMr12.5 SP1 or r12.5 SP1 C1, CCS is not upgraded. The current release contains additional CCS patches that are required to support Windows Server 2012 and SQL Server 2012. If you plan to upgrade the Manager machines to Windows Server 2012 or SQL Server 2012, contact CA technical support for the list of patches to be applied.

While you upgrade from R 12.5, R12.5 SP1, and R12.5 SP1C1 *to CA ITCM Release 12.8, do not run caf kill all before upgrade. Run caf stop, when required.*

Phase 3: Upgrade the DSM Scalability Servers

DSM scalability servers can be upgraded using one of the following different techniques:

- Using the CA ITCM installation DVD
- Using Software Delivery packages for scalability servers
- Using Infrastructure Deployment (DMDeploy) for scalability servers

To upgrade scalability servers using the installation DVD, insert the DVD in the scalability server computer and use the interactive installation wizard.

To upgrade scalability servers using Software Delivery packages, create a Software Delivery deployment job containing the DSM scalability server package and schedule the Software Delivery job for execution on the scalability server computers.

To upgrade Windows scalability servers using Infrastructure Deployment (DMDeploy), deploy the new scalability server package to the scalability server computers. This upgrades the scalability server itself as well as the agent and any agent plug-ins that are already installed. To instruct the installer to upgrade the agent plug-ins, you must specify the following parameters within the "Additional Windows install options" field of the Infrastructure Deployment wizard:

REINSTALL=ALL REINSTALLMODE=vomus

To upgrade Linux scalability servers using Infrastructure Deployment (DMDeploy), deploy the new scalability server package to the scalability server computers. This upgrades the scalability server itself as well as the agent and any agent plug-ins that are already installed.

Phase 4: Upgrade the DSM Agents

DSM agents can be upgraded using one of a number of different techniques as described below. Please review the methods described in the following list and select the most appropriate one. You find the detailed upgrade procedure description after this list.

- Using the CA ITCM installation DVD for Windows, Linux, MacIntel, and UNIX computers.
- Using Infrastructure Deployment (DMDeploy) for Windows, Linux and MacIntel agent computers and the “AM, RC, SD plugin(s)” (all agent plugins) package.

  If agent computers already have the complete set of agent plug-ins installed, you may use the “all agent plugins” package to upgrade them. If this is not the case you may still use the “all agent plugins” package but you should be aware that on Windows any plug-ins not already installed will be added.
- Using Infrastructure Deployment for UNIX agent computers and the “AM, SD plugin(s)” (all agent plugins) package.
- Using Infrastructure Deployment for Windows, Linux, MacIntel and UNIX agent computers and the individual agent plug-in packages.
- Using Infrastructure Deployment you can upgrade a stand alone RC agent.
- Using Software Delivery for Windows, Linux and MacIntel agent computers and the "AM, RC, SD plugin(s)" (all agent plugins) package or individual agent plug-in packages.

  If agent computers already have the complete set of agent plug-ins installed, you may use the “all agent plugins” package to upgrade them. If this is not the case you may still use the “all agent plugins” package but you should be aware that on Windows any plug-ins not already installed will be added.

- Using Software Delivery for UNIX agent computers and the "AM, SD plugin(s)" (all agent plugins) package or individual agent plug-in packages.

  Note: If you are upgrading DSM agents, you must apply the following patches prior to upgrade via Software Delivery.

  - AIX: RO01350
  - HP: RO01319
  - SUN: RO01315

Upgrading Agents Using the Installation DVD

To upgrade DSM agents using the installation DVD, insert the DVD in the agent computer and use the interactive installation wizard.

Upgrade Windows Agents Using Infrastructure Deployment and the “AM, RC, SD plugin(s)” (All Agent Plugins) Package

If agent computers already have the complete set of agent plug-ins installed, you can use the "all agent plugins" package to upgrade them. However, the "all agent plugins" package upgrades the AM, RC, and SD plug-ins but not the DTS plug-in. Use the DTS package to upgrade the DTS plug-in.

Note: Using "all agent plugins" package on Windows will also install any plug-ins that are not already installed except for the DTS plug-in.

To upgrade DSM agents using Infrastructure Deployment for Windows agent computers and the "all agent plugins" package, deploy the “AM, RC, SD plugin(s)” package to the agent computers.

To instruct the installer to upgrade, you must specify the following parameters within the "Additional Windows install options" field of the Infrastructure Deployment wizard:

REINSTALL=ALL REINSTALLMODE=vomus

Upgrade Windows Agents Using Infrastructure Deployment and the Individual Agent Plug-in

To upgrade DSM agents using Infrastructure Deployment for Windows agent computers and the individual agent plug-in packages, perform the following steps:

- Deploy the DSM Remote Control agent plug-in package to the agent computer (if appropriate).

  If you have a previous version of the Remote Control agent plug-in installed on the agent computer, deploy the new version of the plug-in.

  To instruct the installer to upgrade the agent plug-in you must specify the following parameters within the "Additional Windows install options" field of the Infrastructure Deployment wizard.

  REINSTALL=ALL REINSTALLMODE=vomus

- Deploy the DSM Software Delivery agent plug-in package to the agent computer (if appropriate).

  If you have a previous version of the Software Delivery agent plug-in installed on the agent computer, deploy the new version of the plug-in.

  To instruct the installer to upgrade the agent plug-in you must specify the following parameters within the "Additional Windows install options" field of the Infrastructure Deployment wizard.

  REINSTALL=ALL REINSTALLMODE=vomus

- Deploy the DSM Asset Management agent plug-in package to the agent computer (if appropriate).

  If you have a previous version of the Asset Management agent plug-in installed on the agent computer, deploy the new version of the plug-in.

  To instruct the installer to upgrade the agent plug-in you must specify the following parameters within the "Additional Windows install options" field of the Infrastructure Deployment wizard.

  REINSTALL=ALL REINSTALLMODE=vomus

- Deploy the DSM Basic Inventory agent plug-in package to the agent computer (if appropriate).

  If you have a previous version of the Basic Inventory agent plug-in installed on the agent computer, deploy the new version of the plug-in.

  To instruct the installer to upgrade the agent plug-in you must specify the following parameters within the "Additional Windows install options" field of the Infrastructure Deployment wizard.

  REINSTALL=ALL REINSTALLMODE=vomus

Upgrade Linux or MacIntel Agents Using Infrastructure Deployment and the “AM, RC, SD plugin(s)” (All Agent Plugins) package

To upgrade DSM agents using Infrastructure Deployment for Linux or MacIntel agent computers and the "all agent plugins" package, deploy the “AM, RC, SD plugin(s)” package to the agent computers.

By default the "all agent plugins" package upgrades previous versions of installed agent plug-ins. New plug-ins are not added.

Upgrade Linux or MacIntel Agents Using Infrastructure Deployment and the Individual Agent Plug-in Package

To upgrade DSM agents using Infrastructure Deployment for Linux or MacIntel agent computers and the individual agent plug-in packages, perform the following steps:

- Deploy the DSM Remote Control agent plug-in package to the agent computer (if appropriate).

  If you have a previous version of Remote Control agent plug-in installed on the agent computer, deploy the new version of the plug-in.

- Deploy the DSM Software Delivery agent plug-in package to the agent computer (if appropriate).

  If you have a previous version of Software Delivery agent plug-in installed on the agent computer, deploy the new version of the plug-in.

- Deploy the DSM Asset Management agent plug-in package to the agent computer (if appropriate).

  If you have a previous version of Asset Management agent plug-in installed on the agent computer, deploy the new version of the plug-in

- Deploy the DSM Basic Inventory agent plug-in package to the agent computer (if appropriate).

  If you have a previous version of Basic Inventory agent plug-in installed on the agent computer, deploy the new version of the plug-in.

Upgrade Linux or MacIntel Agents Using Software Delivery and the “AM, RC, SD plugin(s)” (All Agent Plugins) Package

To upgrade DSM agents using Software Delivery for Linux agent or MacIntel agent computers and the all agent plugins package, perform the following steps:

- Create a Software Delivery deployment job containing the "all agent plugins" package.
- Schedule the Software Delivery job for execution on the agent computers.

  By default the "all agent plugins" package upgrades previous versions of installed agent plug-ins. New plug-ins are not added.

Upgrade Linux or MacIntel Agents Using Software Delivery and the Individual Agent Plug-in Package

To upgrade DSM agents using Software Delivery for Linux or MacIntel agent computers and the individual agent plug-in packages, perform the following steps:

- Create a Software Delivery deployment job containing at least the DSM Agent + Software Delivery Agent plug-in package.

  If previous versions of other DSM Agent plug-ins have also been installed on the agent computer, include these within the job also.
- Schedule the Software Delivery job for execution on the agent computers.

Upgrade UNIX Agents Using Infrastructure Deployment and the “AM, SD plugin(s)” (All Agent Plugins) package

To upgrade DSM agents using Infrastructure Deployment for UNIX agent computers and the "all agent plugins" package, deploy the “AM, SD plugin(s)” package to the agent computers.

By default the "all agent plugins" package upgrades previous versions of installed agent plug-ins. New plug-ins are not added.

Upgrade UNIX Agents Using Infrastructure Deployment and the Individual Agent Plug-in Package

To upgrade DSM agents using Infrastructure Deployment for UNIX agent computers and the individual agent plug-in packages, perform the following steps:

- Deploy the DSM Software Delivery agent plug-in package to the agent computer (if appropriate).

  If you have a previous version of Software Delivery agent plug-in installed on the agent computer, deploy the new version of the plug-in.

- Deploy the DSM Asset Management agent plug-in package to the agent computer (if appropriate).

  If you have a previous version of Asset Management agent plug-in installed on the agent computer, deploy the new version of the plug-in

- Deploy the DSM Basic Inventory agent plug-in package to the agent computer (if appropriate).

  If you have a previous version of Basic Inventory agent plug-in installed on the agent computer, deploy the new version of the plug-in.

Upgrade Windows Agents Using Software Delivery and the “AM, RC, SD plugin(s)” (All Agent Plugins) Package

If agent computers already have the complete set of agent plug-ins installed, you may use the "all agent plugins" package to upgrade them. If this is not the case, you may still use the "all agent plugins" package but you should be aware that on Windows any plug-ins not already installed will be added.

To upgrade DSM agents using Software Delivery for Windows agent computers and the "all agent plugins" package, perform the following steps:

- Create a Software Delivery deployment job containing the"all agent plugins" package.
- Schedule the Software Delivery job for execution on the agent computers.

Upgrade Windows Agents Using Software Delivery and the Individual Agent Plug-in Package

To upgrade DSM agents using Software Delivery for Windows agent computers and the individual agent plug-in packages, perform the following steps:

- Create a Software Delivery deployment job containing at least the DSM Agent + Software Delivery Agent plug-in package.

  If previous versions of other DSM agent plug-ins have also been installed on the agent computer, include these within the job also.

- Schedule the Software Delivery job for execution on the agent computers.

Upgrade UNIX Agents Using Software Delivery and the "AM, SD plugin(s)" (All Agent Plugins) Package

Note: When upgrading from r11.1 UNIX agents, apply the following patches before you upgrade via Software Delivery.

- AIX : RO01350
- HP : RO01319
- SUN: RO01315

To upgrade DSM Agents using Software Delivery for UNIX agent computers and the all agent plugins package, perform the following steps:

- Create a Software Delivery deployment job containing the all agent plugins package.
- Schedule the Software Delivery job for execution on the agent computers.

  By default the all agent plugins package upgrades previous versions of installed agent plug-ins. New plug-ins are not added.

Upgrade UNIX Agents Using Software Delivery and the Individual Agent Plug-in Package

Note: When upgrading from r11.1 UNIX agents, apply the following patches before you upgrade via Software Delivery.

- AIX : RO01350
- HP : RO01319
- SUN: RO01315

To upgrade DSM Agents using Software Delivery for UNIX agent computers and the individual agent plug-in packages, perform the following steps:

- Create a Software Delivery deployment job containing at least the DSM Agent + Software Delivery Agent plug-in package.

  If previous versions of other DSM Agent plug-ins have also been installed on the agent computer, include these within the job also.
- Schedule the Software Delivery job for execution on the agent computers.

Chapter 7: CA ITCM Connector for CA Catalyst

CA Catalyst connectors expose product data to consuming products such as CA Spectrum Service Assurance and CA IT Process Automation Manager for visualization, analysis, and management in a unique, heterogeneous context.

Note: You can install the CA ITCM connector with an existing domain manager or scalability server only on Windows operating systems.

CA ITCM connector supports SSA 3.2.0. The CA ITCM connector interfaces with the DSM domain manager or a standalone scalability server registered with a domain manager to expose CA ITCM data for use by products that leverage the CA Catalyst infrastructure. Integrating CA ITCM data with consuming products, such as CA Spectrum SA, enables reconciliation and correlation of entity properties with existing configuration items (CIs). Integration also lets you evaluate the data in a different, broader business service context.

Note: CA ITCM connector 3.2.0 supports only the Northbound on SOI 3.2.0.

With CA Catalyst connector integration, there is one CA ITCM connector per domain. The CA ITCM connector interfaces with the domain manager using the following CA ITCM components or functionality:

- CA ITCM Web Services

  CA ITCM Web Services is used to retrieve information about the CIs to be published to CA Catalyst connector.

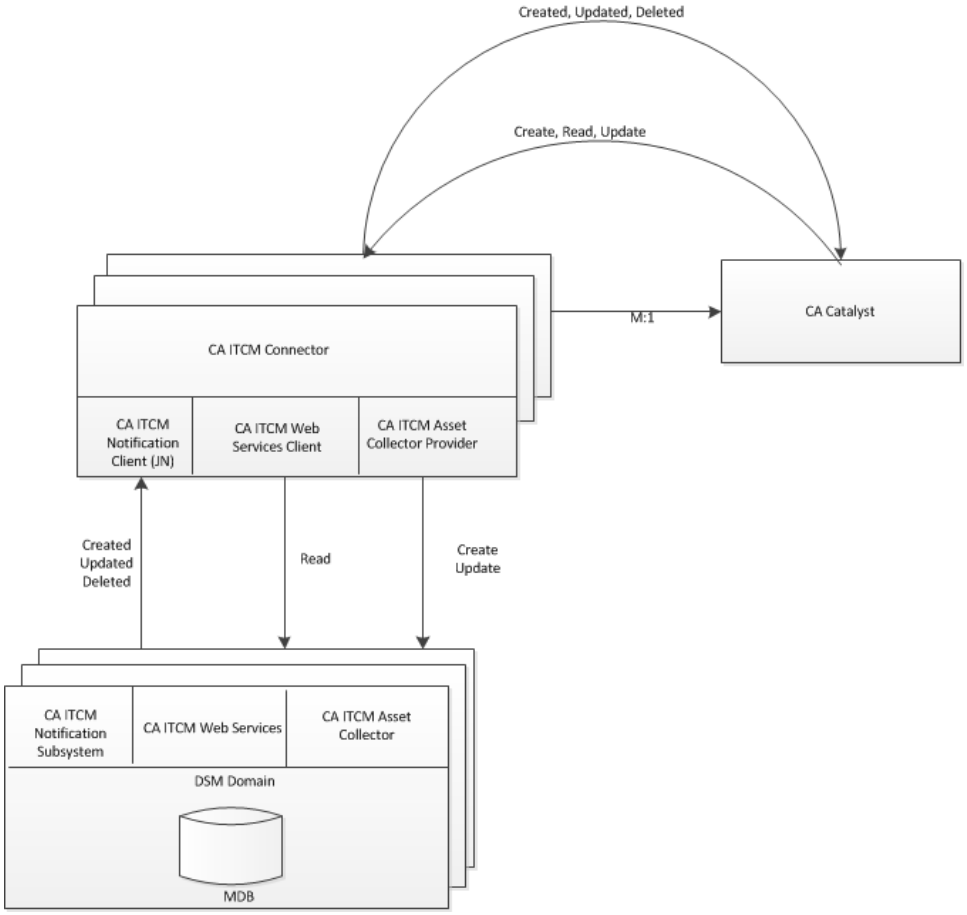
- CA ITCM Event Notification Subsystem

  Events about updates to published CIs are received through the CA ITCM event notification subsystem.

- Asset Collector

  The Asset Collector component is used during CA Spectrum SA subscribe operations for Computer CI data. The Asset Collector files help to move the inbound create data and update data from the connector to the CA ITCM MDB.

The following graphic summarizes CA ITCM - CA Catalyst connector integration:



Note: For more general information about the CA Catalyst infrastructure and its connectors, information that applies to all connectors, and information about custom connector integrations, see the *Connector Guide* distributed with CA Spectrum SA. For complete information about installing, configuring, and using the CA ITCM connector, see the *CA IT Client Manager Connector Guide* also distributed with CA Spectrum SA.

Chapter 8: Desktop Virtualization

This section includes the scenarios about the use of desktop virtualization support functionality. Using CA ITCM, you can manage your virtual desktop infrastructure on VMware View and Citrix XenDesktop. CA ITCM helps you do the following:

- You can manage the golden template, vDisks, and virtual desktops from DSM Explorer.
- You can configure automatic reinstallation of software installed on virtual desktops, without affecting your chages after a reboot or a desktop update with a new version of the golden template.

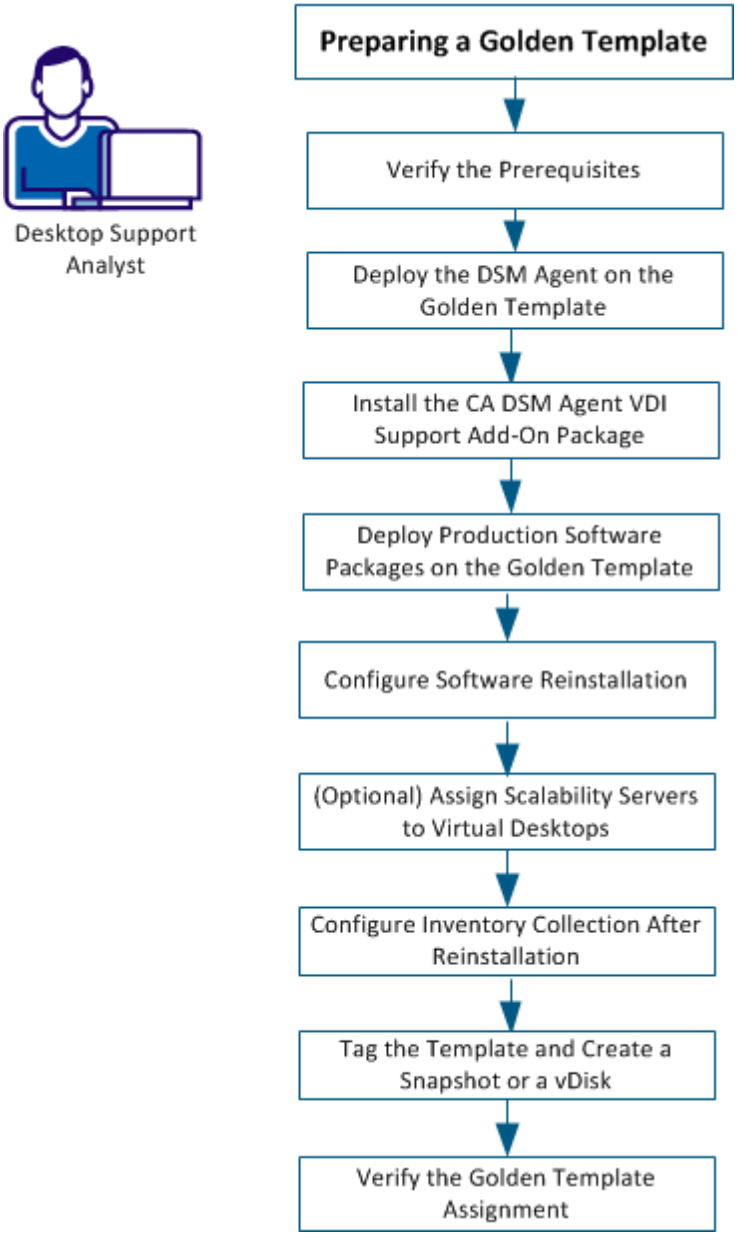
  For example, software installed on a standard mode vDisk based virtual desktop is lost after you log off. You can configure CA ITCM to automatically reinstall these software when you log in next time.
- Includes new virtual desktop identification and registration scheme, improved asset registration speed, and queries and reports.

  Note: The management of user profiles, user data, user personality, or desktop configuration is not supported with this release. Rather, Microsoft methods like roaming user profile and folder redirection handle these tasks. For more information, see your Microsoft documentation.

Preparing a Golden Template

As a desktop support analyst, you must prepare the golden template to integrate your virtual desktop solution with CA ITCM. This integration helps you manage the golden template, VMware View Clones, Citrix PVS streamed virtual desktops, or MCS-based virtual desktops from CA ITCM.

The following diagram illustrates the steps for preparing a golden template:



The golden template preparation includes performing the following tasks:

1. Verify the Prerequisites (see page 271)
2. Deploy the DSM Agent on the Golden Template (see page 272)
3. Install the CA DSM Agent VDI Support Add-On Package (see page 272)
4. Deploy Production Software Packages on the Golden Template (see page 273)
5. Configure Software Reinstallation (see page 274)
6. Tag the Template and Create a Snapshot or vDisk (see page 285)
7. (Optional) Assign Scalability Servers to Virtual Desktops (see page 284)
8. Configure Inventory Collection on Software Reinstallation (see page 285)
9. Verify the Golden Template Assignment (see page 286)

Verify Prerequisites

To prepare a golden template, verify the following prerequisites:

- Verify that the virtual desktop agent is installed on the golden template computer.

  Note: A sound working knowledge of virtual desktop solutions such as VMware View and Citrix XenDesktop is required to implement the integration with CA ITCM.
- Verify that the Citrix PVS target device is installed on the golden template computer if you want to create Citrix vDisk-based virtual desktops.
- (Only for Citrix XenDesktop 7) Verify that .Net 3.5 is available.

Deploy the DSM Agent on the Golden Template

CA ITCM provides different DSM agent packages depending on the functionalities you need. At the minimum, you need the DSM common agent and software delivery agent (CA DSM Agent + Software Delivery plug-in). If you want the complete functionality, deploy the CA DSM Agent + AM, RC, SD plug-ins package.

Note: DSM agent refers to the DSM common agent and the software delivery agent (CA DSM Agent + Software Delivery plug-in) not the full agent as mentioned.

Deploying the DSM agent on the golden template ensures that the DSM agent is available on the virtual desktops that are created from the golden template. The golden template and all the virtual desktops are added as managed computers in CA ITCM.

Follow these steps:

1. Navigate to Control Panel, Deployment, Infrastructure Deployment Wizard from DSM Explorer.
2. Follow the instructions in the wizard and perform the following tasks:
   - Select an agent package depending on the functionalities you need.
   - Select the golden template as the target computer in the wizard.
   - Enter the IP address or fully qualified domain name (FQDN) of the scalability server with which the deployed agent is registered.
3. Click Finish.

   A deployment job is created under Control Panel, Deployment, Deployment Job Status. The job is pushed to the golden template.
4. Monitor the job status in the Control Panel, Deployment, Deployment Job Status node.

   After the deployment is successful, the agent is automatically registered with the scalability server. After the registration, the golden template appears in the domain manager.

Note: By default, golden template and the virtual desktops that are provisioned out of it, report to the same scalability server. You can assign a different scalability server for a range of virtual desktops depending on the virtual desktop naming pattern. See (Optional) Assign Scalability Servers to Virtual Desktops (see page 284).

Important! When you run a golden template on Windows XP, reboot the computer after the DSM agent installation to run the Tag Template activate procedure.

Install the CA DSM Agent VDI Support Add-On Package

Install the CA DSM Agent VDI Support Add-On Package on the golden template to enable software reinstallation and integration between CA ITCM and VMware View or Citrix XenDesktop. The add-on enables the DSM agent to operate and manage the virtual desktop environment.

The CA DSM Agent VDI Support Add-On Package performs the following tasks:

- Enables use of the software state database and, if needed, sets up the paths.
- Sets the agent to the golden template mode.
- Copies a set of cloning scripts to the golden template, which are used during software reinstallation.

Follow these steps:

1. Right-click the golden template in DSM Explorer and select Software Jobs, Deploy software package.

   The Deploy Software Package Wizard opens.

2. Follow the instructions in the wizard. Specify the following tasks in the wizard:

   - Select the CA DSM Agent VDI Support Add-On Windows ENU package under DSM Software Packages.

     Note: The package provides a common solution for both VMware View and Citrix XenDesktop and also supports Sysprep settings on VMware View.

   - Schedule the time and enter the job container name.

3. Click Finish.

   The Setup Jobs dialog opens.

4. Click OK.

   The package is delivered at the scheduled time.

5. Select the golden template, Jobs, Software Jobs in DSM Explorer to monitor the job status.

Deploy Production Software Packages on the Golden Template

You can use software delivery to deploy production software packages on the golden template. The software applications that are installed on the golden template are automatically available on the virtual desktops that are created from the golden template.

Follow these steps:

1. Right-click the golden template in DSM Explorer and select Software Jobs, Deploy software package.

   The Deploy Software Package Wizard opens.

2. Follow the instructions in the wizard. Specify the following actions in the wizard:

   - Select the software packages and procedures you want to deploy.
   - Enter a job container name.

3. Open the advanced job settings dialog and click Finish.

   The Setup Jobs dialog opens.

4. Click the Jobs, Job Options, Store packages in the Scalability Server Staging Library option.

5. Click OK.

   The specified packages are staged on the scalability server of the golden template. The package is delivered at the scheduled time.

Configure Software Reinstallation

Software, that is installed on non-persistent virtual desktops, is lost after a reboot or log-off, or on a desktop update with newer version of the golden template. You can configure CA ITCM to reinstall the software in such cases. CA ITCM uses an instance software state database that contains the information of all software jobs that the agent executes on the virtual desktops. The virtual desktops include the details of the instance software state database and run context. This information is important for CA ITCM to reinstall the software.

Depending on the desktop virtualization solution and the desktop pool/group settings, you configure the software reinstallation in different ways:

VMware View

- For desktop groups with *quickprep* customization, perform one of the following configuration tasks:
  - Configure Software Reinstallation Parameters in the Configuration Policy (see page 278)
  - Configure the Pool Settings to Run Compose.bat on the Virtual Desktops (see page 276)

  Note: If you configure both policy and the pool settings, pool settings take precedence.
- For desktop groups with *sysprep* customization, perform the following configuration task:
  - Configure Software Reinstallation Parameters in the Configuration Policy (see page 278)

Citrix XenDesktop

- For desktops created from MCS, perform the following configuration task:
  - Configure Software Reinstallation Parameters in the Configuration Policy (see page 278)
- For vDisk based desktops, perform one of the following configuration tasks:
  - Configure Software Reinstallation Parameters in the Configuration Policy (see page 278)
  - Configure Personality Data on the Target Devices (see page 281)

  Note: If you configure both policy and the personality data, personality data takes precedence.

Note: You can also modify other configuration policies. For more information about these policies, see Configuration Policies for Desktop Virtualization Support (see page 286).

Configure the Pool Settings to Run Compose.bat on the Virtual Desktops

Specify the following command in the post synchronization script under Guest Customizations when you create the pool:

```
Compose.bat [ISDBPath=<Path>] [Run=<Run>] [ISDBUser=<User> ISDBPassword=<Password>]
```

ISDBPATH

Specifies the path where the instance software database is stored. The path can be local or network depending on the pool type. Specify a network path for nonpersistent pools and local or network path for persistent pools. Environment variables and predefined macros like {SCALABILITY_SERVER} and {POOL_NAME} are allowed as part of the path.

Example: \\{SCALABILITY_SERVER}\%COMPUTERNAME%

Important! On Windows 7, if the path parameter contains the %USERNAME% environment variable, do not pass this parameter as a command line parameter to Compose.bat. Instead, include all the parameters inside the Compose.bat file (for VMware View only).

{SCALABILITY_SERVER}

Returns the scalability server to which the virtual desktop reports to. By default, virtual desktops report to the same scalability server that the golden template reports to. If you have changed the scalability server assignment explicitly (see page 284), the macro returns the new scalability server name.

{POOL_NAME}

Returns the pool name of the virtual desktop. This macro is applicable for VMware View only.

Persistent Use

Environment variables, like %COMPUTERNAME% can be used as part of the ISDB path.

Example: \\MachineName\{POOL_NAME}\%COMPUTERNAME%

This option results in a path unique for a user (because a persistent virtual desktop is always assigned to the same user).

Non Persistent Use

The user-specific environment variables, %USERNAME% and %USERDOMAIN%, can be included to identify uniquely the software state database for a particular user.

Example: \\MachineName\{POOL_NAME}\%USERNAME%

Note: Be careful to select the location in the case of network share paths when multiple desktop pools assigned to a single user. You must ensure that the software state of the virtual desktop used by a user in one pool is not overwritten by the data of another virtual desktop used by the same user in another pool. For example, given that “User1” is entitled to nonpersistent pools, poolA and poolB. if the path for both pools is specified as “//<machine-name>/<share-name>/Database/%USERNAME%”, the software state of “User1” can be overwritten if the user logs on and uses both virtual desktops in both pools. Hence, ensure that you define different paths as follows:

- “/<machine-mname>/<share-name>/PoolA/%USERNAME%”
- “/<machine-mname>/<share-name>/PoolB/%USERNAME%”

ISDBUSER

Specifies the user name to connect to the instance software database path in a network share. The user name must be encrypted using sd_acmd encrypt command.

ISDBPASSWORD

Specifies the password to connect to the instance software database path in a network share. The password must be encrypted using sd_acmd encrypt command.

RUN

Specifies when to execute the Offline RAC process. Valid values are OnRecompose and OnLogon.

OnRecompose

Specifies that the Offline RAC is initiated when the desktop starts after a refresh or recompose. Use this option for desktop groups where the desktop assignment to users is fixed, such as persistent linked clones.

OnLogon

Specifies that Offline RAC is initiated on user logon.

Use this option for desktop groups where the desktop assignment to the users varies from session to session such as nonpersistent desktops.

Examples:

- **Persistent Use:** Compose.bat "ISDBPath=<Path>" "Run=OnRecompose"
- **Nonpersistent Use:** Compose.bat "ISDBPath=<Path>" "Run=OnLogon"

Configure Software Reinstallation Parameters in the Configuration Policy

Follow these steps:

1. Navigate to Control Panel, Configuration Policy, Default Computer Policy, DSM, Software Delivery, Agent.
2. Select RAC: Virtual machine software reinstallation settings, to view the following attributes:

Agent Naming Pattern

Specifies the agent naming pattern of the virtual desktop. For VMware View, the naming pattern must be *name-{n}* and for XenDesktop, the naming pattern must be *name##*. You cannot specify this placeholder (#) at the beginning and more than once.

From

Specifies the starting range for the desktops to be included. The range can be a number; XenDesktop lets you specify an alphabet also. *From* specifies the start of the naming pattern. The start and the place holder length must be equal, and *To* value can be greater than the place holder length.

To

Specifies the ending range for the desktops to be included. The range can be a number; XenDesktop lets you specify an alphabet also.

Examples: Agent naming pattern for VMware View

Agent Naming Pattern	From	To	Possible Desktop Names
Name-{n}	1	100	Name-1, Name-2….Name-100

Examples: Agent naming pattern for Citrix XenDesktop

Agent Naming Pattern	From	To	Possible Desktop Names
Name#	1	100	Name1, Name2, …..Name100
Name###	1	100	Name001, Name002…..Name100
Name##	AA	AZ	NameAC, NameAE,…NameAZ

Instance Software Database Path

Specifies the path where the instance software database is stored. The path can be local or network depending on the pool type. Specify a network path for nonpersistent pools and local or network path for persistent pools (persistent linked clones in case of VMware View and difference mode vDisk based virtual desktops groups in XenDesktop where the desktop assignment is fixed). In the later case, specifying a local path is only possible if the persistent disk associated with the virtual desktop is available. Environment variables and predefined macros like {SCALABILITY_SERVER}, {GROUP_NAME} and {POOL_NAME} are allowed as part of the path.

Example: \\{SCALABILITY_SERVER}\{GROUP_NAME}\%COMPUTERNAME%

{GROUP_NAME}

Returns the desktop group name of the virtual desktop. This macro is applicable only for Citrix XenDesktop.

{POOL_NAME}

Returns the pool name of the virtual desktop. This macro is applicable only for VMware View.

{SCALABILITY_SERVER}

Returns the scalability server to which the virtual desktop reports to. By default, virtual desktops report to the same scalability server that the golden template or vDisk reports to. If you have changed the scalability server assignment explicitly (see page 284), the macro returns the new scalability server name.

Note: For XenDesktop, You can assign multiple users to a single desktop in a pooled static group. To support reinstallation of user installed software in this case, specify the instance software database path in the following way: *<server_name>**%computername%**%username%.* Also, set the run context to *OnLogon.*

Username

Specifies the user name to connect to the instance software database path in a network share. The user name is encrypted using sd_acmd encrypt command.

Password

Specifies the password to connect to the instance software database path in a network share. The password is encrypted using sd_acmd encrypt command.

Run

Specifies when to execute the Offline RAC process. The allowed values are OnRecompose and OnLogon.

OnRecompose

Specifies that the Offline RAC is initiated when the desktop starts after a refresh or recompose (VMware View), desktop reset or snapshot update (Citrix MCS) and vDisk update or desktop reset (Streamed Virtual desktops).

Use this option for desktop groups where the desktop assignment to users is fixed, such as persistent linked clones, pooled static desktops and desktops that are based on difference mode vDisks.

OnLogon

Specifies that Offline RAC is initiated on user logon.

Use this option for pooled desktop groups where the desktop assignment to the users varies from session to session such as nonpersistent desktops, pooled random desktops and pooled desktops that are based on standard mode vDisks.

3. Save and seal the policy.

   The software reinstallation configuration is applied on the golden template.

Configure Personality Data on the Target Devices

For Citrix XenDesktop configure the personality data once you create the catalogs using the XenDesktop setup wizard or Streamed VM setup wizard, and before the desktop group(s) are created out of the machines.

Follow these steps:

1. Open the Target Device Properties dialog in Citrix Provisioning Services Console for a virtual desktop.
2. Click the Personality tab and add the following parameters:

   CA_DSM_ISDBPATH

   Specifies the path where the instance software database is stored. The path can be local or network depending on the pool type. Specify a network path for nonpersistent pools and local or network path for persistent pools (difference mode vDisk based virtual desktops groups in XenDesktop where the desktop assignment is fixed).

   In the later case, specifying a local path is only possible if the persistent disk associated with the virtual desktop is available. Environment variables and predefined macros like {SCALABILITY_SERVER} and {GROUP_NAME} are allowed as part of the path.

   Example: \\{SCALABILITY_SERVER}\{GROUP_NAME}\%COMPUTERNAME%

   {GROUP_NAME}

   Returns the desktop group name of the virtual desktop. This macro is applicable only for Citrix XenDesktop.

   {SCALABILITY_SERVER}

   Returns the scalability server to which the virtual desktop reports to. By default, virtual desktops report to the same scalability server that the golden template or vDisk reports to. If you have changed the scalability server assignment explicitly (see page 284), the macro returns the new scalability server name.

CA_DSM_ISDBUSER

Specifies the name of the Instance software database user in an encrypted form. The user name is encrypted using the sd_acmd encrypt command.

CA_DSM_ISDBPASSWORD

Specifies the encrypted instance software database password in an encrypted form. The password is encrypted using the sd_acmd encrypt command.

CA_DSM_RUN

Specifies when to execute the Offline RAC process. Valid values are OnRecompose and OnLogon.

OnRecompose

Specifies that the Offline RAC is initiated when the desktop starts after a reset or snapshot update (in case of Citrix MCS) and vDisk update or reset (in case of streamed virtual desktops).

Use this option for desktop groups where the desktop assignment to users is fixed, such as pooled static desktops and desktops that are based on difference mode vDisks.

OnLogon

Specifies that Offline RAC is initiated on user logon.

Use this option for pooled desktop groups where the desktop assignment to the users varies from session to session such as pooled random desktops and pooled desktops that are based on standard mode vDisks.

3. Save the properties.

   The virtual desktop is configured to include the instance software state database details.

4. Do one of the following tasks:

   - Perform steps 1 through 3 on all the virtual desktops.
   - Copy the parameters from a desktop to all the virtual desktops.

You have now configured personality data on the target devices.

Streaming of Personality Data to Virtual Desktops in XenDesktop 5.0 and 5.5

With Citrix XenDesktop Virtual Desktop Agent 5.0 and Virtual Desktop Agent 5.5, personality data for virtual desktops is not streamed to the virtual desktops on the start.

When the instance software database configuration is done using personality data and not through the configuration policy, the software reinstallation functionality is affected.

Use the following hot fixes of the Citrix Virtual desktop agent to overcome this issue.

- http://support.citrix.com/article/CTX131268 (32-bit version)
- http://support.citrix.com/article/CTX131269 (64-bit version)

Supported Virtual Desktop Types for Software Reinstallation

CA ITCM supports software reinstallation on the following virtual desktop types:

VMware View:

- Linked clones

Citrix XenDesktop:

- Pooled static desktops
- Pooled random desktops
- Streamed desktops
- Existing catalog-based desktop on standard or difference mode vDisk

Note: You can create the following types out of the golden template but no support is needed for software reinstallation. Only the template software records are reported to the domain manager on startup. You can manage the following types independently as regular CA ITCM agents.

- Private mode vDisk desktops
- Dedicated desktops (through MCS)

Important! Verify that the virtual desktops are configured to reboot when the user logs off for floating linked clones in VMware View. When you create pooled static groups with a desktop assigned to multiple users, specify this setting manually for software reinstallation to work as expected.

(Optional) Assign Scalability Servers to Virtual Desktops

All virtual desktops report to the same scalability server as the agent of the golden template or the vDisk. You can assign different scalability servers to the agents on virtual desktops to distribute the load on the server. Before you can proceed, you must have decided the naming pattern for desktops that is created from the golden template. Based on the naming patterns of the desktop, you can assign different scalability servers to the agents on the desktop. You can also configure the number of desktops you want to assign to the server.

Follow these steps:

1. Open the configuration policy that you want to apply on the golden template in DSM Explorer.
2. Navigate to DSM, Common Components, Registration.
3. Double-click the Scalability Servers Configuration policy.
4. Click Add Row and specify the naming pattern and range in the following fields:

   Agent Naming Pattern

   Specifies the agent naming pattern of the virtual desktop. For VMware View, the naming pattern must be like name-{n} and for XenDesktop the naming pattern must be like name##. You can opt a different naming pattern too.

   Scalability Server

   Specifies the scalability server that you want to assign for the specified pattern and range.

   From

   Specifies the starting range for the desktops to be included. The range can be a number; Citrix XenDesktop lets you specify an alphabet also. The start and the place holder length must be equal, and *To* value can be greater than the place holder length.

   To

   Specifies the ending range for the desktops to be included. The range can be a number; Citrix XenDesktop lets you specify an alphabet also.

Examples: Agent naming pattern for Citrix XenDesktop

Agent Naming Pattern	From	To	Possible Desktop Names
Name#	1	100	Name1, Name2, Name100
Name###	1	100	Name001, Name002, Name100
Name##	AB	BC	NameAC, NameAE, NameAZ

Examples: Agent naming pattern for VMware View

Agent Naming Pattern	From	To	Possible Desktop Names
Name-{n}	1	100	Name-1, Name-2, Name-100

5. Save and seal the policy.

   When virtual desktops are created, they are automatically assigned to a scalability server depending on the configuration you specified.

Configure Inventory Collection on Software Reinstallation

Configure inventory collection to collect the inventory from the virtual desktop, either immediately after RAC or when the user logs in after RAC. Inventory collection helps you verify whether all the software applications are reinstalled.

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, Default Computer Policy, DSM, Software Delivery, Agent.
2. Select the RAC: Collect Inventory After Reinstall configuration policy and set the value to one of the following attributes:

   No

   Specifies that the inventory is not collected after reinstallation, but during the normal run of AM agent that can run after RAC or before RAC.

   Immediately

   Specifies that the inventory is collected immediately after the software reinstallation. Reports the reinstalled software as part of software inventory and client device information such as IP, MAC address, and host name only after the user logon.

   After User Logon

   Specifies that the inventory is collected only when the user logs in after RAC. The reinstalled software and client device information are reported after the user logs in.

   The inventory collection after RAC happens based on the configuration you specified.

Tag the Template and Create a Snapshot or vDisk

Tagging helps you track the version of the template that is used by the virtual desktops. Tag the template to generate a template tag and associate the virtual desktops with their parent golden template.

Follow these steps:

1. Drag the Tag Template procedure from the CA DSM Agent add-on VDI package to the golden template on DSM Explorer.

   The procedure status appears, after executing the procedure.

2. Do one of the following actions depending on the desktop virtualization solution:

   - (For XenDesktop using Citrix Provisioning Services) Create the vDisk using XenConvert or other appropriate imaging tool.
   - (For VMware View and Citrix MCS) Shut down the virtual machine and create a snapshot.

   This action associates the snapshot or vDisk with the template tag.

The snapshot or vDisk are created and associated with the golden template using the template tag.

Important!

- When you run a golden template on Windows XP, reboot the computer after the DSM agent installation to successfully run the Tag Template activate procedure.
- For Vmware View,Nonpersistent desktop pools must be created with the "Power off and delete virtual machine after first use" option selected in VMware View 4.0. Otherwise, the Offline RAC functionality does not work. In VMware View 4.5, select instead the "Delete or refresh desktop on logoff" option and set it either to "Refresh Immediately" or "Delete Immediately".

Verify the Golden Template Assignment

You can verify the assigned golden template from the inventory, template settings.

Follow these steps:

1. Navigate to the Computers and Users, All Computers, *Computer Name*, and Inventory.
2. Click the Operating System tab, Template Settings.

   The list of assigned templates appears.

The golden template is now prepared for managing the virtual desktops.

Configuration Policies for Desktop Virtualization Support

After installing the CA DSM Agent VDI Support Add-On package, configure CA ITCM configuration policies for virtual desktops. Some of these policies are mandatory and preset by the VMware View. Other policies are optional and require input as documented.

A new registration policy group is added and other configuration policy groups are extended to provide support for managing virtual desktops that are provided by Citrix XenDesktop and VMware View.

Note: Apply the configuration policies to the agents of the cloned virtual desktops and to the agents of the golden templates. This process must be done with the exception of the mandatory locally managed policies preset by the cloning scripts before saving the golden template snapshot.

The policy is not automatically inherited by the cloned virtual desktops from the golden template. When the cloned virtual desktop values and the centrally managed policy values are different, the values are overwritten shortly after the registration with the manager.

registration Policy Group

A new policy subgroup, registration, has been added under the Common Components policy group for virtual desktop-specific identification. The registration policy group contains the following policies:

Host key

Defines a string that is used to identify uniquely a cloned machine. A host key is required for linked clones because each Recompose of the virtual desktop generates a new virtual machine that registers a new unique computer in the MDB. The result is that, over time, the domain manager would see many computers that no longer exist. If the host key is used, the existing computer records for the virtual desktops in the MDB are reused over time.

A host key contains plain text plus any number of macros. On registration, CAF expands the macros and sends the result to the scalability server. The engine then uses the host key rather than the host UUID/host name/MAC address to identify assets in the MDB. From now on, the host key identifies the agent.

Note: In typical scenarios, the MAC address is not changed during the Recompose of persistent linked clones. However, in some cases VMware changes the MAC address of the persistent linked clones during the recompose operation. Therefore, the use of a host key is typically needed for both nonpersistent, persistent linked clones, and MCS-based virtual desktops as well.

Use the following macros:

Environment variable: $env(name)

Example: $env(“COMPUTERNAME”)-VDI

Registry key: $reg(key,value)

Example: $reg(“HKLM\SOFTWARE\CA\GuestID”,” GuestUUID”)-VDI

INI file value: $ini(path,section,key)

Example: $ini(“c:\id.ini”,”identity”,”uuid”)-VDI

These macros can also be combined in the same string.

Example:
$env(“COMPUTERNAME”)-$reg(“HKLM\SOFTWARE\CA\GuestID”,”GuestUUID”)-VDI

Note: By default, the CAFPostInit.dms script sets the host key on the agent with $env(“COMPUTERNAME”). Hence, you do not need to modify this policy. However, if you want to use another macro, verify that all generated host keys are unique by using the appropriate host key macro strings in the CAFPostInit.dms script. Also, verify that the host key is not more than 64 characters long.

Default: empty, <locally managed>

Scalability Servers Configuration

Allows the administrator to configure the agent scalability server, which is based on the virtual machine naming pattern that is used for the desktop pool and range. You can apply multiple ranges. This policy is optional, and if no value is set, all clones report to the same scalability server as the agent of the golden template from which they have been cloned. For more information, see scalability servers configuration.

Agent (Software Delivery) Policy Group

The Agent (Software Delivery) policy group has been expanded to include the following configuration policies for managing the software delivery agent in VMware View environments.

Note: The RAC configuration policies in the Agent policy group apply only to Offline RAC. The traditional RAC functionality is configured by the policies in the Software Delivery, Manager policy group.

You can modify policy parameter values by double-clicking a policy to display the Setting Properties dialog.

RAC: Behavior for multiple entries of the same activate/configure procedure

Determines whether duplicate software procedures are excluded during OfflineRAC.

In software delivery, an install procedure is allowed to run only once, but activate and configure procedures can run multiple times. When the agent prepares the RAC container for a software package, a number of activate and configure procedures can be included. The value that is set for this policy determines how duplicate activate/configure procedures within a single software package are handled. Valid values are as follows:

re-run each duplicate activate/configure procedure

Specifies all activate/configure procedures recorded in the database are run.

re-run first duplicate activate/configure procedure

Specifies if any activate/configure procedures are included more than once, only the first duplicate is run.

re-run last duplicate activate/configure procedure

Specifies if any activate/configure procedures are included more than once, only the last duplicate is run.

Default: re-run each duplicate activate/configure procedure

RAC: Container Type

Specifies whether the agent runs software jobs in the offline RAC container as a batch or with no linkage. Valid values are as follows:

Batch

Specifies all jobs be run sequentially as a single unit of work for each target. If any job in the sequence fails, then the remaining jobs for that target are not executed.

No Linkage

Specifies the jobs that are run sequentially but independently from each other.

Default: Batch

RAC: Delete software procedure from software state database in case of failure

Controls whether the software state database is updated when one or more jobs in the RAC container fails. If set to True, the failed job entries are deleted from the software state database. If False, the failed entries remain.

Default: True

RAC: Keep job check GUI until end user closes

Controls whether the Software Delivery Job Check dialog waits for the user to close the dialog if RAC fails during an interactive-mode reinstallation. For example, a value of True ensures that a RAC failure is not overlooked when the user is away from the computer.

Default: True

RAC: Maintain Pre Install Software State Database

Defines whether a preinstall software state database is maintained when no users are assigned to the virtual desktops. A preinstall software state database is useful when virtual desktops in a pool are created and registered as agents but not yet assigned to any users. A preinstall database is useful for the administrator to push required software packages to the virtual desktops.

If set to True, a preinstall software state database is maintained on the local file system before a user is assigned to the virtual desktop. The preinstall database is merged into the assigned users instance software state database whenever the user logs in for the first time.

If set to False, the following conditions apply.

Persistent desktops:

For persistent desktops, if Offline RAC is configured to run on logon, setting this policy to False results in these software packages being reinstalled because the software job records are added to the instance database instead of the preinstall database.

Nonpersistent desktops:

For nonpersistent desktops, setting this policy to False results in software delivery job records not being maintained for these software packages. Furthermore, they cannot be reinstalled when the virtual desktop is refreshed later on.

Default: True

RAC: Maintain Software State Database

Controls whether the software delivery agent maintains a database of its state, regardless of the VMware View functionality.

Note: This policy is mandatory and preset by the VMware View integration scripts to True. Do not manually change the set value.

Default: False, <locally managed>

RAC: Maximum number of seconds to retry

Defines the maximum seconds that an agent can sleep between attempts to contact the scalability server during one job check. This policy works with the RAC: Number of reties in case of offline RAC policy. Reconnection attempts until the limit specified by either of these policies is reached.

Default: 60

RAC: Number of retries in case of offline RAC

Defines the maximum number of connection retries an agent can make to the scalability server during one job check. This policy works with the RAC: Maximum number of seconds to retry policy. Reconnection attempts until the limit specified by either of these policies is reached.

Default: 100

RAC: Password to access the instance software state database

Specifies the password of the user with access permissions to the instance software state database. The password string is encrypted. If specified, the agent uses these credentials to access the network share.

We recommend that you encrypt the password first using the "sd_acmd encrypt" command. Then provide the encrypted password as one of the parameters when running the Compose.bat script, which in turn sets the configuration parameter.

Alternatively, if the password for the share location is the same for all desktop pools to be created from a particular golden template snapshot, you can set the password in the configuration policy. Then apply the policy to the golden template and the cloned virtual desktops.

Default: empty, <locally managed>

RAC: Path to instance software state database

Specifies the installation path for the instance software state database. The specified path can include embedded environment variables, for example, “\\Fileserver1\Share1\%COMPUTERNAME%\InstanceSoftwareDatabase”.

Note: This policy is mandatory, but enter the path manually as one of the parameters when running the Compose.bat script. This script in turn sets the configuration parameter.

Default: empty, <locally managed>

RAC: Path to template software state database

Specifies the installation path for the template software state database. If the value is empty, the agent uses the appropriate unit-specific path, that is, “<ITCM InstallDir>\SD\ASM\DATABASE\Agent\TemplateSoftwareDatabase”.

Default: empty, <locally managed>

RAC: RAC policy setting of the agent

Controls the RAC Policy setting of the software delivery agent. If set to True, the RAC Policy of the agent is set to Offline. If False, RAC Policy is set to the default RAC setting.

Note: This policy is mandatory and preset by the VMware View integration scripts to True. Do not manually change the set value.

The valueset here defaults to the Software Delivery tab of the Computer Properties dialog.

Default: False, <locally managed>

RAC: Set SD agent to golden template mode

Allows the agent to distinguish between running on a golden template or a clone. If True, the agent runs on a golden template.

Note: This policy is mandatory and preset by the VMware View integration scripts.

Default: False, <locally managed>

RAC: Username to access the instance software state database

Specifies the name of the user with access permissions to the instance software state database. The user name must be formatted as: (*domainname* | local\)'user'. The string is encrypted. If specified, the agent uses these credentials to access the network share.

We recommend that you encrypt the user name first using the "sd_acmd encrypt" command. Then provide the encrypted user name as one of the parameters when running the Compose.bat script, which in turn sets the configuration parameter.

Alternatively, if the user name for the share location is the same for all desktop pools to be created from a particular golden template snapshot, you can optionally set the user name in the configuration policy. Then apply the policy to the golden template and the cloned virtual desktops.

Note: By default, when a folder is shared its permissions include only the "Everyone" group with Read access permissions. To ensure that the instance software state database gets saved over a network, the network share must also include the user here in the Share Permissions tab with Full Control (WRITE) access.

Default: empty, <locally managed>

General (CAF) Policy Group

The General (CAF) policy group includes the following configuration policies.

CAF: Pre-initialisation Script

Specifies the script that you want to execute when caf starts up and is starting initialization. The script is executed before the UUID is checked and before any plugins are started.

CAF: Post-initialisation Script

Specifies the script that you want to execute after caf initializes. The script is executed after all plugins have started but before their first registration.

CAF: Pre-initialisation Script timeout (s)

Specifies the time in seconds for which caf waits before terminating the pre-initialisation script.

CAF: Post-initialisation Script timeout (s)

Specifies the time in seconds for which caf waits before terminating the post-initialisation script.

CAF: enable registration on startup

Specifies whether the common application framework (CAF) registers immediately with the domain manager on startup.

Default: True

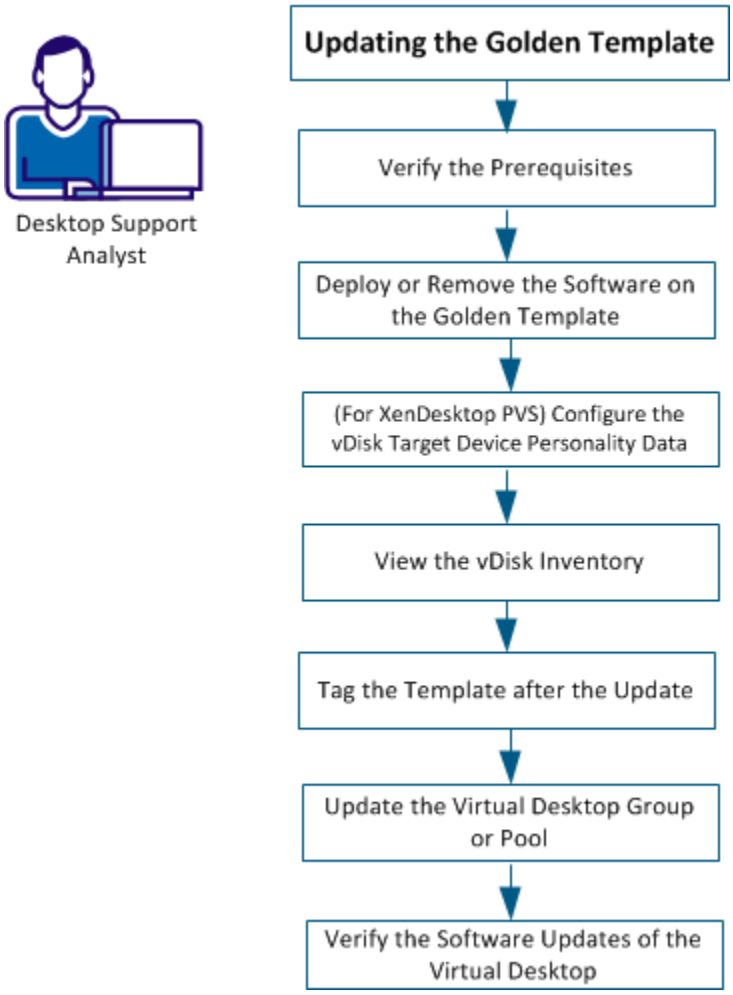
Important! This policy must be made locally managed before the installation of the CA DSM Agent add-on - VDI Support - Windows ENU package. Right-click the policy and select Locally Managed from the context menu.

Note: This Policy is applicable only for Vmware View based virtual desktops and if using CA DSM Agent add-on - VDI Support - Windows ENU package of Pre-R12.5Sp1 Feature pack1.

Updating the Golden Template

As a desktop support analyst, your responsibilities include updating the golden templates when you want to add or remove software packages from the golden template. Updating the golden templates updates the VMware View Clone, Citrix PVS streamed virtual desktop, or MCS-based virtual desktop.

The following diagram illustrates the steps that you perform to update the golden template:



Perform the following tasks to update the golden template:

1. Verify the Prerequisites (see page 295)
2. Deploy the Software to the Golden Template (see page 295)
3. Configure the vDisk Target Device Personality Data (see page 296)
4. View the vDisk Inventory (see page 297)
5. Tag the Template after the Update (see page 299)
6. Update the Virtual Desktop Group or Pool (see page 299)
7. Verify the Software Updates of the Virtual Desktop (see page 300)

Verify Prerequisites

To update the golden template, verify the following prerequisites:

- Verify that you have already prepared and deployed one or more golden templates.
- Verify that the virtual desktop agent is installed on the golden template computer.

  Note: A sound working knowledge of virtual desktop solutions such as VMware View and Citrix XenDesktop is required for this scenario.
- Verify that the Citrix PVS target device is installed if you want to create Citrix vDisk-based virtual desktops.

Deploy or Remove Software on the Golden Template

You can deploy or remove software packages from the golden template in one of the following ways:

- Do the changes directly on the golden template computer. This method is applicable for VMware View and Citrix MCS which are snapshot-based.

- Update a vDisk that is created from the golden template. This method is applicable for Citrix XenDesktop virtual desktops that are streamed by Citrix provisioning services. The following considerations apply:
  - The vDisk must be booted in private mode to a computer that has the same configuration as the golden template computer.
  - The target device that is used to boot the vDisk in private mode in the Citrix Provisioning server is assigned with personality data to indicate that the vDisk is booted for template management. For more information about Personality data, see Configure the vDisk Target Device Personality Data (see page 296).
  - When you boot the vDisk in private mode for the first time, the vDisk is added as a managed entity in CA ITCM. You can then deploy or remove packages from the vDisk using software delivery.
  - The vDisk appears as a computer record under the DSM Explorer, All Computers with the following naming convention:

    <FarmName>-<StoreName>-<vDiskName>

    If the computer record is not found in the DSM explorer, see The vDisk Record Is Not Found in the DSM Explorer.
  - The same computer record is used for the vDisk anytime you boot the vDisk in private mode on any computer for template management.
  - If the computer hosting the vDisk in private mode is already a managed computer in CA ITCM, the software deployments are only done on the vDisk and not on the computer.

    Note: When the computer is booted with the vDisk in private mode, all the software jobs wait until the computer boots with the local drive.

Note: Also, you can update the golden template itself, create a vDisk out of it, or override an existing vDisk for updating the virtual desktops.

(For Xendesktop PVS) Configure the vDisk Target Device Personality Data

Configure the vDisk target device personality data in the Provisioning Server console so that CA ITCM can treat the vDisk booted in the private mode as a golden template.

Follow these steps:

1. Open the Properties dialog of the Target Device in Citrix Provisioning Services Console to which the vDisk is assigned.
2. Click the Personality tab and add the following parameters:

   CA_DSM_GoldenTemplate

   Indicates whether the vDisk is a golden template or a virtual desktop in private mode. Set the value of this parameter as True.

   ProvisioningServer

   Specifies the IP address or host name of the provisioning server.

   ProvisioningServicesUser

   Specifies the user name that has access to the provisioning services farm or the user who is specified while connecting to the provisioning server console. Encrypt the user name using the sd_acmd encrypt command and pass the encrypted value.

   ProvisioningServicesPassword

   Specifies the password of the provisioning services user. Encrypt the password using the sd_acmd encrypt command and pass the encrypted value.

   ProvisioningServerPort

   Specifies the port of the provisioning server where the SOAP service runs. The default value is 54321.

   Note: Pass the provisioning server parameters as user parameters in the CA DSM Agent VDI Support Add-On Package while pushing Install Template Mode to the golden template. Use the following format:

   ```
   /pvsserver:<server IP/Name> /pvsuser:<encrypted username> /pvspwd:<encrypted pwd> /portno:<portno>
   ```

3. Save the changes.

   The vDisk target device personality data is configured as a golden template.

View the vDisk Inventory

After you boot the vDisk in private mode, it is added as a managed entity in CA ITCM. Here is an example for Citrix XenDesktop.

Follow these steps: (in DSM Explorer):

1. Navigate to the Computers and Users, All Computers, *vDisk_name,* Inventory, Operating System node.

   vDisk_name

   Specifies the vDisk name in the *FarmName-StoreName-vDisk.Name* format.

2. Select the Template Settings subfolder to view the values for the following attributes:

   IsGoldenTemplate

   Indicates whether an agent is a golden template (True) or a virtual desktop (False). The value is set to true when a master vDisk or clone of a master vDisk is booted in private mode for template management.

   TemplateHostUUID

   Specifies the host UUID of the golden template. For a master vDisk, the hostuuid is golden template and master vDisk for cloned vDisk.

   For more information, see How vDisk Clones are Handled. (see page 301)

   TemplateName

   Specifies the name of the golden template.

   TemplateTag

   Indicates the date and time at which the golden template was last tagged.

3. Click the Template History node to view the template history for the vDisk. You can see the history of updates to the golden template.
4. Click Virtualization, Citrix XenvDisks.

   The farm, store, and site of the vDisk is displayed.

Follow these steps: (in Web Console)

1. Navigate to the Computers, Inventory, Discovered Inventory, and click Operating System.
2. Click Template Settings under the More Details tab to view the values of the IsGoldenTemplate, TemplateName, TemplateTag, and TemplateHostUUID attributes.
3. Click Template History under the More Details tab to view the template history.

You have reviewed the relationship information and template history.

Tag the Template after the Update

Tagging helps you track the version of the template that is used by the virtual desktops. Tag the template to generate a template tag and associate the clones with their parent golden template.

Follow these steps:

1. Drag-and-drop the Tag Template procedure from the CA DSM Agent add-on VDI Package to the golden template on DSM Explorer.
2. Do *one* of the following actions depending on the virtual desktop solution:
   - (For XenDesktop based on Citrix PVS) Shut down the machine, so that the updates are saved to the vDisk.
   - (For VMware View and Citrix MCS) Shut down the virtual machine and create a snapshot.

     This action associates the snapshot with the template tag.

Update the Virtual Desktop Group or Pool

Update the virtual desktop group or pool that uses the golden template that you updated. For more information about updating the virtual desktop group or pool, see VMware View or Citrix XenDesktop documentation. After the virtual desktop group or pool is updated, the golden template updates are propagated to the virtual desktops on the next reboot.

Assign the updated vDisk or the snapshot to virtual desktops to propagate the golden template updates on the next reboot.

Follow these steps: (for VMware View)

1. Shut down the golden template.
2. Take a snapshot of the golden template.
3. Perform a pool recompose operation using the new snapshot.

Follow these steps: (for Vdisk based Virtual Desktops)

1. Shut down the vDisk computer.
2. Remove the vDisk assignment from the computer.
3. Change the vDisk mode to standard or differential.
4. Assign the updated vDisk to virtual desktops.
5. Restart the virtual desktops; otherwise, the changes take effect whenever the virtual desktops restart.

   Note: Alternately, the updated vDisk can be assigned to the virtual desktops using either the automatic or the Citrix provisioning services incremental vDisk update feature.

Follow these steps: (for MCS-based Virtual Desktops)

1. Shut down the golden template.
2. Take a snapshot of the golden template.
3. Update the Pooled catalog with the new snapshot.

Verify the Software Updates of the Virtual Desktop

View the virtual desktop software to verify whether the updates you made to the golden template are available on virtual desktops.

Follow these steps:

1. Navigate to the Computers and Users, All Computers, *Virtual-Desktop,* Software, Installed Packages node.

   In the right pane, verify whether the changes you made to the golden template or vDisk are reflected in the virtual desktop.

The updates to the golden template are complete.

Managing the vDisks and the vDisk Clones

As a desktop support analyst, you must understand how CA ITCM handles and manages the relationship between the vDisk and its clones.

This scenario describes how CA ITCM handles the vDisks and clones.

How vDisk Clones are Handled

You can copy or clone the vDisks to provision virtual desktops. vDisk copies or clones and their parent vDisk appear as separate management records in the MDB. The comstore values of the provisioning server farm, store, site, vDisk name differentiate a parent vDisk from that of a cloned vDisk.

CA ITCM uses the following rules to identify vDisk clones and create a separate management record for them:

- A new management record is created in CA ITCM and the agent name is in the *FarmName-StoreName-vDisk* format, when a vDisk is booted in private mode for template management.
- A new management record is created for the clone, when a vDisk clone is booted in private mode for template management from a different farm.
- A new management record is created for the vDisk copy, when the clone is booted from the same farm and a different store, and vDisk and its parent name are different.
- A new management record is created for the vDisk copy on the following rule:
  - The clone vDisk is booted from the same farm and a different store
  - vDisk and its parent name are same
  - The site from which the vDisk is booted for template management and its parent are different

    Note: If the site is same as the parent vdisk, Administrator is prompted to verify whether to create a management record in the MDB or reuse the existing one.
- A new management record is created on the following rule:
  - The farm and store are same
  - vDisk name changes
  - The parent vDisk is part of the store
  - vDisk is booted as a copy

    Note: If the Parent vdisk is not part of the store, Administrator is prompted to verify whether to create a management record in the MDB or reuse the existing one.
- An existing managed computer record is reused, when the vDisk, farm and store names are same.

View Relationship Between Golden Template, Master vDisk, and Clones

To identify the vDisk from which a particular vDisk has been derived, CA ITCM collects the inventory under Template settings and template history.

Using this inventory information, you can ascertain the immediate parent of a particular vDisk and history of changes that are made to a vDisk. The relationship is identified as follows:

- A master vDisk points to the golden template as a parent.
- If you created a clone from a master vDisk after booting the master vDisk in private mode, the clone points to the master vDisk as its parent.
- If you created a clone from a master vDisk before booting the master vDisk in private mode, the clone is the same as the master vDisk and it points to the golden template as parent. If further clones are created from such vDisk clones of the master vDisk, all the clones point to the golden template as its parent.

Follow these steps: (in DSM Explorer)

1. Navigate to the Computers and Users, All Computers, vDisk_name, Inventory, Operating System folder.
2. Select the Template Settings subfolder to view the values for the following attributes:

   IsGoldenTemplate

   Indicates whether the agent in question is a golden template (True) or a virtual desktop (False). The value is true for the master vDisk and its clones.

   TemplateHostUUID

   Specifies the host UUID of the golden template. For a master vDisk, the host UUID of the golden template is displayed. For cloned vDisks, the host UUID differs depending on the following factors:

   - If the clone was created after the master vDisk was booted in private mode, the host UUID of the master vDisk is displayed.
   - If the clone was created before the master vDisk was booted in private mode, the host UUID of the golden template system is displayed.

   TemplateName

   Specifies the name of the golden template.

   TemplateTag

   Indicates the date and timestamp of the template for the golden template or vDisk only if the template has been tagged.
3. Select the Template History subfolder to view the template history for the virtual desktop or the templates, providing that the templates have been tagged.

Follow these steps: (in Web Console)

1. Navigate to the Computers, Inventory, Discovered Inventory page.
2. Click the Operating System tab to view the value of the Virtual Machine attribute.
3. Click Template Settings under the More Details tab to view the values of the IsGoldenTemplate, TemplateName, TemplateTag, and TemplateHostUUID attributes.
4. Click Template History under the More Details tab to view the template history for the clone.

   You have reviewed the relationship information and template history.

Managing the Virtual Desktops from CA ITCM

As a desktop support analyst, your responsibilities include managing virtual desktops from CA ITCM. Managing virtual desktops include deploying software or patches to the virtual desktops and collecting inventory from them. You must also be aware of how and when CA ITCM reinstalls the software on the desktops.

Note: Deploying software packages and collecting inventory from virtual desktops is similar to software deployment and inventory collection on any other computer in CA ITCM

Implementation Guidelines for Virtual Desktops

For software packages that are installed to individual virtual desktops rather than to the golden template, you must consider the following limitations and guidelines:

- Packages that are not staged in the software library of the scalability server to which the agent is registered are not reinstalled.
- Reinstall is not supported for added procedures with new files.
- Reinstall is not supported for the User Profiles agent, only the Computer agent.
- When a virtual desktop is checked out using VMware View's Offline Desktop feature and rolled back (that is, checkout is discarded), any changes to the software state remain in the instance software database. When Offline RAC is performed, the software is reinstalled because it was recorded in the state database and not removed during rollback. Therefore, the software must be uninstalled manually if you do not want it.
- Sending software delivery jobs with reboot/logoff/shutdown options enabled is not supported for nonpersistent virtual desktops. A nonpersistent desktop is tied to a user only for as long as the user is logged on. The next time the user logs on, the user can be allocated to a different desktop. Hence, these options are not logical for this case.

- Packages that take a long time to transfer over the network or that take a long time to install must be installed to the golden template rather than to the individual virtual desktop. If not, the reinstallation time becomes unacceptable.
- Virtualized applications can be pre-staged on the golden template and later provisioned to individual virtual desktops using standalone installation. This way your network bandwidth usage is minimized during recompose/refresh and during use.
- A result similar to the previous item can be achieved using managed package formats like SXP, PIF and MSI with some research and possibly some tweaking. For example, SXP provides a user filter that allows the package to be installed to the golden template. However, the filter is only made available to users of the clones that belong to specific local or active directory user groups.
- Virtualized applications must be provisioned to individual virtual desktops in streaming mode. This way network bandwidth usage can be minimized during recompose/refresh, but not during use.
- Applications that store their configuration outside of the redirected user profile/folders do not automatically preserve their configuration after reinstall. Applications that reset their configuration rather than inheriting it as part of install also suffer from this issue.
- If both the template software state database and the instance software state database contain records of the same software but of different versions, the upgrade or downgrade is still performed by the Offline RAC. The administrator is responsible for configuring the system accordingly and preventing such a case, especially in downgrade scenarios.
- DTS download method is not supported for the virtual desktop agent.
- For nonpersistent desktop pools, reinstallations are only done when a user logs on. When the user logs off a cloned desktop that is part of a nonpersistent desktop pool created with the "Power off and delete virtual machine after first use" option selected in VMware View 4.0, then the cloned desktop is in the Locked by RAC state until a user logs on again. For VMware View 4.5, the equivalent situation occurs when the "Delete or refresh desktop on logoff" option is set to "Refresh Immediately" or "Delete Immediately." Therefore, we recommend that any critical patches be deployed as part of the golden template instead of deploying them as a part of the clone.
- We recommend that you disable the user profile mode for software delivery functionality in the case of linked clone virtual desktops.

  User profiles are not needed here because there is a one-to-one relationship between the user and the virtual desktop. Enablement of user profiles causes additional communication between the agent and scalability server, which can affect overall scalability.

Offline RAC

Offline RAC is a reinstall after crash (RAC) task that is driven by the agent rather than by the manager. Virtual desktops are *recomposed* frequently, that is, whenever the golden template is updated and the disk is reset, any changes to the virtual desktop since the previous reset are effectively voided. For virtual desktops, the agent and not the manager is responsible for the creation of the RAC job container. When the disk reset occurs, the agent initiates an Offline RAC to restore any software that has been deployed to the agent.

For Offline RAC, the software delivery agent contains a file system-based software state database. This database contains the following information about each installed software package:

- The procedure used to install the software
- Any post-installation activation or configuration procedures for the computer target of the agent only.
- Any job-specific information such as user parameters.

This software state database is maintained by the software delivery agent and updated each time a software job is executed. If an uninstallation is successful, the records for that particular software package are removed. If enabled, the software state database always reflects the current software delivery state of the agent.

The software state database also inherits the installation history of the golden template on which the virtual desktop is based. The software state database is split into two parts, one for golden template use and one for cloned instance use. The template part of the software state database is stored on the system disk of the golden template. Any software jobs targeting the golden template use this database only. When the virtual desktop is cloned, its agent only uses the instance software state database to track its state.

Because the system disk of a cloned virtual desktop is destroyed during a recompose or refresh operation, the instance software state database cannot be stored there. This database must be stored in a different location, controlled by common configuration policy, for example, either in the user data disk of a VMware View linked clone or on a file server accessible from the virtual desktop.

Important! Administrators must ensure that the software state database is always accessible during the standard software job management and while performing offline installation, when the instance software database is on a network share.

More information:

Agent (Software Delivery) Policy Group (see page 288)

Status of Reinstallation

At the end of the reinstallation process, the success or failure of each job is reported to the domain manager. The status is also visible in the agent's Software Delivery Job Check dialog when the offline reinstallation is on-going.

If a job fails, or if some jobs cannot run due to other settings like Exclude From RAC, the Software Delivery Job Check dialog is configured to remain open until the user closes it explicitly. This software delivery agent RAC policy is configurable and can be turned off. Also, in the case of a failure to initiate offline reinstallation, such as in the case of an invalid download method or an attempt to report to a legacy scalability server, this failure is reported in the Software Delivery Job Check dialog. Additionally, if the scalability server is not accessible due to various reasons, the end user is provided with options to retry, postpone, or abort the reinstallation.

Computer Properties

The RAC policy setting of the agent policy, defaults to the Software Delivery tab of the Computer Properties dialog. The RAC policy field is disabled when the agent policy is set to True, and you cannot change the setting.

The DTS download method is not supported for virtual desktops during Offline RAC. Therefore, this option is not displayed in the Download method drop-down list.

Unlock a Virtual Machine

After the agent reinstalls the software, it sends an Offline RAC completed notification to the scalability server which in turn sends it to the manager. After the manager receives this notification, it unlocks the virtual machine from Offline RAC.

However, if the agent reinstalled the software but was unable to send the Offline RAC completed notification to the scalability server, then you can forcibly unlock the virtual machine. For example, if the agent cannot send the notification if the server was not available at that moment, you can unlock the virtual machine.

Follow these steps:

1. In the DSM Explorer, navigate to the Computers and Users, All Computers folder.
2. Right-click the relevant asset in the corresponding All Computers pane.
3. Select the Clear pending RAC lock command from the context menu that appears.

   Note: This new command is available only if the SD Status column indicates that one or more virtual machines is Locked by RAC. Otherwise, the command is disabled. Furthermore, this command is not enabled for any regular computer that goes into a Locked by RAC state.

   The selected asset is unlocked.

Deleting the Virtual Machine from DSM Explorer

If a golden template is moved from one domain manager to another after the clones are created, the golden template is moved according to standard move functionality. However, if clones created from this golden template are recomposed, the clones automatically report to the new domain manager. Therefore, nothing needs to be moved for a recomposed clone because all of its installation history is recreated using Offline RAC.

To clean up the obsolete clones, which used to report to but are no longer managed by the previous domain manager, manually delete all the moved clones from that manager after the recompose of the clones of the golden template.

Also, if the naming pattern is changed and a particular virtual machine is deleted using VMware View, then a new virtual machine is created with a new name. In this case, manually delete the virtual machine from the DSM Explorer.

Software Procedures

The software delivery system currently lets you enable or disable RAC for individual software procedures. If you do not want an item procedure to execute as part of the RAC process, you select the Exclude from RAC option in the Properties dialog of the actual procedure. This option enables you to exclude obsolete packages or patches from RAC.

The Exclude From RAC functionality has been expanded to support Offline RAC. During offline reinstallation, the Exclude from RAC setting in the Properties dialog is checked for each software procedure, and the procedure is not run if the procedure is excluded.

An example is where an individual patch may be necessary to resolve a critical security issue involving your virtual desktops without having to recompose them. However, once recomposed, the new version of the golden template has all the patches applied and reinstalling that patch is unnecessary.

Applying Security Patches on Virtual Desktops

To trigger software reinstallation on virtual desktops that do not persist changes after the user logout or reboot, CA ITCM performs the offline RAC process. When the user logs in the virtual desktop next time, offline RAC reinstalls the software and patches that the user had installed before a logout or reboot.

(Optional) Configure Patch Manager to Handle Patch Deployment During RAC or on Recomposable Virtual Desktops

By default, patch deployment is excluded during RAC because the patches are redeployed without considering the order of supersedes and rollouts. This behavior can lead to an unexpected outcome. Similarly, blacklisted targets are also excluded during patch deployment.

Recomposable virtual desktops are part of the blacklisted computers by default. The default settings for excluding from RAC and Ignoring blacklisted computers are ideal to handle patch deployment. You can change the settings to modify the default behavior.

Follow these steps:

1. Log in to CA Patch Manager.
2. Navigate to Administration, Configuration, System Settings, DSM, Options.

   The configuration options are displayed.
3. Modify the following parameters as required:

   Exclude From RAC

   Excludes the patch deployment during an RAC process. Clear this option to deploy patches during RAC. The patches are redeployed without considering the order of supersedes and rollouts and hence can lead to an unexpected outcome.

   Ignore Blacklisted computers in Deployment

   Specifies the default option when blacklisted targets are added to the selected targets list during patch deployment. Clear this option to include the selected blacklisted targets for patch deployment. You can also change this option for individual deployments. To ignore blacklisted targets always unless mentioned, keep this option selected.

   Ignore Blacklisted computers in Policies

   Specifies that the blacklisted targets must be ignored during policy evaluation. Selecting this option adds the UPM-Blacklisted query to the UPM policy queries.

   A Black List Query retrieves a list of computers that are excluded from patch deployment. By default, the blacklistQuery parameter is set to UPM–Blacklisted Computers query. This query is linked to a query named Recomposable Computers, which retrieve recomposable desktops that are based on an inventory item. The inventory item IsRecomposable is under Inventory, Operating System, Template Settings. In addition to the recomposable desktops, you can also include computers to the UPM–Blacklisted Computers or create a query to exclude such computers. Verify that the new query includes the query named Recomposable Computers. If you create a query for blacklisted computers, specify the name of the query in the Black List Query parameter.

   Note: To update the existing UPM policies and packages automatically, verify that you have upgraded them. For more information about the upgrade, see Upgrade Patch Manager Packages and Policies.
4. Save the settings.

   Patch management is configured to handle RAC and blacklisted computers during patch deployment.

Apply the Patch on vDisk or Golden Template

Applying the security patches on vDisk or golden template ensures all the virtual desktops have the necessary security patches installed. To apply the patch on vDisk or golden template, follow the process given in the Updating the Golden Template scenario.

Apply the Patch on Blacklisted Targets or Recomposable Desktops

By default, recomposable desktops are part of the blacklisted targets and all the blacklisted targets are excluded from patch deployment. However, you can apply the patch on blacklisted targets when there is a requirement.

Follow these steps:

1. Log in to CA Patch Manager and click the patch that you want to apply on the blacklisted targets.
2. Click Deploy Patch in the Patch Details page.
3. Select the group that contains blacklisted targets or select individual blacklisted targets and add them to the adjacent Selected Targets pane.

   The list of blacklisted targets in the selected group or targets are displayed in the Blacklisted Targets pane.
4. Select the targets on which you want to apply the patch from the Blacklisted Targets pane. Add these targets to the adjacent Selected Targets pane. Click Next.
5. Specify the deployment schedule. Click Next.
6. Clear the Ignore Blacklisted computers in Deployment option. Click Finish.

   The patch deployment on the selected targets begins at the scheduled time.

View VDI Inventory

Inventory information is collected for both the golden template and the virtual desktops with different values that reveal whether a virtual desktop is a template or a clone.

Follow these steps:

1. Navigate to the Computers and Users, All Computers, Computer Name, Inventory, Operating System node in DSM Explorer.

   Displays the Operating System pane.

2. Verify the value of the Virtual Machine attribute.

   Specifies whether the computer is a virtual machine or not.

3. Select Template Settings.

   Shows the following attributes:

   IsGoldenTemplate

   Specifies whether a virtual machine is a golden template (True) or a clone (False).

   Recomposable

   Specifies whether a virtual desktop is recomposable or not.

   TemplateHostUUID

   (Clones only) Specifies the host UUID of the golden template.

   TemplateName

   (Clones only) Specifies the name of the golden template.

   TemplateTag

   (Clones only) Specifies the date and time of the tagged template snapshot.

4. Select Template History

   Shows the template history for the clone if the snapshots is tagged.

5. To view the collected Virtualization Inventory navigate to Computers and Users, All Computers, Computer Name, Inventory, Virtualization node.

   Displays the desktop virtualization technology that the computer uses.

6. Expand the Virtualization node, and select the following:

   VM Ware View

   Shows the Pool name and Agent version.

   Citrix XenDesktop Configuration

   Displays the Citrix Farm, Group, Licensing and Product information.

Note: Like any other inventory data, you can use the virtualization inventory to create queries and reports.

Queries and Reporting

To support querying and reporting on the template desktops, in addition to individual desktops based on those templates, the basic hardware inventory has been extended with the following attributes and values:

Is Golden Template

Boolean

Based on Template Name

String

Based on Template Version

Integer

Based on Template Host UUID

String

These attributes are displayed on the All Computers, *computername*, Inventory, Operating System pane in the DSM Explorer.

Query Designer Changes

When creating a query, you now have additional arguments for reporting on computers with a status of Offline RAC. Additionally, predefined queries have been added for VDI Support.

- For computer-based queries, a value of Offline has been added to the RAC Policy drop-down list in the Select field dialog of the query designer.
- Two predefined VDI Support queries, All Golden Templates and All Clones of Golden Templates, have been added to the Queries node in the DSM Explorer.

DSM Reporter Changes

The following predefined report templates for VDI Support have been added to the DSM Reporter:

- All Golden Templates
- All Clones of Golden Templates

After a report template is run and inventory collected, these reports list all discovered golden templates and their corresponding virtual desktops.

Obsolete Assets Wizard Excludes Golden Images

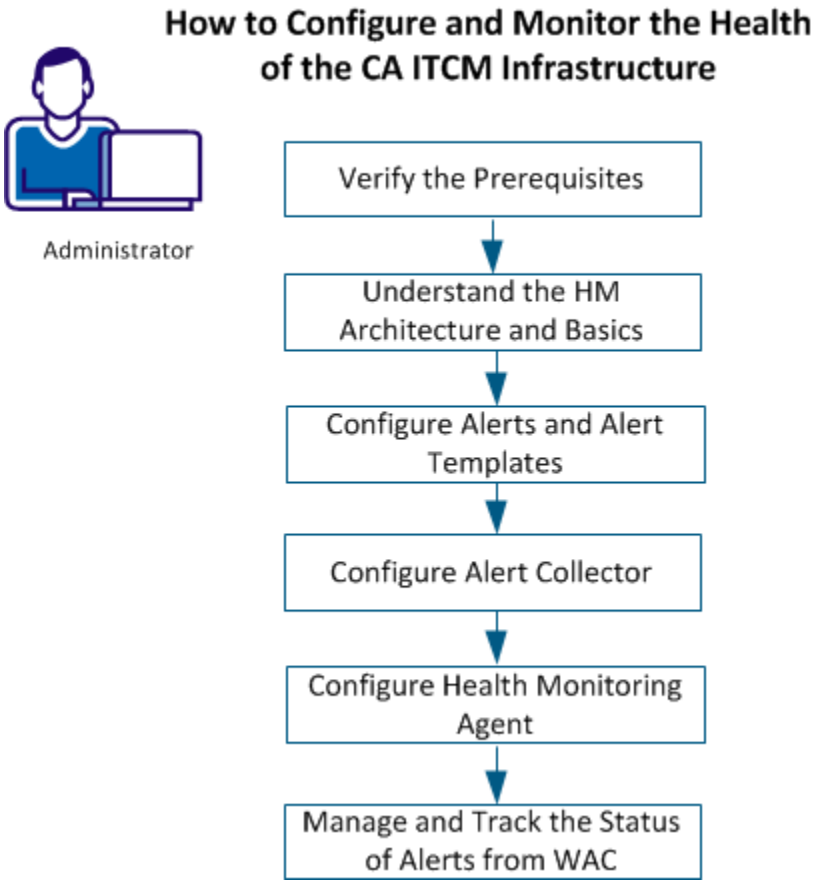
The Obsolete Assets wizard helps you track and optionally remove old and unused computers and users. Because golden templates are logically different from regular computers and their users, they have been excluded from the result sets of the obsolete asset queries generated by the wizard. Any obsolete asset query created using a previous release of CA IT Client Manager does not exclude golden templates and their associated users. Therefore, replace any existing obsolete asset queries to ensure that golden templates are excluded from the result sets.

Chapter 9: How to Configure and Monitor the CA ITCM Infrastructure Health

As an administrator, your responsibilities include managing the health of CA ITCM components. The Health Monitoring (HM) feature provides a health inspection mechanism to:

- Define CA ITCM health conditions
- Monitor the infrastructure periodically
- Raise an alert when a defined condition is detected
- Notify the administrator by sending an email, raising an SNMP trap, and writing to Windows/CCS event logs.

Use the HM feature to improve the CA ITCM availability and resiliency. The following Illustration summarizes the HM process:



You can accomplish the following tasks:

Configure Alerts

Configure the available alerts or define new alerts.

Configure Alert Actions

Configure alert actions such as sending emails, raising SNMP traps, writing to the system, and writing to the CCS event log.

Manage Alerts

View, track, follow up, and clear alerts from WAC.

This section contains the following topics:

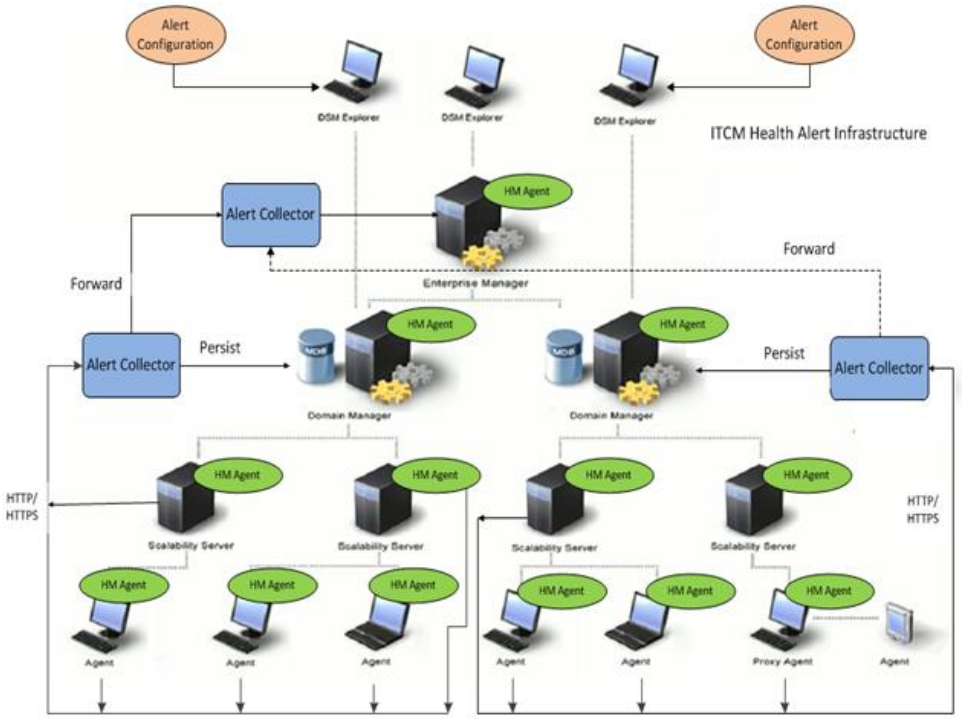
Verify the Prerequisites

Before you configure and monitor the HM alerts, ensure that you:

- Have a working knowledge of the CA ITCM infrastructure
- Understand the HM architecture and basics
- Upgrade the existing infrastructure with CA ITCM Release 12.8
- Install the Alert Collector.

Understand HM Architecture and Basics

The following diagram shows the components of the HM feature and how they interact to monitor the health of CA ITCM:



For more information about the HM basics, see

- Alerts and Alert Templates (see page 318)
- Health Monitoring Components (see page 319)
- External Process Manager (CAF Plug-in) (see page 321)

Alerts and Alert Templates

The HM feature monitors the following alert types:

Parameterized Alerts (Alert Templates):

Supports additional parameters as part of the alert definition. You can customize alert properties such as the monitoring frequency, threshold, and severity based on the values that are set for those parameters. Defining and configuring the parameterized alerts is supported through Alert Templates.

An alert template provides a default definition of a parameterized alert with a list of supported parameters. Use the template as the basis for one or more alerts with different parameter values and associated configurations.

Non-parameterized or Plain Alerts (Alerts):

Supports no additional parameters. Use the alert properties as defined in the system.

The HM feature provides out-of-the-box alert templates and alerts. You can also base customized templates and alerts on DM Script. For a list of Alerts and Alert Templates, see the user interface.

Health Monitoring Components

The HM feature introduces the following components:

HM Agent:

A persistent module that is installed with the common agent and resides on all the tiers of the CA ITCM infrastructure.

- Interprets the alert configuration on the agents, periodically monitors the occurrence of the alert conditions, and notifies the administrator on detecting the health conditions.

  Note: Alert monitoring is disabled by default. To enable health monitoring, apply a configuration policy.

- Provides the following command-line options for interaction:

  `hmagent start`

  Starts the HM agent.

  `hmagent stop`

  Stops the HM agent.

  `hmagent status`

  Displays whether the agent is running and health monitoring is enabled.

- The HM agent is a service on Windows platforms and a daemon on Linux and UNIX platforms.

Alert Collector:

Alert Collector comprises the following modules:

Web Module

Receives the alerts from the HM agent and copies them to a configured folder.

Persistent Module

Monitors the configured folder and processes new alerts according to the configured alert collector role. For more information, see Configure Alert Collector (see page 330).

The alert collector has the following requirements:

- The alert collector is only supported on Windows.
- IIS installation is a prerequisite.
- Ensure that the ISAPI extensions and ISAPI filters available under the Application Development option are installed.
- Depending on the DB type to which the alert collector persists the alerts, 32-bit SQL or the Oracle client must be installed.

The web module application hosts HM web services on IIS. This web service is independent of the existing CA ITCM web services functionality and runs in a separate application pool.

The administrator can start, stop, and query the status of the alert collector process from the supported command line. Alert Collector supports the command line options similar to the HM agent.

Alerts on WAC:

DSM Explorer displays a notification when new alerts are raised. The notification contains a hyperlink that launches WAC and navigates to the Alerts page when the unified login is enabled for WAC. If the unified login is not enabled, enter the appropriate user credentials to navigate to the alerts page.

External Process Manager (CAF Plug-in)

This plug-in (named cfProcessManager) manages external processes such as HM Agent and Alert Collector. The plug-in functionality is similar to CAF, where CAF manages the CA ITCM-conformant plug-ins but Process Manager manages external processes that are not CAF plug-ins.

The external processes that cfProcessManager manages support the regular CAF plug-in properties such as *Maxinstances, Maxrestarts, Restartifdied, Enabled,* and *Maxrestarttime.* The behavior of these properties is similar to that of CAF plug-ins.

The following additional properties are supported:

Startwithcaf

Defines the process to start when CAF starts.

Default: Do not start with CAF.

Stopwithcaf

Defines the process to stop when CAF stops.

Default: Do not stop with CAF.

Commandline

Indicates Command line of the process.

Startcmd

Defines the start command. Default: start.

Stopcmd

Defines the stop command. Default: stop.

Statuscmd

Defines the status command. Default: status.

Note: Restart cfProcessManager when you change the above settings.

A new */EXT* option is introduced to work with the CAF start and stop commands.

Caf start /EXT

Starts all plug-ins and the enabled external processes that Process Manager manages.

Caf stop /EXT

Stops all plug-ins and the enabled external processes that Process Manager manages.

The **Caf status cfProcessManager** command shows the status of the external processes.

Configure Alerts and Alert Templates

You can monitor the health of CA ITCM components like DM, EM, SS, and Agent. Create an alert or alert template specifying severity, threshold, and frequency values.

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, DSM, Health Monitoring, and Alert Configuration.
2. Configure the following entities:

   Alerts

   Configures the alert parameters such as frequency, threshold, severity of the predefined alerts, and create alerts based on templates or create DM script-based alerts.

   Alert Templates

   Configures the parameters of the pre-defined alert templates and create templates based on DM script.

An alert or alert template is now defined.

Configure Alerts

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, DSM, Health Monitoring, Alert Configuration, and Alerts**.**
2. Select Add to create an alert based on a template or a script.
3. Specify suitable values for the following fields:

   Alert Name

   Specifies the name of the alert.

   Template

   Specifies the alert template name from which the alert is derived.

   Note: Select a template from the drop-down list to create a template-based alert. For example, Asset Jobs not Updated.

   Script

   Specifies the script name for script-based alerts.

   Parameters

   Specifies the parameters suitable to the alert.

   Note: When the alert is derived from a template, the template parameters are carried over from the template. For example,
   `GROUPS=ComputerGroups;RequiredPercentage=MINPERCENT;IncludeLinkedAssetJobs=TRUE;IncludeLinkedGroupJobs=TRUE;assetJobNames=%`

   Note: You can also specify parameters for script-based alerts.

   Message

   Defines the alert-related information that is evaluated when an alert condition is detected. This evaluated information is passed as part of the alert raised by HM Agent. For example,
   `Less than $PERCENTAGE of the computers reported the asset job results from within the computer group $GROUPS`

Severity

Configures the severity of the alert from the drop-down list.

Enable

Specifies the state of the alert. When set to True, the alert is monitored by the HM agent otherwise excluded from monitoring.

Detection Tiers

Specifies the tiers on which the alert is detected. For example, EM, DM, SS, and Agent.

Note: For predefined alerts, select the tiers from the supported list. For template-based alert, select a tier from the template-supported ones.

Frequency

Specifies the interval at which the alert is monitored. You can specify the frequency in minutes, hours or days for each detected tier.

Threshold

Specifies the threshold value. This value indicates the minutes/hours/days an alert condition is present, or the number of times an alert condition occurs before raising an alert.

For example, when you configure Agent not able to communicate to SS with a frequency of one hour and a threshold of six hours on the Agent tier, the HM Agent checks every one hour to see if the agent is able to communicate to the remote scalability server. On failure to communicate for six hours, an alert is raised.

4. (Optional) Click Check to verify the values.
5. Click Apply and OK

The alert is now configured.

Create DM Script-based Alerts

You can create custom alerts based on DM Script. Deploy the script to Script Directory, which is configured at *Configuration Policy, DSM, Health Monitoring, Health Monitoring Agent, ScriptDir,* on the agent machines before applying the configuration related to these alerts.

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, DSM, Health Monitoring, Alert Configuration, and Alerts**.**
2. Select Add to create an alert based on a script and leave the template name field empty.
3. Specify the DM script name that is deployed to the agent machines.
4. Specify the parameters in the Parameters fields.
5. In the message field, add any text related to the alert (have parameters if needed).
6. Set other alert parameters and apply to the agents for monitoring.

DM Script Alert Example:

The following DM script reports the presence or absence of alert condition to the HM agent by invoking hmAlertOPFormatter. For example,

```
'Do your alert condition checking here.
'...
' At bottom of your DM script, execute hmAlertOPFormatter
' to create the alert XML output.
dim ret as integer
ret = Exec("hmAlertOPFormatter.exe alertconditionexist=1 raisealertnow=1
""param1=" + argv(1)  + ",param2=" + argv(2) + """ additionalinfo=this is some
additional text for script with Args", true)
print "hmAlertOPFormatter.exe: " + str(ret)
```

To create an XML file for HM Agent to process when invoked for monitoring alerts, execute the following command in the DM script:

hmAlertOPFormatter executable

```
hmAlertOPFormatter.exe alertconditionexist=0|1 [raisealertnow=0|1]
[PARAM1=data1,PARAM2=data2,..,PARAMX=datax] [additional info=Additional Info]
```

`alertconditionexist=0|1`

Use value 0 when your DM script has not determined any alert condition. Use value 1 when your script has determined an alert condition.

`raisealertnow=0|1`

(optional) the default value is 0. Use value 1 to raise the alert immediately.

`PARAM1=data1,PARAM2=data2 .. PARAMX=datax –`

(optional) These key value pairs indicate the parameters and values in the alert message. The sequence of key value pairs is separated by a comma (,) where keys and values are separated by an equal sign (=).

`additionalinfo=<Additional Info>`

(optional) This parameter is the last one on the command line. All the rest of the command line after equal sign (=) is accumulated together as one field of resulting alert XML.

Configure Alert Templates

You can configure the alert templates.

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, DSM, Health Monitoring, Alert Configuration, and Alert Templates**.**
2. Select Add to create a script-based alert template.
3. Specify suitable values for the following fields:

   Alert Name

   Specifies the template name.

   Template

   Configures the alert template name from which the alert is derived. See

   Asset Jobs not Updated (see page 328)

   Asset Inventory not Updated during Collection from SS (see page 329)

Script

Specifies the script name. This name must be same as the script filename passed to the HM agent in *ScriptDir.*

Parameters

Specifies the parameters suitable to the template.

Note: Use name-value pairs separated by a semi-colon (;) for specifying multiple parameters, and comma (,) to separate multiple values for one parameter. For example,
`GROUPS=Group1,Group2;RequiredPercentage=80;IncludeLinkedAssetJobs=TRUE;IncludeLinkedGroupJobs=TRUE;assetJobNames=%`

Message

Defines the alert-related information, that is evaluated when an alert condition is detected. For example,
`Less than $PERCENTAGE of the computers reported the asset job results from within the computer group $GROUPS`

Severity

Configures the severity for the template alert from the drop-down list.

Detection Tiers

Specifies the tiers on which the alert is detected. For example, EM, DM, SS, and Agent.

Default Frequency

Specifies the default frequency for the template.

Default Threshold

Specifies the default threshold for the template.

4. (Optional) Click Check to verify the values.
5. Click Apply and OK

   The alert template is now configured.

Pre-defined Alert Templates

CA ITCM provides the following alert templates out-of-the-box.

Asset Jobs not Updated (see page 328)

Asset Inventory not Updated during Collection from SS (see page 329)

Asset Jobs not Updated

This template detects and alerts if a specified percentage of Asset jobs for one or more computer groups is not updated.

Parameters

This template supports the following parameters:

groups=<comma separated list of groups of interest>;

Specifies one or more computer group names separated by commas.

requiredPercentage=<Required percentage>;

Specifies the required percentage of the identified jobs within the specified groups that must be successful to avoid the alert being raised.

IncludeLinkedGroupJobs=[TRUE]|[FALSE];

TRUE

Specifies the value TRUE to include jobs that are linked to groups while identifying the jobs that must be included for verification.

FALSE

Specifies the value FALSE to ignore jobs that are linked to groups while identifying the jobs that must be included.

IncludeLinkedAssetJobs=[TRUE]|[FALSE];

TRUE

Specifies the value TRUE to include jobs that are linked to assets while identifying the jobs that must be included for verification.

FALSE

Specifies the value FALSE to ignore jobs that are linked to assets while identifying the jobs that must be included.

Note: When you do not specify *IncludeLinkedGroupJobs* or *IncludeLinkedAssetJobs* in the parameter list, the default behavior is to include the respective job link types.

assetJobNames=<comma separated list of job names>

Specifies the required job names for evaluation. When you do not specify, all the asset jobs for the specified group or groups are considered for evaluation.

Note: You can specify multiple job names with comma-separated value in the assetJobNames parameter. Use the following wild characters:

% (percentage)

Specifies a string of zero or more characters. For example, title LIKE %computer% finds all book titles with the word *computer.*

_ (underscore)

Specifies a single character. For example, *_ean* finds all four-letter first names that end with *ean.*

Example for the Parameters for Asset Jobs not Updated:

```
GROUPS=Groups1,Group2;RequiredPercentage=80;IncludeLinkedAssetJobs=TRUE;I
ncludeLinkedGroupJobs=FALSE;assetJobNames=%
```

Asset Inventory not Updated during Collection from SS

This template detects and alerts if the inventory update is not successful from one or more Scalability Servers or Scalability Server groups in a specified amount of time.

Parameters

This template supports the following parameters:

Servers=<comma separated list of scalability server>;

Specifies one or more servers separated by commas.

Note: Servers parameter requires the name of a server as listed in DSM Explorer, not the FQDN.

ServerGroups=<comma separated list of scalability server groups>;

Specifies one or more server groups separated by commas.

Note: Server Groups parameter requires the name of a group from All Scalabiltiy Servers, DSM Explorer, and not from the All Computers and Users section.

Note: When you do not specify the parameters, all the Scalability Servers are considered for evaluation.

Example for the Parameters for Asset Inventory not updated during Collection from SS**:**

```
Servers=Server1,Server2;ServerGroups=Group1,Group2
```

Configure Alert Collector

Configure Alert Collector in one of the following roles:

Persist Alerts into MDB

Configures the alert collector to persist alerts into MDB.

Persist Alerts into MDB and Take Configured Actions

Configures the collector to persist the alerts into MDB and take configured actions such as sending mails, raising SNMP trap, writing to Windows/CCS event log.

Persist Alerts, Take Configured Actions, and Forward

Configures the collector to persist the alerts into MDB, take configured actions, and forward alerts to another alert collector.

Note: You can filter the alerts that are forwarded based on the severity or detection tier. For example, only forward High, Medium severity alerts raised on the DM.

Forward

Configures the collector to forward the alerts to another alert collector.

Note: Alert Collector is not supported in a cluster environment.

For more information about Alert Collector Roles, see Install Alert Collector (see page 151).

Set Alert Collector Properties

Configuring the alert collector involves configuring both the web module and the alert collector process.

Web Module Configuration:

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, DSM, Web Services, and Health Monitoring.
2. Specify suitable values for the following options:

   Alert Upload Folder

   Specifies a folder on the alert collector machine where the alert info xml files are uploaded.

   Default: *HMAlertUploads.* This folder is relative to the CA ITCM installation folder.

   When you use non-default value, the user account, under which the web module runs, must have write permissions for the folder.

   Note: A network path for the folder location is not supported.

   Copy Files to Alert Collector

   Specify value 1 to copy the uploaded files to the input folder of the alert collector.

   Default: 1

   Delete Files after Copy to Alert Collector

   Specify value 1 to delete the alert info xml files after copying to the alert collector input folder.

   Default: 0

Web module is now configured.

Alert Collector Process Configuration:

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, Policy Name, DSM, Health Monitoring, and Alert Collector.
2. Specify suitable values for the following options:

   Alert Collector Role (Locally Managed)

   Specifies the role in which the alert collector must run. This value is initially set during the installation. Post-installation, change to a different role in one of the following ways:

   - Change the role parameter to centrally managed, set the role value, and apply to the alert collector machine.
   - Use *ccnfcmda* CLI locally on the alert collector machine to set this value and restart the alert collector process.

   Alert Info Folder

   Specifies a folder on the alert collector machine where the alert info xml files are uploaded.

   Default: AlertCollectorInput. This folder is relative to the CA ITCM installation folder.

   When you use non-default value, the user account, under which the web module runs, must have write permissions for the folder.

   Note: A network path for the folder location is not supported.

Manager (Locally Managed)

Configures the manager to which the alert collector must connect. This value is initially set during the installation. Follow the Alert Collector Role (Locally Managed) procedure to change the manager post-installation.

Output Folder

Configures the folder where alert info xml files are placed after processing by alert collector.

Default: AlertCollectorOutput. This folder is relative to the CA ITCM installation folder.

Alert Purge Maximum Age

Specifies the number of days after which the alerts are purged.

Default: 60 days

Alerts Purge Interval

Specifies the interval at which the alerts that are older than the alert purge maximum age value are deleted.

Default: 10 days

Alert Collector process is now set.

Configure Alert Actions

Configure alert actions, apply to the alert collector(s) which are configured to take the following actions:

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, Policy Name, DSM, Health Monitoring, Alert Collector, Alert Actions, and Actions Configuration.

   The alert actions dialog appears.

2. Select Add to create an action for one of the configured alerts.

3. Specify suitable values for the following items:

   Alert Name

   Defines the alert name.

   Note: You can select the alert from the list.

   Possible Actions

   Specify the following actions as required:

   Send Email

   Sends the alert information to the email address that is specified in *To Address.* When the address is not specified, mail is sent to the recipient address, specified globally in SMTP Email configuration.

   Raise SNMP Trap

   Raises SNMP traps to the IP address specified in SNMP server. When the server is not specified, traps are raised to the SNMP server, specified globally in Alert Actions.

   Write to Windows Event Log

   Writes the alert information to the windows event log.

   Write to CCS Event Log

   Writes the alert information to the CCS event log.

   To Address

   Configures the email address where you send the alert information. You may specify multiple addresses separated by semicolon.

   SNMP Server

   Configures the SNMP server where the SNMP traps are raised.

4. Click Apply and OK

   Actions for the alert are now configured.

Note: You can configure the global settings for SMTP Email and SNMP Server from Alert Actions.

SMTP Email Configuration

Configure SMTP Email with the following details:

From Address

Defines the mail address to be sent in the mail header. For example,

Default: *HealthMonitoringSystem*

Note: Do not have spaces in From Address.

Mail Server

Specifies the DNS name or IP Address of SMTP mail server.

To Address

Defines the recipient mail address. You may specify multiple addresses separated by semi colon.

Subject

Specifies the subject of the mail.

Default: *Health Monitoring Alert*

Configure SNMP server with the following details:

SNMP Server

Configures the SNMP server where the SNMP traps are raised.

Specify the Alert Forwarding Details

Apply these settings for the alert collectors which are configured in a forwarding role.

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, Policy Name, DSM, Health Monitoring, Alert Collector, Alert Forwarding.
2. Specify suitable values for the following items:

   Alert Collector Address

   Defines the host name or IP address of the alert collector server to which the alerts are forwarded.

   Alert Forwarding: Alert Detected Tier

   Specifies the tiers that are used as a filter while forwarding the alerts.

   Default: DM

   Alert Forwarding: Alert Detected Severity

   Specifies the alert severity that is used as a filter while forwarding the alerts.

   Alert Forwarding: Forward Pending Folder

   Specifies the folder in which the alert info xml files, that failed to forward for the first time, are placed.

   Alert Forwarding: Forward Rejected Folder

   Specifies the folder in which the alert info xml files that are no longer forwarded are placed.

   Retry Interval

   Specifies the time interval in minutes to re-forward the pending alerts.

   Use Https

   Specifies the use of https or plain http for connecting to the server. When set to True, https is used. To configure Alert Collector to connect through Https, see Configure Alert Upload Settings (see page 340).

Alert forwarding details are now configured.

Forward Collector Settings

Configures the authentication details that are used for connecting to and authenticating the alert collector server to which the alerts are forwarded.

For more information, see Configure Alert Collector Server Settings (see page 341).

Proxy Server Settings

Configures the proxy server details that are used for connecting to the alert collector server for alert forwarding.

For more information, see Configure Proxy Settings (see page 342)

Configure Health Monitoring Agent

Modify the properties on Health Monitoring Agent.

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, Policy Name, DSM, Health Monitoring, Health Monitoring Agent.
2. On the Setting Properties dialog, specify suitable values for the following items:

   Enable Health Monitoring

   Specifies the state of Health Monitoring. Default: False

   True

   Enables health monitoring.

   False

   Disables health monitoring.

   Script Directory

   Specifies the folder to which custom alert scripts must be copied. Default: scriptdir

   Note: When an absolute path is not specified, the folder is taken relative to the HM folder under DSM installation directory. Network paths are not supported.

   Script Output Directory

   Defines the name of the folder to which the output of custom alert scripts are copied. Default: scriptoutputdir

   Note: When an absolute path is not specified, the folder is taken relative to the HM folder under DSM installation directory. Network paths are not suported.

   Script Timeout

   Defines the time in seconds for the health monitoring agent to wait for script execution to complete. Default: 120 seconds

   Note: When the script execution fails with time-out error; increase the time in seconds, and retry.

   Maximum Upload Retries

   Defines the number of times alert information upload is reattempted. Default: 3

   Upload Retry Interval

   Defines the interval in seconds at which, the alert information upload is reattempted. Default: 5 seconds.

3. Click OK.

The health monitoring agent is now enabled.

You must also configure additional parameters for HM event logging

Follow these steps:

1. Navigate to Configuration Policy, Default Computer Policy, DSM, Common Components, Event Logging, Health Monitoring Events.
2. Configure the following parameters

   Event Log Destination Folder

   Defines the folder location relative to the DSM install folder for the event log files. The folder must exist on the agent.

   Default: HM

   Event Log File Name

   Defines the file name to use for logging the health monitoring events

   Default: hmevents_list.xml

Configure Alert Upload Settings

Configure the alert collector server details and apply on the agent to enable the health monitoring agent to upload the detected alerts.

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, Policy Name, DSM, Web Services, Client, and Health Monitoring.
2. Specify suitable values for the following options:

   Alert Collector Address

   Specifies the hostname or IP address of the alert collector server where the alerts are uploaded.

   Note: For HM agent on EM, configure the alert collector that is installed on the DM.

   Use Https

   Specifies the connection to the alert collector server through http or https.

   Default: False indicates http.

   When the alert collector is configured for https, perform the following steps on the agent machine:

   - Export CA Root Certificate in DER format from the webserver (alert collector) machine.
   - Copy the certificate to the agent and import using the following command:

     ```
     cacertutil import -i:<cert-file-path> -it:X509V3 -trust
     ```

When HM agent must connect to the alert collector through the proxy and the alert collector server is configured to authenticate the client requests, configure the following options:

Configure Alert Collector Server Settings

Configure the alert collector server settings details in the following way:

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, Policy Name, DSM, Web Services, Client, Health Monitoring, and Alert Collector Server Settings.
2. Specify suitable values for the following items:

   Authentication Method

   Defines the value that determines the authentication method.

   Http Authentication Type

   Defines the value that determines the type of http authentication.

   Note: Http offers the basic, digest, and NTLM authentication.

   Domain

   Specifies the domain name of the server.

   Password

   Defines the password to authenticate with the proxy.

   Username

   Defines the username to authenticate with the server.

Alert collector server settings are now configured.

Configure Proxy Settings

Configure the proxy settings in the following way:

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, Policy Name, DSM, Web Services, Client, Health Monitoring, and Proxy Server Settings.
2. Specify suitable values for the following items:

   Proxy Password

   Defines the password to authenticate with the proxy.

   Proxy User

   Defines the user to authenticate with the server.

   Proxy Server Address

   Defines the address of the proxy server.

   Proxy Server Port

   Defines the port on which the proxy verifies for connection requests.

   Proxy Type

   Defines the value that determines the type of proxy. The value *None* indicates the direct http connection.

Proxy settings are now configured.

Note: The HM agent supports only HTTP proxy. SOCKS proxy support is not available with this release.

Manage and Track the Status of Alerts from WAC

Alert Display

When a new alert is raised, you can see a notification in the system status portlet of the domain node in the DSM explorer. This notification has a hyperlink which launches WAC and takes the user to the Alerts page when the unified login is enabled. Apart from the hyperlink, see a count of the newly raised alerts.

To configure the unified login for WAC:

Follow these steps:

1. Navigate to WAC Config.properties file 'DSM\Web Console\webapps\wac\WEB-INF\classes\com\ca\wac\config\'
2. Set the value of attemptUnifiedLogin to **true**.
3. Restart tomcat.

   ```
   Caf stop tomcat
   ```

   ```
   Caf start tomcat
   ```

The unified login for WAC is now configured.

You can configure the link of WAC for alert display.

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, Policy Name, DSM, Health Monitoring, Alert Display, and WAC.
2. Configure the link to the WAC alerts page.

   Default: http://localhost/wac?context_launch_class=DSMHMAlert

   Note: Replace the *localhost* with wac machine hostname.

Manage and Track the Status of Alerts from WAC

Manage alerts from WAC by adding notes and updating its state to New, Follow-up or Cleared.

Follow these steps:

1. Navigate to Alerts.

   The alerts page is displayed.

2. Select an alert or multiple alerts and select Update or Delete.

   The dialog opens.

   - To update, change alert(s) status from the drop-down option:

     New

     Specifies the alert as new.

     Follow-up

     Specifies the alert for follow-up.

     Cleared

     Specifies the alert state as cleared.

   - To delete, select the alerts and confirm delete.

     Note: You can select the delete all option to delete all the alerts.

3. Update Notes with useful information to track the status of the alert.

The alerts are now updated or deleted.

Note: You can track, update, and delete the alerts from Domain Manager level only. All HM alerts on the Enterprise Manager are read-only.

Alert Replication

Alert Replication helps with replication of alerts.

- When the updates to the alerts at the DM are replicated to the EM by the engine, new alerts are not created as part of replication. The alerts are created at the EM only through alert forwarding at the DM with appropriate filters.
- Before the Engine replicates an alert to the EM, Engine checks if the alert exists. When an alert is not found, the engine does not replicate the alert upwards. When an alert is deleted at the DM, the corresponding alert at the EM is deleted.
- When a DM is unlinked from an EM, the following managed configuration policy parameter controls whether all the alerts with domain_uuid of that DM are left at the EM or deleted. On such deletions, the engine does not re-replicate alerts from the DM to the EM. This behavior is a limitation when the DM is re-linked to the EM.

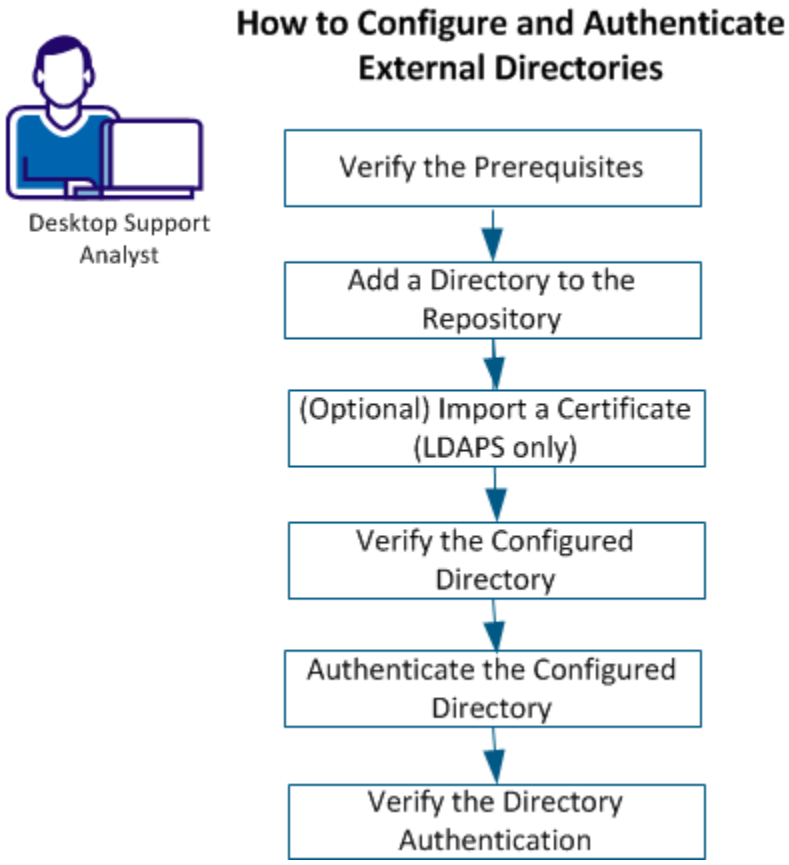
To edit the parameter that controls the deletion of the alerts of a particular domain on unlinking the domain from the EM, navigate to Control Panel, Configuration, Configuration Policy, Default Computer Policy, DSM, Manager, Engines, Delete replicated Alerts on unlinking. And set the value to True, on unlinking a DM, the replicated alerts from the DM are deleted at the EM.

Chapter 10: How to Configure and Authenticate External Directories

As a desktop support analyst, you use external directories for *authentication.* Using the external directories in the DSM Explorer, you can do the following tasks:

- Authenticate users, including native mode Active Directory users.
- Authorize users by mapping security profiles to entities in the directory.
- Define Query Groups with targets matching computers or users held in a container on a directory.
- Target the deployment of agents.
- Produce reports using a hierarchy obtained from a directory.

To authenticate using external directories, perform the following steps:



Perform the following steps:

1. Add a Directory to the Repository (see page 348)
2. (Optional) Import a Certificate (LDAPS only) (see page 354)
3. Verify the Configured Directory (see page 355)
4. Authenticate the Configured Directory (see page 358)
5. Verify the Directory Authentication (see page 361)

Supported External Directories

CA ITCM supports the following directories:

- Lightweight Directory Access Protocol (LDAP)
- Microsoft Active Directory
- Novell Directory Services (NDS)

See Compatibility Matrix for an updated list of the supported directory integration services.

Verify the Prerequisites

To authenticate using an external directory, verify the following prerequisites:

- Verify you have access permissions to configure an external directory.
- Ensure you have working knowledge of Directory Integration capability.

Add a Directory to the Repository

To authenticate users and authorize users by mapping security profiles to entities in the directory, add the external directory to the repository first.

Follow these steps:

1. Navigate to the Control Panel, Directory Integration, Add Directory to access the Add Directory Wizard, Click Next.

   The Introduction/Directory Name page appears.

2. Specify the directory name to identify the directory when connecting to Active Directory in Directory Name.

3. Select the type of directory using one of the Directory Type options. The following options are available:
   - Active Directory
   - LDAP
   - NDS

   Default: Active Directory.
4. Click Next to go to the Server Details page.

Specify Directory Server Details

Use the Server Details wizard page to specify the name of the directory server holding the directory you are adding and the port number to which you are connecting.

Note: For external directories that use Secure Sockets Layer (SSL), the certificate that the Lightweight Directory Access Protocol (LDAP) server uses must be valid and certifiable through the Microsoft Windows certificate authority chain. Previous versions of Windows gave the LDAP developer the opportunity to verify certificates; however, Windows 2003 SSL enforces this for you.

Follow these steps:

1. Enter the name of the name of the server supporting the directory in the Server Name field.
2. Enter the directory service's port number in the Port field.

   The directory client always attempts to create a secure encrypted connection to the directory using the port specified here. Some directories support port 389 for secure and insecure communications. Some directories also support port 636 as a secure-only channel. Your directory administrator can tell you which port to use.

   For the port specified, a secure channel is used if one is available; otherwise, if the port specified allows insecure communication, this is used. (If insecure communication is not acceptable, the directory import is rejected with a corresponding error message when you click Finish.)

   Note: Common configuration policies for directories—in particular, the Enable LDAP simple authentication policy—can have an impact on whether authentication can take place over an insecure communication channel.
3. Click Next to go to the Directory Binding page.

Note: If, after adding an LDAP directory, the specified access port is changed, the *original* security authority is not removed correctly and the security authority list may contain an invalid security authority. This has no functional impact on CA ITCM, but the original security authority is listed as valid in security dialogs. Removing the extraneous security authority requires a tool from Technical Support. Contact your support representative and request the *cfspsetpass* utility.

Specify Directory Binding Information

Use the Directory Binding wizard page to specify whether you want to access the directory anonymously or with user credentials.

Follow these steps:

1. (Optional) Select the Use Anonymous Binding option. By default, this option is not selected (False).

   Note: If selected, you may have limited or no access to the directory.

2. Enter the user name and password in the appropriate fields.
3. (Optional) Select the Use Secure Protocol (LDAPS) option. If you select this option, the secure LDAPS protocol is used instead of LDAP. However, ensure that LDAPS is supported by the directory you are configuring.

   Note: This field appears only if you are configuring an Active Directory or LDAP directory.

4. Click Next to go to the Base Directory Node page.

Specify the Base Directory Node Details

Use the Base Directory Node wizard page to specify the root node from which directory browsing starts.

Follow these steps:

1. In the Base Directory Node field, enter the Distinguished Name (DN) of the root object for browsing the current directory.

   Note: Try to use the lowest possible Base DN in the directory hierarchy as possible to ensure that searches are more efficient. Your directory administrator can tell you the best value to use.

2. Click Next to go to the Choose Schema Mapping page.

Choose Schema Mapping Attributes

Use the Choose Schema Mapping wizard page to specify the schema mapping for your directory. You can either select a predefined, common schema map or define one of your own.

Follow these steps:

1. (Optional) Select the Define New Mapping option if you want to use your own schema mapping.

   This option lets you define a mapping of the attribute names associated with data objects (such as users, computers, and groups) in your external directory to those attribute names used by corresponding DSM objects.

2. Select a predefined schema map using one of the Schema Maps options. Valid options are Active Directory , eTrust Directory, and NDS Directory.

   Default: Active Directory

3. Click Next to go to the Refine/Define Schema Mapping page.

Refine/Define Schema Mapping Details

The Refine/Define Schema Mapping wizard page lets you define a new schema map or refine the specified schema. Schema of the directory defines the names and types of the attributes. Schema mapping translates a directory objects attributes, or properties, as defined by that directory schema to a common schema used by other DSM-based applications.

Note: A number of predefined schema maps are provided for the most popular schemata, including hard-coded maps for the WinNT and UnixL providers.

Follow these steps:

1. When creating a new schema, enter a unique name for the schema map in the Schema Name field. Otherwise, this field displays the name of the existing schema selected.

   The appropriate mapping table appears, displaying the names and types of the attributes in the specified directory schema.

2. (Optional) To change the default value of a DSM attribute, click that attribute in the mapping table.

   The Attribute Mapping dialog appears.

3. (Optional) Change the value of one or more DSM attributes, and click OK.

   The Attribute Mapping dialog closes, returning you to the wizard page.

4. Click Next to go to the Finish page.

See Schema Mapping (see page 363) for more information on schema.

Review Configuration Options and Add the Directory

The Finish wizard page summarizes the configuration settings and options you have selected for the directory. Click Finish to complete the process of adding the specified directory to the repository, or click Back to change any of the settings and options.

The external directory is now configured.

(Optional) Import a Certificate (LDAPS only)

When using LDAPS to secure access to a defined LDAP or OpenLDAP directory, the Windows server must be able to trust the certificate from the LDAPS server. If the certificate is not from a trusted certificate authority, then you must manually import the certificate to the certificate store to complete the configuration process for your new directory.

Note: For detailed information about the wizards and dialogs in the following procedure, see the Microsoft documentation for x.509 certificates.

Follow these steps:

1. Locate ..\CA\DSM\bin\itrm_dsm_r11_root.der and double-click this file.

   The Import Certificate dialog appears.

2. Click Install Certificate.

   The Certificate Import Wizard appears.

3. Click Next.

   The Certificate Store wizard page appears.

4. Select the Place All Certificates in the Following Store option.

5. Click Browse.

   The Select Certificate Store dialog appears.

6. Select the Show Physical Stores option.

7. Do *one* of the following:

   - If the certificate is self-signed, expand Trusted Root Certification Authorities and select Local Computer.
   - If the certificate is *not* self-signed, expand Third-Party Root Certification Authorities and select Local Computer.

   Important! This step is essential. The certificate must be added to the physical store: otherwise, the current user's store will be used and the certificate will not be available to the local system account used by CA ITCM.

8. Click OK.

   The dialog closes, and you are returned to the wizard.

9. Click Next and Finish.

   The import was successful message appears.

10. Click OK.

    The specified certificate was added to the certificate store.

    Note: You can also use the encUtilCmd certimport command to perform the same operation.

Verify the Configured Directory

After you add and configure the directory, you can verify whether the Configured directory is added to DSM Explorer.

Follow these steps:

1. Navigate to the Control Panel, Directory Integration, Configured Directories node.

   The name and descriptions of all the configured *external directories* in the current domain is displayed. The description column displays an LDAP URL for each of your Active Directory configured directories, if any.

The external directory is now configured.

(Optional) Update the Directory

You can also update the directory properties.

1. (Optional) Update a configured directory using Properties of a configured directory.

   Update Directory dialog with the following tabs appears.

   - Settings
   - Security
   - Schema

Update Directory: Settings Tab

The Settings tab contains the main configuration options for directories.

This tab contains the following fields:

Directory Name

Specifies the directory, directory server, or NDS tree name as follows:

- Specifies the name used to identify the directory when connecting to Active Directory. It should be a name that the directory itself can resolve to a directory server.
- Specifies the name of the directory server when connecting to a stand-alone directory (that is, not a distributed directory like Active Directory) using LDAP. The name should be the full DNS name of the server that will be used for directory access and authorization.
- Specifies the name of the NDS tree when connecting to Novell NDS.

Example: An Active Directory domain HQDirectory.com is hosted on machine FAKE_MACHINE. When configuring this directory for integration, you could specify HQDirectory.com in this field, as Active Directory can successfully resolve HQDirectory.com to FAKE_MACHINE.

Directory Type

Specifies the type of directory. Valid options are Active Directory, LDAP, and NDS. By default, the directory type that was specified when the directory was added is selected.

Directory Server

Specifies the name of the server supporting the directory.

Port

Specifies the directory service's port number. The directory client always attempts to create a secure encrypted connection to the directory using the port specified here. Some directories support port 389 for secure and insecure communications. Some directories also support port 636 as a secure-only channel. Your directory administrator can tell you which port to use.

For the port specified, a secure channel is used if one is available; otherwise, if the port specified allows insecure communication, this is used. (If insecure communication is not acceptable, the directory import is rejected with a corresponding error message when you click Finish.)

Note: Common configuration policies for directories—in particular, the Enable LDAP simple authentication policy—can have an impact on whether authentication can take place over an insecure communication channel. For more information, see the Configuration Policy section of the *DSM Explorer Help*.

Default: 389 (for LDAP directories)

Base DN

Specifies the Distinguished Name (DN) of the root object for browsing the current directory. Ask your directory administrator for the best value to use.

Note: Because many directory searches may be performed from this base node, think carefully about the efficiency and accuracy of the searches that will be performed. Try to use a Base DN as low in the directory hierarchy as possible, as this will ensure that searches are more efficient.

Information

Displays tips for selecting options or entering information in fields or dialogs.

Update Directory: Security Tab

The Security tab provides security options for connecting to the directory.

This tab contains the following fields:

Anonymous Binding

Specifies whether to use anonymous binding. By default, the value that was specified when the directory was added is selected.

User

Specifies the user's name if anonymous binding is not selected.

Password

Specifies the password of the specified user if anonymous binding is not selected.

Information

Displays tips for selecting options or entering information in fields or dialogs.

Update Directory: Schema Tab

The Schema tab provides configuration options for mapping directory attributes to the CA ITCM schema.

This tab contains the following fields:

Schema

Indicates the schema to be used. A number of predefined schema maps are provided for the most popular schema, including hard-coded maps for the WinNT and UnixL providers. Choose one from the drop-down list.

Information

Displays tips for selecting options or entering information in fields or dialogs.

Authenticate Using the Configured Directory

Authentication identifies members of a trusted computing base, based on the credentials provided. Add the external directories as a security authority for DSM authorization operations. CA ITCM authenticates a security object to the external directory and uses the authenticated identity or group memberships for subsequent authorization calls.

For example, if you wish to allow a Linux DSM manager to authenticate Active Directory users using LDAP, then you ensure that Active Directory is configured for the maximum security available. Use certificate services on the directory and ensure that the Linux installation trusts the certification chain provided in the directories certificate.

Add a Security Profile

Creating a security profile means mapping a new one to either a user account or group provided by the current security providers. You can select the users or groups who can access the system and add them to a security profile.

Follow these steps:

1. Select Security Profiles from the Security menu.

   The Security Profiles dialog appears.

   Note: You must have sufficient access rights to open this dialog; otherwise, a security error message is displayed. Administrators have these access rights by default.

2. Click Add.

   The Add Security Profiles dialog appears.

3. Select the security authority from the Available Directories tree, browse and click the required security principal.

   You can view the selected security authority and principal in the Container Identifier and Names fields, respectively.

4. Double-click a principal in the tree, or click Add to List.

   The security principals shown in the Names field are added to the List of security profiles.

   To add more profiles, repeat the last two steps on the Add Security Profiles dialog.

5. Click OK.

   The selected user account or group is mapped to the security profile and the Class Permissions dialog is displayed.

   Note: If you have added more than one security principal, the Class Permissions dialog is not displayed. You must select the profile in the Security Profiles dialog, and click Class Permissions.

6. In the Class Permissions dialog, select the object class to which you want to assign the rights.

   Note: You can select multiple object classes and specify the class permissions for all of them. For continuous selection, press the Shift key and then click the objects; for random selection, press the Ctrl key and then click the objects.

7. Select the permission in the Class access drop-down list, and click OK.

   The given permissions are assigned to the new security profile.

The Add Security Profiles dialog displays a list of available security authorities: Windows NT domains, UNIX authentication targets, external directories such as NDS and LDAP, and the X.509 certificate subsystem.

The manager stores the list of available security authorities. When running in a Windows NT domain environment, the manager node will automatically calculate all explicit domain trusts available. You can see the list of available security authorities from the Add Security Profiles dialog.

In some cases you may wish to use an implicitly trusted domain when creating security profiles - a domain that is not in the directly calculated list.

The Security Profiles dialog allows you to add and remove authorities, but only within the Windows NT name-space (winnt).

- To add an implicitly trusted domain, click Add and enter the domain name in the new dialog.
- To remove an implicitly trusted domain, highlight the domain you wish to remove and click Remove.

Note: Conferring trust is enforced by the operating system. You cannot add a domain and have the manager trust this domain unless the underlying operating system already trusts the domain in question.

Predefined Access Types

The following example shows the results of various access rights on the Computer object class:

Class Access	Resulting Permission
View	Displays all computers under the All Computers folder.
Read	Lets you view the properties of the computers.
Manage	Lets you deploy a software package or run a job on a computer.
Change	Lets you add a new computer or delete a computer.
Full Control	Gives you full control on the computers.

Verify the Directory Authentication

To help ensure that the directory integration is successful, verify the directory authentication by logging into CA ITCM.

Follow these steps: on DSM Explorer

1. Specify the User Name and Password.

   Defines the user name to log in.

   Default: DN format.

   Important! When you want to use UID or SN formats for authentication, configure the value of configuration policy appropriately. For more information, see Modify the Policy to Use a Different Username Format (see page 363).

2. Select the security authority from the following list:

   Security Provider

   Specifies the security provider. As CA ITCM uses the external directories, operating system user account and groups for granting access rights, the operating system acts as the security provider. Select the appropriate security provider, and the corresponding windows domain or directory appears.

   Windows Domain (Windows) / Directory (ldap)

   Select the domain or the computer in which you have the user account. The configured directory that can access CA ITCM appears in the drop-down list.

3. Click Log in

   Logs in to the system if the login credentials are correct.

Follow these steps: on Web Console Access

1. Select the Manager Name from the Web Console drop-down.
2. Specify the User Name and Password.

   Defines the user name to log in. You can use DN format.

   Important! When you want to use UID or SN format for authentication, configure the value of configuration policy appropriately. For more information, see Modify the Policy to Use a Different Username Format (see page 363).
3. Select the security authority from the following list:

   Security Provider

   Specifies the security provider. As CA ITCM uses the external directories, operating system user account and groups for granting access rights, the operating system acts as the security provider. Select the appropriate security provider, and the corresponding windows domain or directory appears.

   Windows Domain (Windows) / Directory (ldap)

   Select the domain or the computer in which you have the user account. The configured directory that can access CA ITCM appears in the drop-down list.
4. Click Log in

   Logs in to the system if the login credentials are correct.

Note: The administrator on the domain manager authenticates the user with access rights to the configured directory.

Modify the Policy to Use a Different Username Format

Configure the value of configuration policy only when you are not using the DN format for authentication. Use the Setting Properties dialog to modify configuration policies to suit your specific requirements and environment.

Note: Before you can modify a policy, you must unseal it.

Follow these steps:

1. Navigate to Configuration, Configuration Policy, Default Computer Policy, DSM, Common Components, Security, Providers, Components, ldap.
2. Right-click Oracle ldap: Shortname Type in the pane and select Setting Properties from the context menu. Alternatively, click Setting Properties in the Tasks portlet.

   The Setting Properties dialog opens.
3. In the Value field, select *one* of the following values to suit your needs:

   sn

   Specifies the Short name for Oracle ldap.

   uid

   Specifies the unique id for Oracle ldap.
4. Click OK.

   The new value specifies whether the user name supplied for authentication is sn or uid.

Note: The *sn* must be unique for active directory-based ldap.

Understand the Schema Mapping Attributes

A *schema map* is a mapping of the attribute names associated with data objects (such as users, computers, and groups) in an external directory to those attribute names used by corresponding DSM objects. The fixed and standard set of DSM attribute names is used for querying directories and for formulating complex queries and reports.

Three predefined, common schema mappings are provided in CA ITCM. You also have the option to create your own custom schema based on the predefined schema set.

DSM Attribute Names

The following table lists the standard set of attribute names, with brief descriptions, used by DSM-based applications for querying directories:

Attribute Name	Description
objectClass	The class of the objects
dc	The domain controller
o	Organization
ou	Organizational unit
c	Country
l	Location
userDn	User's distinguished name
userCn	User's common name
userSn	User's surname
givenName	User's given name
displayName	Display name
userName	User name
userID	User identifier
userPassword	User password
memberOf	The names/distinguished names of the groups in which a user is a member
directReports	The names/distinguished names of the people who report to this user
streetAddress	Street address
postalCode	Postal code
company	Company
department	Department
email	Email address
telephoneNumber	Telephone number
jobTitle	Job title
userDescription	A description of the user
assetDn	Computer's distinguished name

Attribute Name	Description
assetCn	Computer's common name
assetName	Computer's name
dnsHostName	DNS host name
operatingSystem	Operating system
operatingSystemServicePack	OS service pack
operatingSystemVersion	OS version
assetDescription	A description of the computer
groupDn	Group's distinguished name
groupCn	Group's common name
groupName	Group's name
groupMembers	The names/distinguished names of users who are members of the group
groupDescription	A description of the group.

Additionally, the DSM schema map contains fields that are not attribute names. They are the names of the object classes that DSM-based applications use:

- The GUI uses computerMap, groupMap, and userMap to determine the type of nodes to display.
- The directory synchronization job uses userMap and computerMap.

The DSM schema map contains the following fields:

computerMap

Maps to the objectClass name representing a computer in the configured directory.

groupMap

Maps to the objectClass name representing a group in the configured directory.

userMap

Maps to the objectClass name representing a user in the configured directory.

containerMap

Maps to the class name for *container*.

Active Directory Schema

The following table shows the Active Directory attribute names mapping to the DSM schema:

DSM Attribute Name	Active Directory Attribute Name
objectClass	objectClass
dc	dc
c	c
l	l
userCn	cn
userSn	sn
givenName	givenName
userName	name
displayName	displayName
userID	name
userPassword	userPassword
memberOf	memberOf
directReports	directReports
streetAddress	streetAddress
postalCode	postalCode
company	company
department	department
email	mail
telephoneNumber	telephoneNumber
jobTitle	title
userDescription	description
assetCn	cn
assetName	name
dnsHostName	dnsHostName
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion

DSM Attribute Name	Active Directory Attribute Name
assetDescription	description
groupCn	cn
groupName	name
groupMembers	member
groupDescription	description
containerMap	container
groupMap	group
userMap	user
computerMap	computer
uniqueUserFields 1 – uniqueUserFields 5	–
uniqueComputerFields 1 – uniqueComputerFields 5	–
userDn*	distinguishedName
groupDn*	distinguishedName
assetDn*	distinguishedName
o*	o
ou*	ou

*** Note:** The mapping for these attributes is fixed and cannot be changed. However, you can use these DSM attribute names in queries.

Oracle Directory Schema

The following table shows the Oracle Directory attribute names mapping to the DSM schema:

DSM Attribute Name	Oracle Attribute Name
objectClass	objectClass
dc	dc
c	c
l	l
userCn	cn
userSn	Sn
givenName	givenName

DSM Attribute Name	Oracle Attribute Name
userName	name
displayName	displayName
userID	name
userPassword	userPassword
memberOf	–
directReports	–
streetAddress	streetAddress
postalCode	postalCode
company	company
department	departmentNumber
email	mail
telephoneNumber	telephoneNumber
jobTitle	title
userDescription	description
assetCn	cn
assetName	name
dnsHostName	host
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion
assetDescription	description
groupCn	cn
groupName	name
groupMembers	member
groupDescription	description
containerMap	container
groupMap	groupOfUniqueNames
userMap	inetOrgPerson
computerMap	computer
uniqueUserFields 1 – uniqueUserFields 5	–

DSM Attribute Name	Oracle Attribute Name
uniqueComputerFields 1 – uniqueComputerFields 5	–

*** Note:** The mapping for these attributes is fixed and cannot be changed. However, you can use these DSM attribute names in queries.

eTrust Directory Schema

The following table shows the eTrust Directory attribute names mapping to the DSM schema:

DSM Attribute Name	eTrust Directory Attribute Name
objectClass	objectClass
dc	dc
c	c
l	l
userCn	cn
userSn	sn
givenName	givenName
userName	name
displayName	displayName
userID	name
userPassword	userPassword
memberOf	–
directReports	–
streetAddress	streetAddress
postalCode	postalCode
company	company
department	departmentNumber
email	mail
telephoneNumber	telephoneNumber
jobTitle	title
userDescription	description

DSM Attribute Name	eTrust Directory Attribute Name
assetCn	cn
assetName	name
dnsHostName	host
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion
assetDescription	description
groupCn	cn
groupName	name
groupMembers	member
groupDescription	description
containerMap	container
groupMap	groupOfNames
userMap	inetOrgPerson
computerMap	device
uniqueUserFields 1 – uniqueUserFields 5	–
uniqueComputerFields 1 – uniqueComputerFields 5	–
userDn*	dn
groupDn*	dn
assetDn*	dn
o*	o

*** Note:** The mapping for these attributes is fixed and cannot be changed. However, you can use these DSM attribute names in queries.

NDS Directory Schema

The following table shows the NDS attribute names mapping to the DSM schema:

DSM Attribute Name	NDS Attribute Name
objectClass	objectClass
dc	dc

DSM Attribute Name	NDS Attribute Name
c	c
l	l
userCn	cn
userSn	Surname
givenName	givenName
userName	name
displayName	displayName
userID	name
userPassword	userPassword
memberOf	–
directReports	–
streetAddress	streetAddress
postalCode	postalCode
company	company
department	departmentNumber
email	mail
telephoneNumber	telephoneNumber
jobTitle	title
userDescription	description
assetCn	cn
assetName	name
dnsHostName	host
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion
assetDescription	description
groupCn	cn
groupName	name
groupMembers	member
groupDescription	description

DSM Attribute Name	NDS Attribute Name
containerMap	container
groupMap	group
userMap	user
computerMap	computer
uniqueComputerFields 1 – uniqueComputerFields 5	–
uniqueUserFields 1 – uniqueUserFields 5	–
userDn*	dn
groupDn*	dn
assetDn*	dn
o*	o
ou*	ou

*** Note:** The mapping for these attributes is fixed and cannot be changed. However, you can use these DSM attribute names in queries.

Directory Integration in CA IT Client Manager

CA ITCM supports the following Directory Services:

Note: See Compatibility Matrix for an updated list of the supported directory integration services.

Directory Services on Windows

Directory Service	Authentication	Queries	Reports	Deployment	Remote Control Rights
Active Directory 2000	+	+	+	+	+
Active Directory 2003	+	+	+	+	+
OpenLDAP v2.0	+	+	+	+	+
OpenLDAP v2.1	+	+	+	+	+
OpenLDAP v2.2	+	+	+	+	+
Novell NDS	+	+	+	+	+

Directory Service	Authentication	Queries	Reports	Deployment	Remote Control Rights
Novell eDirectory v8.5	+	+	+	+	+
eTrust Directory r8	+	+	+	+	+

Legend:

+ = supported

- = Does not work

Directory Services on Linux

Directory Service	Authentication	Queries	Reports	Deployment	Remote Control Rights
Active Directory 2000	+	+	+	+	+
Active Directory 2003	+	+	+	+	+
OpenLDAP v2.0	+	+	+	+	+
OpenLDAP v2.1	+	+	+	+	+
OpenLDAP v2.2	+	+	+	+	+
Novell eDirectory v8.5	+	+	+	+	+
eTrust Directory r8	+	+	+	+	+

Legend:

+ = supported

Chapter 11: CA ITCM Security Features

The security features in CA ITCM cover two subject areas.

Authentication

Provides confidence that the requesting object is what it says it is.

Authorization

Provides configuration and validation of access rights and privileges for performing operations on secured objects.

This section contains the following topics:

Authentication

Authentication identifies members of a trusted computing base, based on the credentials provided.

Members of a trusted computing base are as follows:

Users, and indirectly group membership

Primarily, these are homogeneous security principals from the current operating system. These could be, for example, Windows users (Active Directory, domain or local), UNIX (LDAP), or UNIX local users.

Machines

Computers that are part of a trusted computing base, such as Windows NT, can be identified and authenticated. Theoretically, UNIX computers could be identified, as they also are part of a trusted computing base that we can establish a trust relationship with.

Different information is used to authenticate a user or machine, as follows.

- In Windows operating environments:
  - User name
  - Password
  - Windows Domain
  - Security Provider
- In Linux and UNIX operating environments:
  - Machine name
  - User name
  - Password
  - Security Provider

Different applications have differing requirements for authentication. If possible, unified logon is used, that is, the user's current credentials are used implicitly rather than prompting the user for explicit credentials.

However, in some cases, these credentials are not valid for the resource they are accessing or special operations may require reauthentication. When unified logon is not to be used or the credentials are not valid, a GUI application will be able to prompt for credentials whenever they are required, whereas a command line application running in batch mode will fail and record an authentication error.

If you are using an LDAP security provider for authenticating users against a directory when you specify login credentials, make sure these credentials are valid for the target directory and are fully specified. For an Active Directory you should use the full LDAP DN, for example:

```
CN=user,OU=Users,OU=myOU,DC=mydomain,DC=com
```

When using external generic LDAP directories for authentication, access rights must be given directly to the authenticating objects, as group membership cannot be directly evaluated. This does not apply to Active Directory.

Supported User Name Formats

The following user name formats are supported by CA ITCM. These name formats apply for all CA Technologies applications requiring a user name, for example, the Explorer GUI and the Web Services.

Windows native security or Linux/UNIX local security (local users and trusted domains)

User name format: *username* (Windows NT downlevel format or Linux user)

LDAP talking to Active Directory (Windows and Linux/UNIX)

User name format: UPN or DN

LDAP talking to any directory (except Active Directory) (Windows and Linux/UNIX)

User name format: DN

User name format: UID or SN (for Oracle ldap)

NDS Directory (Windows only)

User name format: DN

X.509 Certificate-Based Authentication

Whenever a CA ITCM client process connects to a CAF plug-in that requires authentication, the client process must pass security credentials relevant to the target services security requirements. Where the client process is running as an autonomous process, such as a Windows NT service or a UNIX daemon, the client process may authenticate using X.509 V3 certificates in the absence of any user credentials.

An X.509 certificate for CA ITCM authentication comprises a set of attribute-value pairs packaged together with the public encryption key of an asymmetric key pair. The certificate is digitally signed and sealed by a root certificate. The certificate records the name of the subject to whom the certificate was issued, the issuing certificate authority name and expiry information. The subject name is often referred to as the Distinguished Name (DN). The subject name is mapped to a Uniform Resource Identifier (URI) in the x509cert namespace, such as the following:

```
x509cert://dsm r11/CN=Basic Host Identity,O=Computer Associates,C=US
```

For an overview of the current certificates see Common Certificates (see page 531) and Application-specific Certificates (see page 532).

Using public key cryptography, clients will authenticate themselves to scalability servers upon request. A scalability server can then use the certified identity to perform subsequent authorization checks and commit audit records. The management console enables certificate URIs to be assigned privileges to tasks or objects within the CA ITCM management database.

Object-Level Security and Certificates

The CA ITCM management database provides class and object-level security (OLS). The permissions assigned in the database are associated with a security profile, which is represented by an object URI. Certificate URIs can be associated with security profiles and therefore can be used to regulate access to the CA ITCM management database.

For example, when scalability servers connect to a domain manager, they will authenticate themselves using the registration certificate. The URI associated with the registration certificate has been given only enough permission to the database to allow registration of the scalability server node.

Root Certificates

CA ITCM uses trusted root certificates to validate the certificates used for authentication. Multiple root certificates can be used in parallel to allow management of distinct authority chains or to help migrate from one certificate chain to a new chain.

For two nodes to successfully communicate and subsequently authenticate, the authenticator node (responder) requires access to the root certificate that signed the authenticating party's certificate (initiator). If the certificate is not available, not recognized or otherwise invalid then the authentication will fail. During planned certificate migration, the authenticator can be updated with one or more trusted root certificates to allow phased migration of clients. Initiators with different versions of certificates will still successfully authenticate if they are signed by root certificates that are trusted by the responder.

Certificate Storage

Authentication certificates are stored securely on each CA ITCM node. The certificate files are password-protected and the usage password is encrypted with the CA ITCM configuration.

Basic Host Identity Certificates

Every CA ITCM node has a certificate that provides Basic Host Identity (BHI) installed by default. Other certificates for specialized purposes are installed with the services that require them (see "Current Certificates" (see page 531)). The installation of CA IT Client Manager comes with a default standard certificate signed by a CA ITCM root certificate. This certificate is installed on every CA ITCM node within the enterprise.

We recommend that end users should plan on creating their own root certificate, Basic Host Identity (BHI) certificates, and the application-specific certificates. See "How You Introduce Your Own X.509 Certificates into the Install Image" (see page 216) for information on replacing the default certificates with end user-specific certificates.

When creating new BHI certificates, there are three primary paradigms:

- Create a single host identity certificate that is used on all CA ITCM nodes within the enterprise. This is the simplest solution, as the custom install image will only have to be generated once to create a tailored package.
- Create a unique host identity certificate for each individual node in the DSM enterprise. This is the most complex solution. The DN assigned to each node should be unique and reflect the identity of the host machine. A fully qualified host name is usually suitable for this purpose. A custom installation image will be required to install the appropriate certificate file onto the target machine.
- A hybrid of the two paradigms above. Create a single host identity certificate for use on the majority of the CA ITCM nodes. Create tailored identity certificates for use on DSM scalability server and manager nodes. When a requirement for a tailored certificate is identified, issue a new certificate and install it on the specified node. This is the most flexible solution. Important nodes in the enterprise are more effectively identified and protected.

Certificate Distribution

Certificate distribution must be covered before certificate creation. Depending on the method of certificate creation chosen (see description in "Basic Host Identity Certificates" (see page 378)), certificate distribution can be quite complex.

CA ITCM does not provide any automated certificate distribution technology. It comes delivered with default certificates for each CA ITCM node and application-specific certificates.

To migrate away from the default certificates after a default install, the certificates should be distributed in the following (simplified) way. This allows a successful migration of trust without causing any downtime in communications and authentication due to the parallel use of trusted roots.

1. Create new root certificate. Ensure that the root name (DN) is different from the existing CA ITCM root certificate.
2. Schedule the distribution of the new root DER encoded certificate to all nodes within the CA ITCM infrastructure. This will enable the root as a trusted root authority to all CA ITCM nodes.
3. Create new security profiles in the CA ITCM management database to replace the existing application-specific certificate profiles. Do not delete the old profiles yet.
4. Schedule the distribution of new certificates to all of the CA ITCM nodes.

5. After the certificate distribution is successful, schedule the deletion of the previous CA ITCM certificates.
6. Delete the old security profiles for the application-specific certificates.

This list is not exhaustive. Contact CA Technologies's Technical Support for advice on major-scale certificate distribution and replacement with a full scale PKI implementation.

Creation of New Certificates

To create new certificates, you can use the supplied cacertutil tool or use an existing PKI to generate certificates for you. The use of external PKI systems is outside the scope of this documentation, but the certificate requirements would be the same as for cacertutil certificate creation.

Note: An external PKI would not need to create a new root certificate for the CA ITCM infrastructure.

Generation of a New Root Certificate

When generating a new root certificate, the following two forms of the certificate must be created:

- A PKCS#12 encoded file. This contains both the public section of the certificate and the private key.
- A DER encoded file. This contains only the publicly accessible part of the certificate.

Both forms of the certificate are generated at the same time with the CA ITCM tool. When using an external PKI, the root certificate can be exported in DER format.

The new root certificate is central to the security in CA ITCM and so should be protected from accidental or deliberate disclosure. The PKCS#12 certificate file should be protected with a complex pass phrase and stored in a secure administrative data store.

The PKCS#12 format certificate is used to sign other certificates. The DER format certificate is used to verify these signed certificates.

The command to create a new root certificate has the following format:

```
cacertutil create -o:rootname.p12 -od:rootname.der -op:passphrase
“-s:CN=YourRoot,O=YourOrg,C=Country” -d:NumberOfDays -oe
```

-o

Specifies the output *filename* for the PKCS#12 packaged certificate.

-od

Specifies the output *filename* for the DER encoded certificate.

-op

Specifies a pass phrase used to encrypt the PKCS#12 certificate file.

-s

Specifies the subject of the certificate.

-d

Specifies the lifetime of the certificate in days (for example, 730 (= 2 years)).

-oe

Generates a random encrypted version of the pass phrase used to decode the certificate and outputs it to the console. This encrypted pass phrase can be provided to the certificate tool instead of a clear-text password.

Generation of Application-specific Certificates

For each application listed in "Current Certificates" (see page 531), create a new certificate. If you do not use the DN as listed in the appendix table, then you will also need to assign the required permissions for the certificate security profile in the CA ITCM security browser.

To ensure that the newly created certificate is visible to the CA ITCM security browser, the DER encoded certificate should be imported into the CA ITCM certificate database on the manager nodes.

The command to create the new certificates is as follows:

```
cacertutil create -o:certname.p12 -od:certname.der -op:passphrase "-s:CertDN"
-i:rootname.p12 -ip:rootpassphrase -d:730
```

-o

Specifies the output file name for the PKCS#12 packaged certificate.

-od

Specifies the output file name for the DER encoded certificate.

-op

Specifies the pass-phrase to protect the PKCS#12 output certificate.

-s

Specifies the DN to whom the certificate should be issued.

-i

Specifies the file name of the root PKCS#12 certificate.

-ip

Specifies the pass-phrase protecting the root PKCS#12 certificate.

-d

Specifies the lifetime of the certificate in days (the example shows 2 years (= 730 days)).

Generation of the Basic Host Identity Certificate

The Basic Host Identity (BHI) certificate does not have any rights to the CA ITCM management database and no associated security profile in the default installation. Thus, choosing a new DN for the certificate does not involve any additional effort to amend CA ITCM security profiles and permissions.

The default DN assigned to the BHI certificate is as follows:

CN=Basic Host Identity,O=Computer Associates,C=US

The command to create a new Basic Host Identity certificate has the following format:

```
cacertutil create -o:certname.p12 -od:certname.der -op:passphrase “-s:CertDN”
-i:rootname.p12 -ip:rootpassphrase -d:730
```

-o

Specifies the output file name for the PKCS#12 packaged certificate.

-od

Specifies the output file name for the DER encoded certificate.

-op

Specifies the pass-phrase to protect the PKCS#12 output certificate.

-s

Specifies the DN to whom the certificate should be issued.

-i

Specifies the file name of the root PKCS#12 certificate.

-ip

Specifies the pass-phrase protecting the root PKCS#12 certificate.

-d

Specifies the lifetime of the certificate in days (the example shows 2 years (= 730 days)).

Installation of New Certificates

When installing new certificates to a CA ITCM node, the process that installs the certificate must be running as a local administrative user, that is, a member of the Administrators group on Windows.

Installation of a New Root Certificate

To install a new root validation certificate on to a CA ITCM node, use the DER encoded file. The command to install this certificate has the following format:

```
cacertutil import -i:rootcert.der -ip:passphrase -it:X509V3
```

This imports the certificate's publicly accessible information as a trusted root certificate into the certificate database.

Installation of Application-specific Certificates

In the CA IT Client Manager code base, the application specific certificates are referenced through a tag name rather than the certificates assigned DN. The relevant tag names are detailed in "Current Certificates" (see page 531). The certificate should be installed only to the nodes that require them to authenticate to a DSM scalability server or manager.

The command to install an application-specific certificate has the following format:

```
cacertutil import -i:certname.p12 -ip:passphrase -t:tagname
```

-i

Specifies the name of the PKCS#12 certificate file to import.

-ip

Specifies the pass-phrase used to protect the certificate.

-t

Specifies the tag name of the certificate.

To make the certificate visible to the DSM security browser, the DER encoded certificate must be imported into the certificate database on the manager nodes. The command to import a DER encoded certificate has the following format:

```
cacertutil import -i:certname.der -it:X509V3
```

-i

Specifies the name of the DER encoded certificate to import.

-it

Specifies the type of certificate to import. X509V3 specifies DER encoding.

Installation of the Basic Host Identity Certificate

The Basic Host Identity certificate is always installed with the tag name dsmcommon. The command to install the BHI certificate has the following format:

```
cacertutil import -i:certname.p12 -ip:passphrase -t:dsmcommon -h
```

-i

Specifies the input PKCS#12 certificate file name.

-ip

Specifies the pass-phrase used to protect the input certificate.

-t

Specifies the tag name of the certificate.

-h

Specifies that the certificate should be used to provide the default host identity.

Certificate Replacement

Replacement of the default CA ITCM certificates requires that any new certificates use the same physical file names as the originals. The subject names assigned to the certificates do not have to be the same as the original. These are recorded and controlled by the cfcert.ini installation file, and will be inserted into the database during installation according to this file's instructions.

The following table lists the file names and their association:

File Name	Associated to CA ITCM subject
itrm_dsm_r11_root.der	Root certificate
basic_id.p12	Basic Host Identity certificate

File Name	Associated to CA ITCM subject
itrm_dsm_r11_root.der	Root certificate
dsmpwchgent.p12	Enterprise access
dsmpwchgdom.p12	Domain access
dsmpwchgrep.p12	Reporter access
ccsm.p12	CSM access
itrm_dsm_r11_cmdir_eng.p12	Directory Synchronization access
registration.p12	Registration access
itrm_dsm_r11_sd_catalog.p12	SD Catalog access
itrm_dsm_r11_agent_mover.p12	SD Agent Mover access

Certificate Removal

Certificates can be removed either one at a time or in bulk.

To remove a certificate individually, issue the following command:

`cacertutil remove -s:`*`subject_name`* `[-t:`*`tag_name`*`] [-l:{local|global}]`

-s

Specifies the subject name that the certificate is issued to.

-t

Specifies the tag name of the certificate, if installed with one.

-l

Specifies if the certificate was installed in the global or local common store.

The command to remove certificates in bulk is as follows:

`cacertutil flush`

Important! This command will remove all certificate entries from the common store for both the current user and the local machine (if the current process user has sufficient rights).

VMware ESX Security and Authentication

CA ITCM's AM remote agent only supports VMware ESX servers running in secure HTTP mode. VMware recommends that secure HTTP (HTTPS, the default configuration) be used for production deployment. For this reason, the AM remote agent connects only to ESX hosts where the default, recommended configuration of secure HTTP is used.

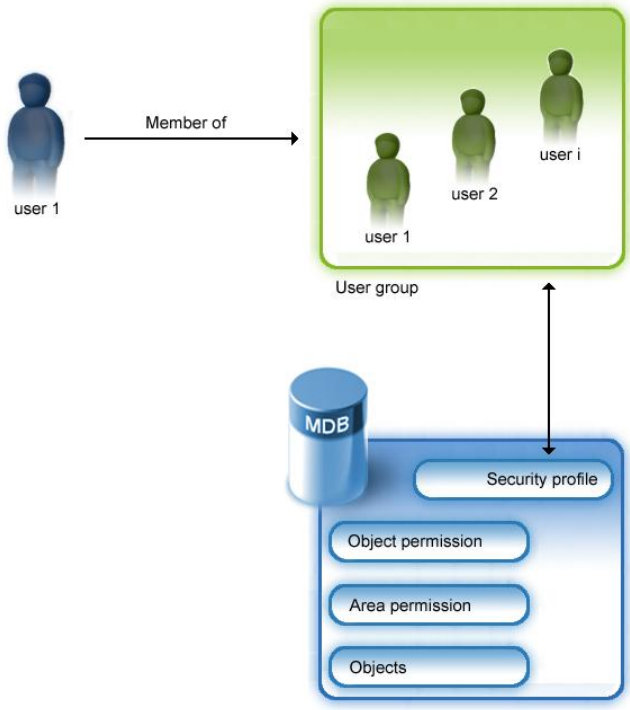
Secure Sockets Layer (SSL) is used as the connection protocol between the DSM agent and the ESX host machine. However, because the identity of an ESX host machine is not known in advance, there is no authentication between the DSM agent and ESX host. Certificates will not be used to authenticate an ESX host.

Authorization

Authorization controls the rights and privileges for an object associated with an authenticated entity, typically, a logged-in user. An authenticated entity is managed by security profiles. That means that a user or a user group is represented by a security profile and all permissions are managed in connection with the security profile.

The CA ITCM security subsystem is managing the authorization by providing a robust and generic security option for the entire CA IT Client Manager. It is responsible for controlling the rights and privileges for an object associated with an authenticated entity named security profile.

The following illustration gives an overview of the security subsystem that controls the authorization:



Normally, a user who is logged on to a system is a member of one or more user groups where the user group is represented by a security profile.

That means that the CA ITCM administrator is responsible for creating the security profile for either a user group or a separate security profile for a particular user.

The permissions for the security profiles to the objects are also stored in the MDB in addition the CA ITCM objects.

For example, you can create security profiles to determine which operating system-dependent groups and users can access the CA ITCM system. You can also establish class permissions, group and object permissions, and restrict the access of users or user groups to selected folders or objects.

Security Profiles

A security profile is an operating system user account or group in the domain manager (local profiles) or in its network domain (domain profile).

The security subsystem in CA ITCM supports multiple security profiles. A security profile is either built-in (that is, created at installation time) or user-defined.

A user-defined security profile represents either a single user or a user group.

The most important security profiles created at installation time include:

- Owner (virtual account)
- Everyone (default virtual account for everyone)

In addition to the security profile there is a set of security classes, which is associated with a profile. Each profile has its own set of security classes. A security class allows setting the permissions that will be assigned to an instance of such a class as soon it is created.

You can also create security profiles for users in the trusted domains. Every user should have a valid security profile to log in to the system. If new users are added to a managed group, they automatically inherit the access rights given to the group and can log in to the system instantly.

A user can have multiple profiles. However, each profile can be mapped to only one user or group. For example, if a user is a member of a group, then that user can have two profiles: one mapped to the user account and the other mapped to the group. In this case, the user will have the (mathematical) union of permissions in both profiles.

If a user is a member of more than one security profile, the effective permission for that user is a (mathematical) union of the individual permissions defined for each security profile (like applying (mathematical) OR to all permissions).

If you want to deny access for a user of an individual security profile, you must remove that user from the security profile.

The system provides predefined security profiles and lets you create as many profiles as you want, using the Security Profiles dialog.

We recommend that at least one of these profiles has Full Control as access right to the system.

Overview of Permissions

Authorization covers the following types of permissions:

- Class permissions
- Object permissions
- Area permissions

The security subsystem manages all types of permissions and uses a cumulative approach to get the effective permissions.

If you have enabled area permissions, both types of permissions (object and area permission) are checked to get access to objects. That means a user needs objects permissions *and* area permissions to get an object managed. Object permissions are checked only if area support is disabled .

Class Permissions

Class permissions are the access rights you specify on class level. This means that the class-level permissions are the default rights for each object that is an instance of this class.

You must specify the class permissions for each security profile when you create a security profile. For all security classes, No Access is set by default. Security profiles with appropriate class permissions give you access rights to the system. You can specify this in the Class Permissions dialog.

Class permissions are globally applicable to all objects in an object class. If you want to restrict users on a specific object or folder in the Explorer, or grant extended access rights, use the Object Permissions dialog or the Security Group Permissions dialog, respectively.

Security classes are used for grouping objects of the same type. The security subsystem in CA IT Client Manager supports the following security classes:

- Discovered hardware (Computer)
- Users
- Computer Users
- Manager
- Servers
- Asset Groups
- Server Groups
- Domain Groups
- Queries
- Security Classes
- Security profiles
- Software packages
- Software procedures
- Procedures groups
- Job Containers
- Software Jobs
- Asset Jobs
- Modules
- Query Based Polices
- Event Based Policies
- OSIM Boot images
- OSIM OS images
- Engine
- Configuration Policies Computer
- Configuration Policies User
- External Directory Access
- Report Templates
- Inventory modules

The following security classes are used for class level only.

- MDB Access
- Enable Control Panel
- Enable Remote Control

Class level security means that every object or instance of a class will get the permission as defined for the class by default.

Combined Class Permissions Required for Specific Actions

A couple of Object Class rights are depending on each other; this means if you want to perform the following actions, you have to grant rights to more than one object class.

Report Templates

If you want to schedule a Report template, you need to grant Change right for object class "Report Scheduling" *and* Change right for object class "Engine".

Security Profiles

The security class "Security Profiles" controls the handling with just security profiles (delete, and so on). If you want to modify object class permissions in a security profile, you must have Special Access (VRP, with the 'P' permission) for the object class "Class Permissions".

Engine

If you want to link an engine task to an engine, you must grant Change right for the "Engine" object class *and* Manage right for the "Engine Task" object class.

Regarding engine security, if you want to start, stop, or modify engine objects, you must grant Full Control right for the "Engine" class in the security profile *and* beyond NT Administrator or root rights to the computer where the engine is running.

Software Job security

If you want to modify or remove a software job under the /computer folder, the software is delivered to /Jobs/Software Jobs; the object classes "Computer" and "Software Job" must have Change rights.

Procedure Security

If you want to start, stop, or modify Procedure objects, you must grant Change (VRWXD) for the "Procedure" class *and* beyond the file permissions administrator or root.

Security Area Support

If you want to enable or disable the Security Area support and define Default Security Areas, the class permissions for the object class "Security Area" must be set at least to Special Access (VP).

If you want to link security profiles to a security area, View (V) permissions are sufficient for the object class "Security Area". The class permissions for the object classes "Security Profiles" must be set at least to Special Access (VW).

Object Permissions

Setting object permissions is helpful when you want to restrict the access rights on a particular object. By default, all objects inherit the permissions set for the object class.

Object permissions take precedence over the class and group permissions.

The object permissions are always present and managed by the security subsystem and cannot be disabled. If you do not want to take care of object permissions you may set the class-level permissions for all security classes to Full Control.

Authorization is based on the concept of an Access Control Entry (ACE). An ACE is any combination of the code letters shown in the following table, for example, VR. This ACE allows you to show and read objects; any other access is denied.

If the ACE is empty (contains no code letter), no access right is granted at all.

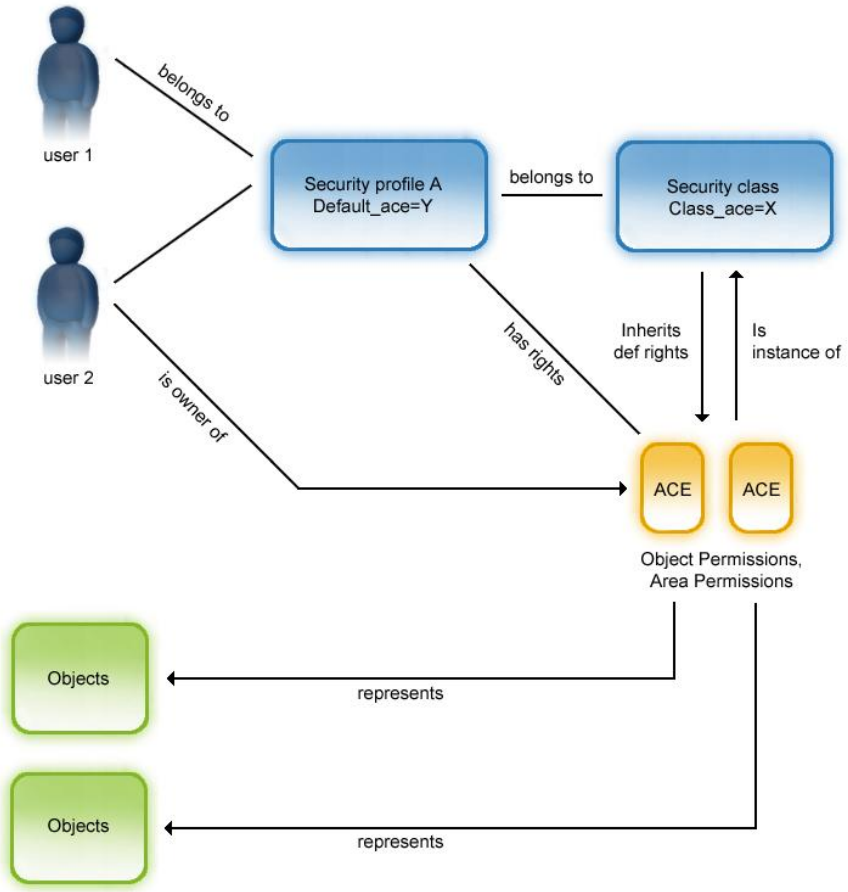
The following table defines object permissions:

Code letter in ACE	Meaning	Rights Granted
V	View	Allows you to show objects
C	Create	Allows you to create objects

Code letter in ACE	Meaning	Rights Granted
V	View	Allows you to show objects
R	Read	Allows you to read sub-objects of an object
W	Write	Allows you to change an object
X	Execute	Allows execution, depends on object type
D	Delete	Allows you to delete objects
P	Permission	Allows you to change the ACE itself
O	Ownership	Allows you to take ownership of an object

A user may belong to one or more security profiles. A user can also be the owner of an object. A set of security classes is assigned to each security profile. The security class permission defines the default permission that is assigned to an object when an instance of the class is created.

The following illustration shows how security profiles, security classes and object permissions are related to each other and that an object inherits the rights from the security class where the object is an instance of:



In the illustration, user 1 belongs to security profile A, user 2 belongs to security profile A and is also owner of objects, represented by an ACE. User 1 and user 2 have specific ACEs, for example, VR, through security profile A. User 2 has an additional ACE, for example, VCRWD, as owner of an object.

To check the access rights of user 1 and user 2 to an object, the security system makes a (logical) union of the user-specific ACE and the ACE associated to the specific secured object. In the example, both user 1 and user 2 have "view" and "read" rights to the object, but only user 2 has write or delete access.

Security Levels

Depending on how the object permissions are derived, there are different types of security levels for the object:

Class-level security

When the object permission derives from the class-level permission (from the class where the object belongs), the security level is set to class-level. This is the default if a secured object is created.

Group-level security

When a secured object is member of a security group where inheritance is enabled, the security level is set to group-level. Permissions derive from the group that the object is a member of (group-level permission).

Object-level security

When the user sets the object permission manually for a certain secured object, the security level is set to object-level (because the permissions are set individually for the object.)

Permission Inheritance from a Group

If an object is member of a group, the security subsystem in CA ITCM supports dynamic inheritance of permissions from a group to a member, as follows:

- A flag marks a group for dynamic inheritance.
- The specified member permissions are inherited to all members of this group.
- If a member is added to a group, it automatically inherits the permissions of the group.

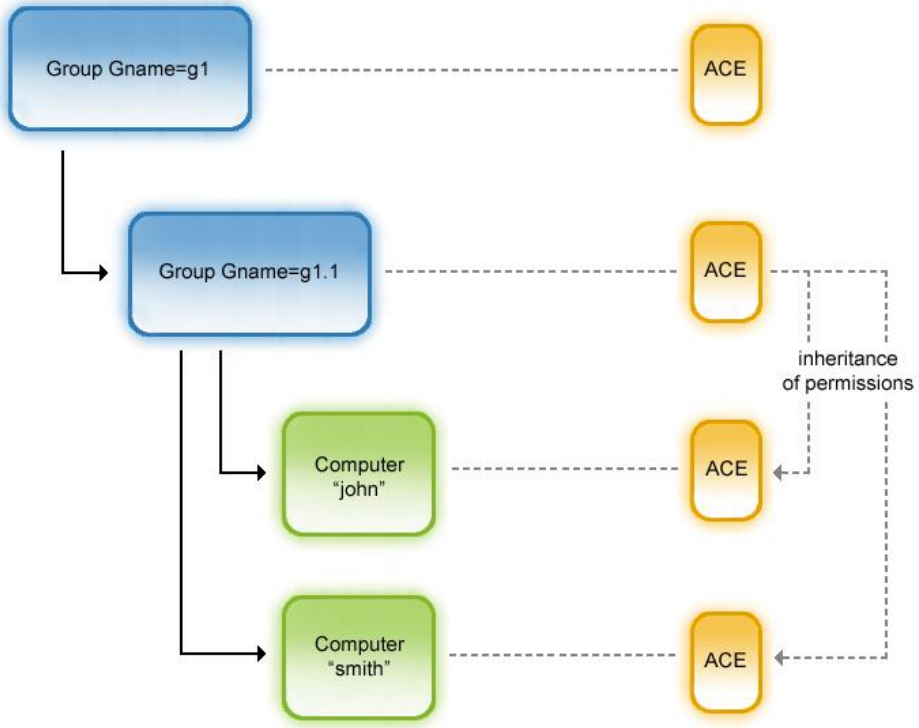
The design of group security is based on following decisions:

- Security inheritance can be turned on or off on a group. When turned on, the group becomes a security group (the application may use a different icon for visualization).
- The group will have two permission masks, one for the group itself (just like any other secured object) and an inheritance mask.
- When a group inherits from a parent group, both masks will be changed to the inherit mask of the parent group.
- The permission mask of a member of a group or many groups is evaluated to the "union" of all the permissions from the member’s parents, and so on. (the permissions are ORed together).
- The inheritance is done from parent to child which can result in a recursive update of objects.
- There are no restrictions of inheritance depth.

- In the order of precedence, object permissions preside over group permissions, which preside over class permissions.
- If an object is a member of at least one security group, the only change allowed on that object is to apply object security, because applying class security would break the model. For class security to become active, the object needs to be removed from the group or security inheritance turned off on the group.

Note: Inheritance from a group is switched off, if the security level of an object is set to object-level.

The following illustration shows the inheritance when an object is a member of a group and the group enables the inheritance of the object permissions:



Group g1.1 is a sub-group of group g1. The computers "john" and "smith" are members of the group g1.1.

For the group g1 inheritance of permissions is disabled, for g1.1 it is enabled. Therefore, the computers "john" and "smith" inherit their permissions from the permissions of group g1.1.

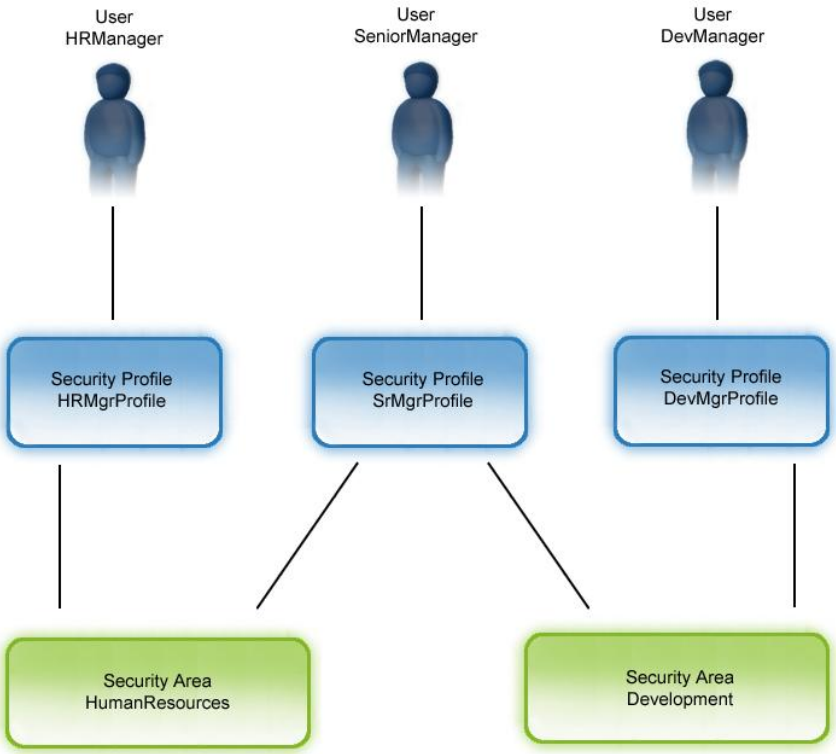
Area Permissions

The security area concept extends the security model. A security area is an optional feature that is suitable for large implementations with thousands of objects managed by different users.

A security area is a geographical, organizational, or topological division. Defining security areas is helpful if you want to restrict the access of users to only the objects linked to their security area. In the security area concept, users, represented by security profiles, and objects are linked to security areas. A security area can be linked to one or more profiles and one or more objects. A user can access an object, if at least one security area linked to the object is also linked to at least one security profile of the user. If object access is denied, the object is not visible for the user.

Example: Two security areas and three users

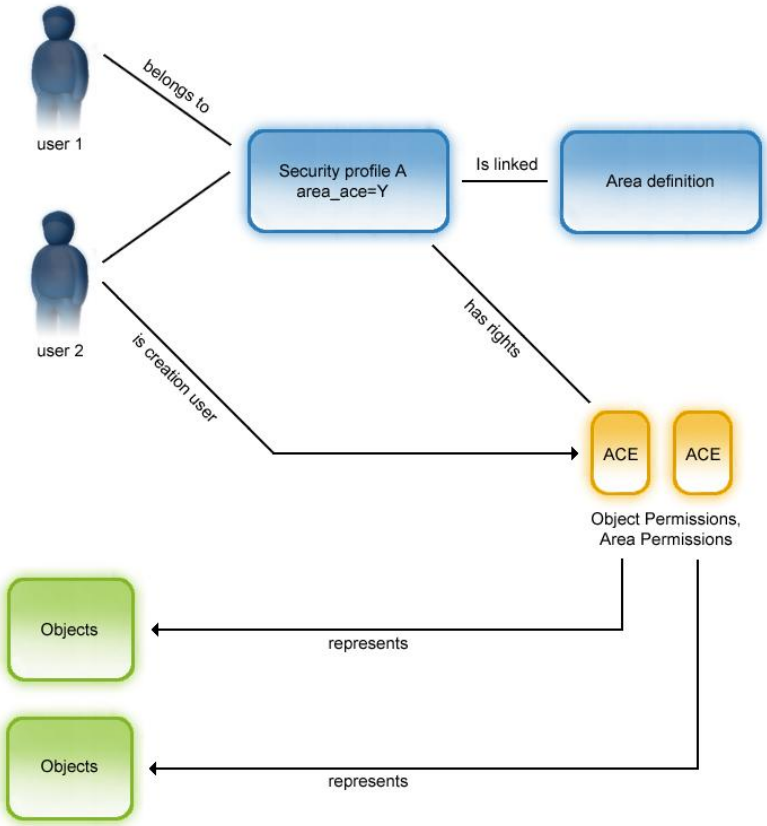
Three users, HRManager, SeniorManager, and DevManager have the user profiles HRMgrProfile, SrMgrProfile, and DevMgrProfile (with all access rights) assigned. Two security areas have been defined, HumanResources and Development. The profiles HRMgrProfile and SrMgrProfile are linked to the security area HumanResources. The profiles SrMgrProfile and DevMgrProfile are linked to the security area Development. Then SeniorManager, represented by SrMgrProfile, has access to both security areas, HumanResources and Development. HRManager has only access rights to security area HumanResources and the user DevManager has only access rights to security area Development. If HRManager, for example, creates a query on his console in the HumanResources area, this is not visible for the user DevManager. Only objects created by the system are visible for all user profiles.



Setting area permissions lets you restrict the access rights on a particular object of one or more profiles. That means that even the class-level permissions defined for a profile are the same. You may assign or link an object to different areas or restrict the access for profiles to see only objects that are linked to a certain area.

In addition to the object permissions, which are basically managed by the security classes, the security subsystem allows to create up to 32 areas.

The following illustration gives you an overview of the area support of the security subsystem.



User 1 and user 2 belong to security profile A. In the area definition, which is linked to profile A, it is defined which areas are visible to the users belonging to security profile A.

User 2 created an object, which is visible to all users who are linked to the appropriate area.

For important use cases and the descriptions of what area support is doing in the context of these use cases refer to the section "Security Area Support Use Cases" (see page 537).

Preconditions for Object Access in Areas

The following conditions must be fulfilled before the area permission of the user is evaluated:

- The user must have object access (View or Read) to the object.
- The security area support on the domain manager must be enabled.
- All security profiles that the user is member of must be enabled for security area support.

If the first condition is not fulfilled, the object access for the user is denied regardless of the second and third condition. If the second or third condition is not fulfilled, the user will not be restricted based on the area permissions and be allowed to access all the objects.

Notes:

- All objects are accessible to the users who are members of security area disabled security profiles. We recommend that the administrator ensures that all security profiles are enabled for security area support.
- Security area support is not available on the DSM enterprise managers.
- The “Distributions” profile is the only built-in profile that can be enabled for security area support. All other built-in profiles are disabled for security area support.
- Objects belonging to the "Procedure" or "Software Job" security classes cannot be linked to any security area within the DSM Explorer. They are automatically linked to the areas their parent containers, "Software Package" and "Software Job Container", are linked to.

Area Permissions Derived

Area permissions can be set or are derived in the following ways:

Area permission from security profile

If the creation user is valid when a secured object is created, then the area permissions are derived from the user who created the object.

(Security level: Creation User)

Area permission from a group

This case only applies when the secured object is member of a group and inheritance is enabled.

(Security level: Group)

Area permission set manually

A user may set the area permission for a certain object manually.

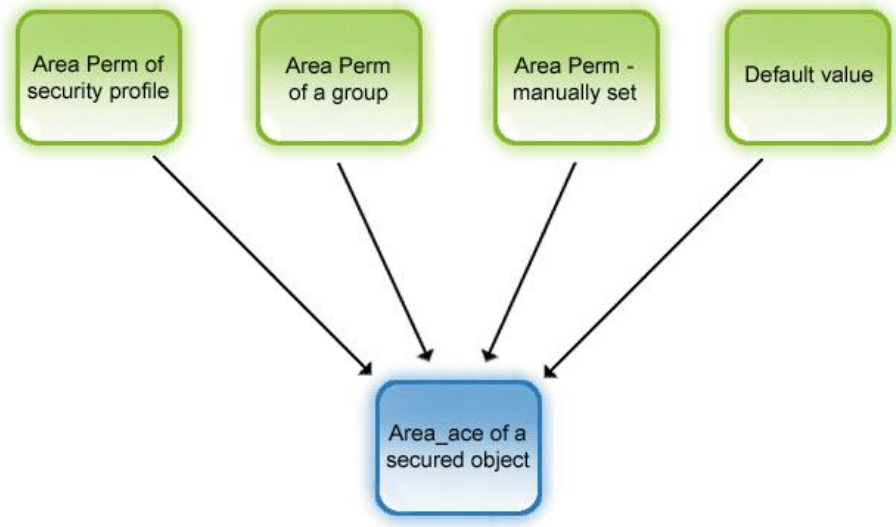
(Security level: Object)

Area permission by default

If a secured object is created and the creation user is not set or could not be found in the user list, then the area permissions are derived from the global configuration settings (global default permissions).

(Security level: Global Settings)

The following illustration shows the different ways an object's area permission can be derived:



Replication

The security subsystem excludes the authorization data from the replication between enterprise and domain tiers. The large number of objects holding the permission data makes them unsuitable for replication. Instead the security will be "reset" for an object that is moved from one database to another.

That means that the permissions (object and area permissions) will be re-calculated as soon as a replicated secured object is created. This is valid for upward and downward replication. For example, replication of Area Definitions is not needed.

- **Pre-Conditions**
  - A query is created on enterprise level by a user X.
  - User X has only access to areas 1 and 2.
  - User X is also known on the domain tier and has only access to area 5.
- **Action**

  A query is replicated downward.
- **Post-Conditions**
  - A query is created at domain tier.
  - The area permission is set as defined by the creation user, in this case, for the user X.
  - User X on domain tier will not see the query because the user has no area permissions on area 1 and 2.

Limitations

- Software Delivery tasks are always visible under the control panel for all Administrators because the tasks are not secured (neither objects nor area permissions). However the task list is read-only.
- Permissions for Software Delivery application objects are derived from the target object.
- The number of areas is restricted to 32.

Security Scenario - Software Delivery

The following scenario gives you a better understanding of the security concept.

Scenario:

You want to allow a user to create software and have full permissions to edit and distribute this software for a specific group of computers. At the same time, you want to deny these permissions to other users.

You can create more than one user group, thus creating independent islands of subadministrators.

Open the Security Profiles dialog. Do not make changes to the Everyone and Owner/creator groups, and you can reserve the Administrators group for users with more overall privilege. So for this scenario you should define some new security profiles.

To implement the above scenario

1. Create a new security profile, USER1 (a user account), that will have restricted usage.
2. Set the class permissions for this profile as shown in the following table, using the Administrator group:

Object Class	Class Permissions	Comments
Software Package	Special Access (C)	Creates the software package. No other rights are required as you are the owner of the software package after you create it.
Procedure	Special Access (C)	Creates a procedure.
Software Job	Special Access (C)	Creates a software job on the target computer.
Software Job Container	Special Access (CVRW)	Creates, writes, and views the job container. This is available under the Jobs, Software Jobs, All Software Jobs folder.
All Other Object Classes	No Access	Restricts the user from accessing other objects.

3. Navigate to the asset group on which you want to distribute the software and set the group permissions for this profile as follows:
   - Object access: Manage (VRX)
   - Members access: Manage (VRX)

   Note: The specific asset group must be a security group with the Members inherit permissions option.
4. Set Read (VR) permissions for the Domain (node), Computer and Users, and Software Package Library objects in the Object Permissions dialog.

Jobs that the user creates are visible to the user.

Set up another similar security profile, USER2. USER2 will not have access to USER1's computer, software groups, and jobs, and conversely.

If USER1 looks at the installations on the computers in Special, the ordered installations will be visible. Also, the Software Delivery software installed on these computers is visible to USER1 here, but nowhere else.

Configuring Common Security

Configuring security is one of the crucial steps after installation, as it provides the gateway to the CA IT Client Manager system. You can decide the security model that suits your organization and set up the security system accordingly. Decision on the security model can be made based on the following factors:

- Individual users and groups (both local and domain) who need access to the system.
- The type of access, say, read, write, execute and so on, required by each user and group.
- The level of permission required, say, class, group, object or area level permissions.

Note: If a user has two profiles, one mapped to his user account and the other mapped to a group, then the resulting permissions is the union of permissions in both the profiles. This rule is also valid, if a user is member of several groups which are defined as security profiles.

By default, the members of the administrators group are granted full access control. So, once the installation of CA IT Client Manager is complete, any member of the administrators group can login to the DSM domain and create further users and grant access rights.

How Security Is Set Up

Setting up security-controlled access to the system involves the following tasks. Understanding these tasks helps you set up a powerful and efficient security system.

- Add security profiles to the system. By default, predefined profiles are added to the security system and cannot be removed.
- Specify class permissions for the object classes that are listed in the Class Permissions dialog.

  Make sure that you restrict profiles from changing access rights to security profiles, security areas and class permissions object classes. Open the profiles and set their class permission access type to No Access for these three object classes.

However, to fine tune the security system further, you can do the following:

- Set the group access or object access for each folder, or object visible in the Explorer.
- Use Special Access to select any combination of access permissions: view, read, write, delete, execute, change permissions and take ownership.

Any operating system user with a valid account on the domain manager can connect to the system, that is, a user need not be an Administrator anymore. Access to system features and functions is controlled by its internal security mechanisms. By default, Administrators and the owner get full access, everyone else gets No Access. However, you can change access rights by updating the permissions after installation.

Note: If you are connected to the enterprise manager, ensure that you have an account with sufficient user rights (or user group rights) for accessing the security functions on each downstream domain manager. If you are connected to a domain manager, ensure that you have an account with sufficient rights for accessing the security functions on the enterprise manager.

Add Security Profile

Creating a security profile means mapping a new one to either a user account or group provided by the current security providers. You can select the users or groups who can access the system and add them to a security profile.

To add security profiles

1. Select Security Profiles from the Security menu.

   The Security Profiles dialog appears.

   Note: You must have sufficient access rights to open this dialog; otherwise, a security error message is displayed. Administrators have these access rights by default.

2. Click Add.

   The Add Security Profiles dialog appears.

3. Select the security authority from the Available Directories tree, browse and click the required security principal.

   You can view the selected security authority and principal in the Container Identifier and Names fields, respectively.

4. Double-click a principal in the tree, or click Add to List.

   The security principals shown in the Names field are added to the List of security profiles.

   To add more profiles, repeat the last two steps on the Add Security Profiles dialog.

5. Click OK.

   The selected user account or group is mapped to the security profile and the Class Permissions dialog is displayed.

   Note: If you have added more than one security principal, the Class Permissions dialog is not displayed. You must select the profile in the Security Profiles dialog, and click Class Permissions.

6. In the Class Permissions dialog, select the object class to which you want to assign the rights.

   Note: You can select multiple object classes and specify the class permissions for all of them. For continuous selection, press the Shift key and then click the objects; for random selection, press the Ctrl key and then click the objects.

7. Select the permission in the Class access drop-down list, and click OK.

   The given permissions are assigned to the new security profile.

The Add Security Profiles dialog displays a list of available security authorities: Windows NT domains, UNIX authentication targets, external directories such as NDS and LDAP, and the X.509 certificate subsystem.

This list of available security authorities is stored at the manager. When running in a Windows NT domain environment, the manager node will automatically calculate all explicit domain trusts available. These are returned for display when the list of available security authorities is requested by the Add Security Profiles dialog.

In some cases you may wish to use an implicitly trusted domain when creating security profiles - a domain that is not in the directly calculated list. To enable this, the Security Profiles dialog allows you to add and remove authorities, but only within the Windows NT name-space (winnt).

To add an implicitly trusted domain, click Add and enter the domain name in the new dialog. After clicking OK, the domain will be added to the list of available authorities. To remove an implicitly trusted domain, highlight the domain you wish to remove and click Remove.

Adding a domain to the authorities list does not confer trust to that domain; this is enforced by the operating system. It is not possible to add a domain to this list and have the manager trust this domain unless the underlying operating system already trusts the domain in question.

Predefined Access Types

Access types denote the rights to access an object or folder. An access type takes one of the following values:

View

Permissions to view (V)

Read

Permissions to view and read (VR)

Manage

Permissions to view, read and execute (VRX)

Change

Permissions to view, read, write, execute and delete (VRWXD)

Full Control

Permissions to create, view, read, write, execute, delete, change permissions and take ownership (CVRWXDPO)

Special Access

If you want any other combination of rights to be granted, select Special Access. The Special Access dialog appears with all the rights.

No Access

Blocks the user from accessing the objects in the object class.

Note: Do not assign this value to the group Owner / Creator. It could completely block the access to the application.

The following example shows the results of various access rights on the Computer object class:

Class Access	Resulting Permission
View	Displays all computers under the All Computers folder.
Read	Lets you view the properties of the computers.
Manage	Lets you deploy a software package or run a job on a computer.
Change	Lets you add a new computer or delete a computer.
Full Control	Gives you full control on the computers.

Specify Class Permissions

You can change the class permissions assigned for a security profile.

To specify class permissions

1. Select Security Profiles on the Security menu.

   The Security Profiles dialog appears.

2. Select the security profile for which you want to change the class permissions and click Class Permissions.

   The Class Permissions dialog appears.

3. Select the object class to which you need to assign the rights.

   Note: You can select multiple object classes and specify the class permissions for all of them. For continuous selection, press the Shift key and then click the objects; for random selection, press the Ctrl key and then click the objects.

4. Select the class permissions in the Class access field and click OK.

   The members of the selected security profile are now allowed to access the object class to the specified extent.

   To specify different combinations of rights, select Special access in the object access drop-down list.

Specify Object Permissions

You can specify object permissions for each object, such as a computer, a user, a job, and so on. By default, an object inherits the class permissions from its object class.

Note: Object permissions takes precedence over class and group permissions.

To specify object permissions

1. Select the objects and do one of the following:

   - Select Permissions from the Security menu.
   - Right-click the object and select Permissions from the context menu.

   The Object Permissions dialog appears.

   Note: You can select multiple object classes and specify the class permissions for all of them. For continuous selection, press the Shift key and then click the objects; for random selection, press the Ctrl key and then click the objects.

2. Select the required access type from the Object access drop-down list and click OK.

   The members of the profile can access with the rights granted to them.

   To specify different combinations of rights, select Special access in the object access drop-down list.

Specify Group Permissions

Group permissions can be specified for any user-created folders.

Note: In the order of precedence, object permissions precede over group permissions, which precede over class permissions. That means setting class permissions do not replace individually specified object and group members permissions.

To specify group permissions

1. Select the folder and do one of the following:
   - Select Permissions from the Security menu.
   - Right-click the group and select Permissions from the context menu.

   The Security Group Permissions dialog appears, where you can set the group level permissions.
2. Select a profile and specify the object access and member access.

   Note: Selecting Default overrides the member permissions with the class permissions.

   The members of the profile are now allowed to access the folder or group to the specified extent.

   To specify different combinations of rights, select Special access in the object access drop-down list.

Cumulative Permissions

Permissions are always cumulative for the mapped security profiles as explained in the following statements and examples:

- If a user is a member of more than one security group, the rights of each group is OR'ed together to determine the user's access rights.

  For example, if a user is a member of two groups and one of the groups has Write access for an object and the other Read access, the user will have Write access.
- Object level permissions override group level permissions, which in turn override class level permissions.

Examples:

- To expand any folder, for example to list the computers in a group, you must have Read rights for that folder.
- To create an object, you must have the Create rights on the object.

  If the created object should be placed in a folder, you must also have Read and Write rights for the folder.
- The Paste and Link operations require Write rights on the current folder or object (for example, when pasting files and folders).
- The Move operation requires Write rights on two folders or objects, both the source and destination.

Security Area Support

A security area is a geographical, organizational, or topological division. A security area can be linked to one or more security profiles and one or more objects. A user can access an object, if at least one security area linked to the object is also linked to at least one security profile of the user.

For important use cases and the descriptions of what area support is doing in the context of these use cases, refer to the section "Security Area Support Use Cases" (see page 537).

In the following sections you will find information on how to work with security areas.

Global Settings for Security Areas

Global settings define the status of the security area support and whether system created objects are shown or hidden in the security area. You can change the global settings in the Security Areas dialog which is available through the Security menu.

The security area support on the domain manager is turned off by default. You must turn on the area support to implement the security area feature in your security system, though you can create and link areas with profiles and objects even without turning on this option. To turn on the security area support on the domain manager, select the On option button in the Security Area support field.

By default, security areas are configured to show system created objects. If you want to hide system created objects in a specific security area, clear the check box next to the security area name in the Security Areas dialog.

Enable Security Area Setting for a Security Profile

You must enable the security area support for each suitable security profile to implement this feature at the security profile level.

To enable security area setting for a security profile

1. Select Security Profiles from the Security menu.

   The Security Profiles dialog appears.

2. Select the security profiles for which you want to enable the security area settings and click Security Areas.

   The Security Area Linkages dialog appears.

3. Select the Enable Security Area support for Profile check box.

   The icon next to the check box shows a green tickmark to indicate that the security area support is enabled.

Create a Security Area

You can create areas for each geographical, topological, or organizational divisions or any other kind of area management you choose.

To create a security area

1. Select Security Areas from the Security Menu.

   The Security Areas dialog appears.

2. Click Add.

   The New Security Area dialog appears.

3. Enter a name and description for the new area and click OK.

   The new area is added to the list of security areas in the Security Areas dialog and the Security Profile Linkages dialog appears where you can link the security profiles with the new area.

Delete a Security Area

You can delete a security area when you no longer need it. A deleted security area is removed from the system and is automatically unlinked from all the linked profiles and objects.

To delete a security area

1. Select Security Areas from the Security Menu.

   The Security Areas dialog appears.

2. Click Delete.

   A confirmation message appears.

3. Click Yes.

   The security area is deleted.

Link or Unlink the Security Area to or from the Security Profiles

Linking a security profile to a security area lets users or groups access only those objects that are linked to their security areas. You can link a security profile to one or more suitable security areas. In the case of multiple areas, users will have access to the objects linked to all the security areas they belong to.

You can unlink a security area if the user no longer belongs to that area.

To link or unlink the security areas

1. Select Security Profiles from the Security Menu.

   The Security Profiles dialog appears.

2. Select the security profiles and click Security Areas.

   The Security Area Linkages dialog appears listing the linkage status of the selected profiles.

3. Select the security areas and click Link or Unlink.

   The selected security profiles are linked or unlinked from the security areas.

Link or Unlink the Security Area to or from the Secured Objects

Linking a secured object to a security area lets only the users belonging to that area have access to the object. You can link a secured object to one or more suitable areas. In the case of multiple areas, the object will be accessible to the users linked to all the security areas to which the object belongs.

Note: When you link or unlink an object to or from a group, the object automatically inherits the group area permissions regardless of whether the area permissions for the object are defined. If you want to retain the object level area permissions, you must review and modify the area permissions after linking or unlinking the object.

To link or unlink the security areas

1. Select the objects in the Explorer and right-click.

   The context menu appears.

2. Select Permissions.

   The Object Permissions dialog appears.

3. Click Security Areas.

   The Security Area Linkages dialog appears, listing the linkage status of the selected objects.

4. Select the security areas and click Link or Unlink.

   The selected secured objects are linked or unlinked from the security areas.

Configuring Encryption

CA ITCM provides support for stronger encryption algorithms, in particular the Advanced Encryption Standard (AES), within the session messaging subsystem and directly related components.

You can configure the encryption algorithms that are used for communication to other partners using the encryption policies. This configuration is valid for communication using session messaging, Software Delivery store-and-forward, Remote Control viewer/host communication, the DTS agent, and the Software Delivery server for NOS-less file transfer.

The available encryption algorithms, the selection of the best algorithm for communication, and the communication with pre-r11.2 partners are considered in the following sections:

- Encryption Algorithms for Communication (see page 414)
- How the Matching Encryption Algorithm is Chosen (see page 414)
- Encryption in Top Secret Environments (see page 415)
- Communication with Older Versions (see page 416)

Encryption Algorithms for Communication

The encryption algorithms used for communication and their preferred order are defined in an encryption policy, the cipher preference list.

When a communication should be established, the defined algorithms of both communication partners are considered and the most preferable matching algorithm in the list is chosen for the session following. To establish a communication session, at least one common algorithm must be shared by both communication partners.

The following list shows the available encryption algorithms, sorted by increasing order of their strength (that is, AES-256 is the strongest algorithm):

Triple-DES (Data Encryption Standard)

Indicates a symmetric key according to the Data Encryption Standard with a key length of 168 bits.

AES-128 (Advanced Encryption Standard)

Indicates a symmetric key according to the Advanced Encryption Standard with a key length of 128 bits.

AES-192

Indicates a symmetric key according to the Advanced Encryption Standard with a key length of 192 bits.

AES-256

Indicates a symmetric key according to the Advanced Encryption Standard with a key length of 256 bits.

Selection of the Matching Encryption Algorithm

Each communication partner has a list of preferred ciphers defined in the encryption policy, with the most preferable cipher in first position of the list. The lists of both communication partners are compared and evaluated according to the following rules:

- For each list, the ciphers are taken from the first to the last and the matching cipher is searched in the other list until there is a match or the list ends.
- If there are two matching ciphers, the stronger one is used for the following session.
- If there is one matching cipher, this cipher is used for the following session.
- If no matching cipher was found, communication is not possible.

Example:

The cipher list of partner A contains: Triple-DES, AES-192, AES-128. The cipher list of partner B contains: AES-256, AES-128, Triple-DES, AES-192.

The system performs the following steps to identify matching ciphers:

1. Go through the cipher list of partner A:

   The first entry, Triple-DES, is searched in the list of partner B.

   A match is found; Triple-DES is the first matching cipher.

2. Go through the cipher list of partner B:

   The first entry, AES-256, is searched in the list of partner A.

   No match is found.

   The second entry, AES-128, is searched in the list of partner A.

   A match is found; AES-128 is the second matching cipher.

3. The system considers AES-128 stronger than Triple-DES and uses this algorithm for the subsequent session.

Note: Only the first two matches are considered; no further search and compare action is performed on the two cipher lists.

Encryption in Top Secret Environments

For customers who need encryption in their top secret environment we recommend that you first install the manager and change the default policy for the cipher preferences to have only AES-256 in the list and to set the property DSM/common components/encryption/compatibility/pre_11_2 to "False".

As soon as the configuration change takes place at the agent on the manager system (that is, the configuration job has finished), it is safe to install additional scalability servers.

At the scalability server level you must check if the cipher list was spread out by typing the commands:

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences
-pncipher0

ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences
-pncipher1

ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences
-pncipher2

ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences
–pncipher3
```

Cipher 0 should contain AES-256, the other ciphers should be empty. This could be done at manager level or agent level to check if the cipher configuration has already arrived.

Now it is safe to install agents that point to that server. The agents will use AES-256 encryption for their communication right away.

As soon as the common configuration is spread out to agents, they also have only AES-256 in their cipher list and fail to communicate when contacted with any other cipher.

Communication with Older Versions (Compatibility Policy)

To communicate with pre-r11.2 partners, the pre_11_2 compatibility policy must be set to True.

With the default configuration, this policy value is set.

When there are no pre-r11.2 installations left in the whole environment, you should set the pre_11_2 compatibility policy to False to improve the establishment of a session.

FIPS-Compliant Cryptography

CA ITCM supports FIPS-compliant cryptography in two modes—FIPS-preferred and FIPS-only. You can switch to FIPS-only mode after all the components in your infrastructure have been upgraded or are operating in FIPS-preferred mode. You can also switch back to FIPS-preferred mode if necessary.

More information:

FIPS 140-2 Support (see page 75)

Before You Switch the FIPS Mode

Before you switch the FIPS mode of your CA ITCM infrastructure, you must understand the practical considerations for operating in a particular FIPS mode. This section lists the considerations and prerequisites that you must review before switching the FIPS mode.

Mixed FIPS Modes

When your CA ITCM infrastructure is operating in mixed FIPS modes, that is some components in FIPS-preferred mode and others in FIPS-only mode, the following restrictions apply:

- Some of the OSIM functionalities may not function correctly when the following components communicate:
  - FIPS-preferred domain manager to FIPS-only scalability server
  - FIPS-preferred enterprise manager to FIPS-only domain manager
- Communication between the following components fail:
  - CA ITCM r12 components to FIPS-only DSM components

The following considerations apply when you are linking a domain manager to an enterprise manager:

- You can link only FIPS-only domain managers to a FIPS-only enterprise manager.
- When the FIPS mode of the domain manager or the enterprise manager is FIPS-Preferred (Ready for FIPS-Only) or FIPS-Preferred (Re-run conversion for FIPS-Only), you cannot perform a link operation.
- If the enterprise manager is in FIPS-preferred mode, you can link FIPS-preferred or legacy domain managers to it.

FIPS-Preferred to FIPS-Only Mode

The following operations or functionalities are not supported after you have switched from FIPS-preferred to FIPS-only mode:

- PLAIN and CACRYPT encryption filters for DTS
- ADT functionality of trusted transfers and DTS domains
- DTS transfer using multicast or broadcast to a group of computers operating in both FIPS-only and legacy mode
- Create or open password encrypted DNA files
- Use of legacy OS and boot images that are not yet upgraded. For information about upgrading images, see the *OS Installation Management Administration Guide*.

Prerequisites

You must verify that you have done the following before you switch the FIPS mode:

- If you are upgrading a cluster, disable automatic start of CA ITCM on all nodes of a cluster prior to upgrading. You can enable the services when all the nodes in the cluster have been upgraded.
- Close all the instances of DSM Explorer (local and remote), Web Console, and CLI sessions when you are running the conversion utility; Do not open new instances of these until the conversion utility has completed the execution.
- Verify that all the configuration policies on the enterprise and domain managers are sealed.

How to Switch to FIPS-Only Mode

Switching the CA ITCM infrastructure to FIPS-only mode allows the use of only FIPS-compliant cryptography. After you switch to the FIPS-only mode, the components cannot communicate with r12 components.

Note: We recommend that you use the FIPS-preferred mode until you are ready to use only FIPS-compliant cryptography.

The following process describes the steps for switching your CA ITCM infrastructure to FIPS-only mode:

Note: The steps pertaining to an enterprise manager apply only if you have a CA ITCM enterprise manager in your environment.

1. Verify that all the DSM components have been upgraded to Release 12.8.
2. Update all OS and boot images to FIPS-compliant format. For more information about updating images, see the *OS Installation Management Administration Guide*.
3. Run the conversion utility on the enterprise manager. The utility converts global OSIM configuration policies to FIPS-compliant format, and distributes managed values and parameter definitions to all the domain managers.
4. Check the Event Log on the enterprise manager to verify that the policy has been successfully replicated to all the domain managers.
5. Run the conversion utility on the domain managers. The utility converts local OSIM configuration policies and distributes managed values to all the components in CA ITCM infrastructure.
6. Modify the default configuration policy on the enterprise manager to switch to FIPS-only mode.

   Note: Changing the FIPS mode through custom configuration policies is not recommended.

7. Check the Event Log on the enterprise manager to verify that the policy has been successfully replicated to all the domain managers.
8. If you do not have an enterprise manager, modify the default configuration policy on the domain managers to switch to the FIPS-only mode.

Note: You must restart CAF for the FIPS mode to take effect.

More information:

Supported FIPS Modes (see page 76)
Run the Conversion Utility (see page 420)
Modify the Configuration Policy to Change the FIPS Mode (see page 421)

How to Switch to FIPS-Preferred Mode

In rare circumstances, you may need CA ITCM to communicate with components that are not FIPS-compliant, a legacy agent for example, after you have switched the infrastructure to FIPS-only mode. As FIPS-only mode does not support backward compatibility, you need to switch it back to FIPS-preferred mode.

The following process describes the steps for switching your infrastructure to FIPS-preferred mode:

Note: The steps pertaining to an enterprise manager apply only if you have a CA ITCM enterprise manager in your environment.

1. Modify the default configuration policy on the enterprise manager to switch to the FIPS-preferred mode.

   Note: Changing the FIPS mode through custom configuration policies is not recommended.
2. Check the Event Log on the enterprise manager to verify that the policy has been successfully replicated to all the domain managers.
3. If you do not have an enterprise manager, modify the default configuration policy on all the domain managers to switch to the FIPS-preferred mode.

   Note: You must restart CAF for the FIPS mode to take effect. You must have restarted CAF at least on the enterprise or domain manager before you run the conversion utility on it; otherwise, the conversion utility will fail.
4. Run the conversion utility on the enterprise manager to convert global OSIM parameters to backward compatible format.

5. Check the Event Log on the enterprise manager to verify that the policy has been successfully replicated to all the domain managers.
6. Run the conversion utility on the domain managers to convert local OSIM parameters to backward compatible format.

More information:

Supported FIPS Modes (see page 76)
Run the Conversion Utility (see page 420)
Modify the Configuration Policy to Change the FIPS Mode (see page 421)

Run the Conversion Utility

Running the conversion utility configures DSM components to use the required FIPS mode. Run this utility in the following order:

- Enterprise manager (if present)
- Domain managers

To run the conversion utility

1. Verify that all the configuration policies are sealed on the manager.
2. Open the command-line window and navigate to the *ITCM_installpath*\bin folder.
3. Execute the following command:

   `dmscript dsm_fips_conv.dms` *`FIPS_Mode`*

   FIPS_Mode

   Specifies the FIPS mode you want to switch to. Valid values are FIPS-Only and FIPS-Preferred.

   After the utility completes, it returns a success or failure message. If you have executed the utility with the FIPS-ONLY parameter, the utility changes the FIPS mode of the corresponding manager depending on the success or failure of the utility execution.

4. Open DSM Explorer on the manager, click the root node, and check the System Status portlet for FIPS-140.

   The FIPS-140 setting displays the FIPS mode of the manager.

   - If the utility had executed successfully, this setting displays FIPS-Preferred (Ready for FIPS-Only). You can proceed to modify the configuration policy to change the FIPS mode in this case.
   - If the utility had failed, the setting displays FIPS-Preferred (Error Running dsm_fips_conv). The manager continues to operate in this mode until the conversion utility is successfully run on the manager.

   Note: When the manager is operating in any of these two modes, r12 clients (DSM Explorer, CLI, and so on) are prevented from connecting to the manager.

5. Perform the following steps, if the utility had completed with errors or warnings:

   a. View the log file osimfiputil.log in the *ITCM_installpath*\bin folder if the script completed with errors or warnings. You can also find more information in the Event log.

   b. Take corrective actions to fix the errors and run the conversion utility again.

      The DSM components are configured to use the required FIPS mode.

Example: Command for running the conversion utility for FIPS-only mode:

```
dmscript dsm_fips_conv.dms FIPS_ONLY
```

More information:

How to Switch to FIPS-Only Mode (see page 418)
How to Switch to FIPS-Preferred Mode (see page 419)
Verify the FIPS Mode of DSM Components (see page 424)

Modify the Configuration Policy to Change the FIPS Mode

You must modify the FIPS-related policies in the default configuration policy to change the FIPS mode of your CA ITCM infrastructure. These policies determine the FIPS mode you want to switch to and the action to take before switching the FIPS modes.

If you have an enterprise manager, perform the following steps on the enterprise manager. The policy changes, in this case, are automatically propagated to all the associated domain managers, scalability servers, and agents. If you do not have an enterprise manager, perform the following steps on all the domain managers.

Note: Perform this task only if the FIPS mode of the manager is FIPS-Preferred (Ready for FIPS-Only).

To modify the configuration policy to change the FIPS mode

1. Navigate to Control Panel, Configuration Policy, right-click Default Configuration Policy, and click Un-Seal.

   The policy is unsealed and is ready for updates.

   Note: Changing the FIPS mode through custom configuration policies is not recommended.

2. Navigate to DSM, Common Components, Security, FIPS 140 Settings and modify the following policies:

   FIPS 140 Setting

   Defines the FIPS compliance level. Modify this setting to specify the FIPS mode you want to switch to.

   Change action

   Defines the actions to take when the FIPS 140 setting is changed.

   Note: For more information about the policy values for these settings, see the *DSM Explorer Help*.

3. Seal the policy on the manager. For more information about sealing the policy, see the Configuration Policy section of the *DSM Explorer Help*.

   The policy changes are propagated to all the associated DSM components. This process takes sometime depending on the size of your CA ITCM infrastructure.

4. Change the FIPS mode of the following components manually as the policy changes will not be automatically propagated to these components:

   - Stand-alone remote control agents
   - Unmanaged DSM agents on the enterprise manager

     Note: An unmanaged agent is the one which is not linked to any domain manager. If you link the unmanaged agent to a domain manager subsequently, the FIPS mode of the agent will be overridden by the FIPS mode of the domain manager.

   To change the FIPS mode manually, use the following command:

   ```
   ccnfcmda –cmd setparametervalue –ps /itrm/common/security/fips140 –pn
   installmode –v FIPS_MODE
   ```

   FIPS_MODE

   Specifies the FIPS mode. Specify 1 for the FIPS-preferred mode and 2 for the FIPS-only mode.

   When the command is successfully executed, the specified FIPS mode is set on the agent.

   Note: Stand-alone DSM Explorer and DSM Reporter do not require any specific configuration as the DSM agent is always installed along with the stand-alone installation of these two components. The agents automatically receive the policy update from the manager in this case.

5. Execute the following command on all DSM components, if you have not modified the Change action policy default setting or you have set it to "Switch FIPS mode on next restart of ITCM":

   ```
   caf stop
   caf start
   ```

   After the caf restarts, the manager operates in the new FIPS mode.

6. Restart all the instances of DSM Explorer, DSM Reporter, and Web Console.

   The updated FIPS mode is now available in the GUI.

7. Verify that the FIPS mode of the agents and managers are changed to the required FIPS mode.

   The verification helps ensure that the switch is successful.

   Note: If the conversion utility is not executed successfully, the FIPS mode of the manager remains as FIPS-Preferred (Error Running dsm_fips_conv).

More information:

How to Switch to FIPS-Only Mode (see page 418)
How to Switch to FIPS-Preferred Mode (see page 419)
Verify the FIPS Mode of DSM Components (see page 424)
Scenarios When the FIPS Policy Changes Do Not Take Effect (see page 427)

Verify the FIPS Mode of DSM Components

You can view the FIPS mode of DSM managers, scalability servers, and agents to verify whether the switch operation is successful. The FIPS mode is available as an inventory data.

To view the FIPS mode of DSM components

1. Click the root node in the DSM Explorer.

   The System Status portlet.displays the FIPS mode of manager.

2. Navigate to Computers and Users, All Computers, *Computer_Name*, Inventory, System Status.

   The FIPS Mode attribute in the right pane displays the FIPS mode of the selected computer.

Note: You can also run FIPS-specific queries and reports to view the FIPS mode of multiple agent computers and manager.

More information:

Predefined Queries and Reports for FIPS Mode (see page 425)

Predefined Queries and Reports for FIPS Mode

The following predefined queries and the report let you view the FIPS mode of the DSM components in your infrastructure:

Queries

Assets Running in FIPS-Only Mode

Assets Running in FIPS-Preferred Mode

Assets Running Without FIPS Support

Reports

All Computers by FIPS Mode

Note: The FIPS mode of r11.x or r12 agent computers that are connected to a Release 12.8 manager (operating in the FIPS-preferred mode) is reported as "NONE". The FIPS mode of NRI agents is reported as "N/A."

Configure FIPS-Compliance for DSM Web Components

You must configure your Web Console, browser, and the web server to help ensure that the communication between web components and other DSM components is FIPS-compliant.

To configure FIPS-compliance for CA ITCM Web Console

1. Configure SSL between the following components:
   a. Client browser and CA ITCM Web Console
   b. CA ITCM Web Console and CA ITCM web services

   Note: For more information about configuring TLS 1.0 on IIS, see the green paper titled *Securing the Web Admin Console Communication Using SSL*. For more information about configuring TLS 1.0 on Apache web server, see the Apache web server documentation.
2. Configure your browser to use TLS 1.0 for communication. For more information, see the browser documentation.
3. Configure SSL with FIPS-compliance on your web server. For information, see the your web server documentation.

4. Modify the settings in the *Install_Path*\Web Console\webapps\wac\WEB-INF\classes\com\ca\wac\config\WACConfig.properties file as follows:

   ```
   AMS_URL=https://hostname/AMS/login.do
   WEBSERVICE_URL=https://hostname/UDSM_R11_WebService/mod_gsoap.dll (For Windows)
   WEBSERVICE_URL=https://hostname/UDSM_R11_WebService (For Linux)
   SSL_Enabled=True
   TrustStoreFileFullPath=truststorepath
   TrustStorePassword=password
   ```

   The Web Console is configured to use TLS for all the communication.

5. Restart tomcat using the following commands:

   ```
   caf stop tomcat
   caf start tomcat
   ```

   The updated configurations take effect after tomcat is restarted successfully.

Repair a FIPS-Only Agent Connected to r12 Component

If a FIPS-only agent is connected to r12 manager or scalability server, they cannot communicate with each other because of incompatible FIPS modes. You must either upgrade the manager or scalability server, or change the FIPS mode of the agent to FIPS-preferred.

To change the FIPS mode of the agent to FIPS-preferred

1. Execute the following command at the agent:

   ```
   ccnfcmda –cmd setparametervalue –ps /itrm/common/security/fips140 –pn installmode –v 1
   ```

   When the command is successfully executed, the FIPS mode on the agent is set to FIPS-preferred.

2. Restart caf using the following commands:

   ```
   caf stop
   caf start
   ```

   When caf restarts successfully, the agent operates in the FIPS-preferred mode.

Scenarios When the FIPS Policy Changes Do Not Take Effect

After you change the FIPS 140 setting in the configuration policy and apply the policy on the manager, CA ITCM takes the action based on the value set in the Change action policy. In the following scenarios, the FIPS policy changes do not take effect and you do not see any action based on the Change action policy.

- The policy has not yet arrived at the target computer—check the settings on the target computer using the following command:

  ```
  ccnfcmda –cmd getparametervalue –ps /itrm/common/security/fips140 –pn policy
  ```

  The command returns 0 (legacy), 1 (FIPS-preferred), or 2 (FIPS-only). If the command returns the new FIPS mode value, the new mode will be effective when CA ITCM restarts and copies the new value to the installmode parameter. If the command does not return the new FIPS mode value, it indicates that the policy has not yet arrived at the target computer.

  To get the current FIPS mode on the target computer, use the following command:

  ```
  ccnfcmda –cmd getparametervalue –ps /itrm/common/security/fips140 –pn
  installmode
  ```

  Typically, the installmode parameter and the policy parameter must contain the same value. However, if CA ITCM has not been restarted after applying the policy, the installmode parameter will continue to hold the previous policy value until you restart CA ITCM.

  Note: For more detailed information about the ccnfcmda configuration agent command, type <command> /? at the command prompt.

- A FIPS-only policy is applied on a DSM manager that has either not executed the conversion utility or completed the conversion utility with errors. As the FIPS-only mode requires that the conversion utility must be successfully executed, changing the policy has no effect until you run the conversion utility successfully on the manager:

  To view whether conversion utility has been run on the manager, use the following command:

  ```
  ccnfcmda –cmd getparametervalue –ps /itrm/common/security/fips140 –pn
  ready_for_fips_only
  ```

  If the command returns 1, it indicates that the utility has been run successfully on the manager.

  Note: The conversion utility must have been run successfully if you are trying to switch from the FIPS-preferred mode to the FIPS-only mode or from the FIPS-only mode to the FIPS-preferred mode.

- The new FIPS mode is the same as the current FIPS mode. If the target computer is already operating in the same FIPS mode as the new FIPS mode, the changes do not take effect on the target computer.

- If the Change action policy is set to “Politely ask user to restart ITCM when ready”, then a dialog appears asking the user to restart CA ITCM when the policy reaches the target computer. If this dialog does not appear, check the restartaction parameter on the target machine using the following command:

  ```
  ccnfcmda –cmd getparametervalue –ps /itrm/common/security/fips140 –pn restartaction
  ```

  If the command does not return 2, it indicates that the policy has not yet arrived at the target computer.

  Important! Do *not* enable the “Politely ask user to restart ITCM when ready” option on a terminal server as it prompts all the users to restart CA ITCM!

Chapter 12: Extended Network Connectivity (ENC)

This section contains the following topics:

Introduction to Extended Network Connectivity

CA IT Client Manager (CA ITCM) provides the Extended Network Connectivity (ENC) feature that allows DSM components and services to establish connections between end points that are

- Behind personal or network firewalls
- In different IP address spaces

ENC provides a virtual network environment where you can create connections between different DSM components that are all operating behind different firewalls or DMZs (demilitarized zones). This includes enterprise managers, domain managers, GUI, scalability servers, and agents.

Important! ENC can be used only by authorized, authenticated applications to connect to specific end points that already have ENC-enabled applications installed for very specific purposes. ENC does not provide a general channel through the firewall that can be used by other applications.

If two computers want to connect but cannot normally do so because of a firewall in the way, ENC arranges for both computers to connect to a third computer (ENC Router) that relays data between the two computers.

The ENC Gateway provides secure connections through firewalls by requiring the following:

- All connections through the ENC Gateway virtual network must be correctly authenticated by means of certificates.
- All connections must be correctly authorized. The authorization rules are set by policy and configure who can connect to whom at what time and for what operation. This is especially important when connecting across the public network or an internet.
- All connection attempts and other operations can be audited for security and troubleshooting purposes.

ENC Components

ENC uses specific components in the CA IT Client Manager environment, including the following:

ENC Client

Runs on all ENC Gateway-enabled computers and co-ordinates all connections made by applications over the ENC Gateway network. ENC Clients maintain a connection to an ENC Gateway Server.

ENC Gateway Server

Acts as a scalability server for the ENC Gateway by accepting connections and registrations from ENC Clients and passing them on to the ENC Gateway Manager. Multiple servers can be used in an ENC network.

ENC Gateway Manager

Arranges all connections between end points. The ENC Gateway Manager knows about all ENC Gateway Servers, clients, and routers because these components register when they start up. Only one ENC Gateway Manager is allowed in an ENC network.

ENC Gateway Router

Relays data between end points. Multiple routers can be used in an ENC network.

Secure Socket Adapter

Provides the link between applications and the ENC network. It intercepts low level network calls and redirects them to direct connections, if possible, otherwise to ENC connections.

Note: The ENC Gateway is a single program that can operate as a manager, server, router, or any combination. The manager always has a server as well. The role is controlled by the following settings in the configuration store (comstore): itrm/common/enc/server - MRS, SRS, and Router. If a setting has the value of 1, the server takes on that role.

Supported Platforms

The operating system platforms that are supported by ENC are listed in the "Supported Operating Environments" chapter of the *CA IT Client Manager Release Notes,* available as part of the online CA ITCM documentation set (Bookshelf).

ENC Gateway Connection Process

The ENC Gateway functionality allows CA ITCM to communicate with computers behind firewalls. If two computers want to connect but cannot normally do so because of a firewall in the way, the ENC Gateway arranges for them both to connect to a third computer that can relay data between the two computers.

In an ENC Gateway network, the connection process between two end points (computers) is as follows:

- End point 1 wishes to listen for connections on some port. Two ports are opened, one real and one virtual. The real port accepts direct connections; the virtual port is maintained by the ENC Client and listens for ENC Gateway connections.
- End point 2 wants to connect. The Socket Adapter tries to establish a direct connection. If this succeeds (it may be in the same network), the ENC Gateway has no further part to play.
- If it fails, the Socket Adapter asks the ENC Gateway Manager to arrange a connection.
- The ENC Gateway Manager sends a list of known ENC Gateway Routers to both end points. Each end point pings the routers and returns the results. The ENC Gateway Manager chooses a router that can be reached by both end points and tells each one to connect to it.
- Each end point connects to the ENC Gateway Router, which then relays data between them.

This relies on end points being able to connect outward bound from the firewalls around their networks to ENC Gateway Servers and ENC Gateway Routers. Inward bound connections are never made, so no inward bound ports need to be opened.

ENC Gateway Security

The ENC Gateway allows communication through firewalls in a secure manner using the following security mechanisms:

- Authentication

  All ENC Gateway nodes (clients, managers, servers, and routers) must mutually authenticate with each other, using transport layer security (TLS), which is an updated version of Secure Sockets Layer (SSL). This authentication method requires the installation of certificates using the Microsoft PKI or similar.

- Authorization

  All ENC Gateways are configured with a set of rules that define who is allowed to do what at what time to whom. This takes the form of:

  - Realm membership of nodes (analogous to NT groups but working over different networks)
  - IP address white listing. This is a list of IP addresses that are allowed to establish ENC Gateway connections.
  - Allow or deny rules for each ENC Gateway operation such as connect, register, and so on, based on realm membership, time of day, and so on.
  - Time ranges

When first installed, an ENC Gateway is locked down. It has no authorization rules and so refuses all connections. This is appropriate because these servers are usually facing the Internet. This can introduce problems because CA ITCM is used to maintain the authorization rules, and a domain manager may be cut off from the computer that runs the ENC Gateway by a firewall. The steps around this are described in the Deployment Scenarios section.

Authentication

Both ends of a secured connection validate (authenticate) their peers' certificate (mutual authentication), including the issuing certificate authority.

To this end, both parties must have trust in the third-party certificate authority. ENC uses the Microsoft SCHANNEL TLS provider, and subsequently the WinTrust library, to enforce the certificate trust. The trust of the root (and possibly) intermediate certificates is provided by the operating system, using the certificate store and APIs.

ENC Gateway Authorization Rules

The ENC virtual infrastructure is protected by authentication, authorization, and auditing. Authentication is provided using the industry standard TLS protocol and is described in the Authentication (see page 375) and the ENC Gateway Authentication (see page 433) sections. The auditing component is also detailed in the Auditing Events (see page 449) section.

This section describes how and where authorization is used and will finalize with a worked example.

General Terms

The following is a list of terms used in the context of authorization rules. Some are industry standard and some have been adapted for use by ENC.

Security Principal

A security principal is an authenticated object – always a computer in ENC – that has proved its identity to the Gateway servers. The object is always referenced by its Uniform Resource Identifier (URI). This object is the entity making a request to access a secured object or operation. In ENC, a security principal is primarily an individual computer, though can also be referenced through a realm (group) of computers or a sub-group of computers defined by pattern matching against the URI.

Secured Object

The secured object is the target of an access request or operation. The secured object is always a computer named by URI, but access rules can apply to a single computer, a pattern matched set of computers, or a complete realm.

Realm

A realm is a logical grouping of computers for use by the authorization component upon a set of computers. In an outsourced scenario, a realm will usually represent computers at an organization or organizational unit level. Security Principals are mapped into a realm either by an exact match of the URI or by pattern matches against the URI.

Pattern Matching

ENC can use pattern matching in determining realm membership. The pattern matching uses regular expressions to perform the matching algorithm.

ENC uses PERL Compatible Regular Expressions (PCRE, see http://www.pcre.org/) for the pattern matching functionality. For the full syntax of PCRE, see http://perldoc.perl.org/perlre.html.

TACE – Timed Access Control Entry

A TACE is a rule that defines whether or not a given operation (or operations) can be performed by a security principal against a secured object at a certain time. Some rules deny access, whilst others allow access. Deny type TACEs take precedence over Allow types. Any operations that have no matching rules are implicitly denied.

Important! The active time of an access control entry is always the local time of the target of an operation. If an agent wishes to connect to another agent in another time zone, the ENC Gateway Manager node will validate the time range within the context of the target agent.

TACL – Timed Access Control List

A TACL is a list of TACE rules.

Infrastructure Nodes

This term refers to the ENC nodes that provide the ENC virtual network infrastructure, including the Manager, Server and Router nodes, but not the ENC agents themselves.

URI – Uniform Resource Identifier

A URI is a string used to name or identify or name a resource. ENC uses a URI to represent all authenticated objects.

ENC and Uniform Resource Identifiers

ENC Authorization uses Uniform Resource Identifiers (URI's) for its internal database. An ENC URI has the following format:

```
x509cert://[TLS-SCHANNEL]/CN=forward,OU=computers,DC=forward,DC=com
```

x509cert

Indicates the namespace. X509cert means that the URI represents an x.509 certificate identity.

[TLS-SCHANNEL]

Specifies the authority embedded in the URI. This special authority name shows that the authentication is devolved to the TLS SCHANNEL security provider and the WinTrust provider. These providers manage the certificate trust on ENC's behalf.

CN=forward,OU=computers,DC=forward,DC=dom

Defines the x.500 subject name as embedded in the certificate. The actual format and content of this name is provider-specific. The above example is from a certificate created by Microsoft Active Directory integrated Certificate Services. Different PKIs and manual certificate creation may use different naming conventions.

To find out a computer URI programmatically, you can use the encUtilCmd utility. Executing "encUtilCmd certv" shows the certificate identities that the machine uses for ENC authentication—both as a client and server if applicable.

Example: encutilcmd certv command

```
C:\>encutilcmd certv
INFO: Current process user is a member of local administrators group.
INFO: Created and validated client side TLS context OK.
URI: x509cert://[TLS-SCHANNEL]/CN=mach-02,CN=encserver,O=enc
INFO: Created and validated server side TLS context OK.
URI: x509cert://[TLS-SCHANNEL]/CN=mach-02,CN=encserver,O=enc
```

Authorization Rules Configuration

The ENC Gateway Service Authorization Rules are configured from the DSM configuration policy editor. Unlike other policy sections, there is no direct access to the underlying authorization tables and configuration is provided by a custom view dialog. The dialog handles inter-table dependencies and provides precommit evaluation of the specified rules.

The configuration view is provided across five tabbed views within the configuration dialog. The tabs and their contents are as follows:

Realms

This view provides the ability to view or define an ENC realm and add some short notes relevant to the realm.

Name Mapping

This view provides the ability to review or define the mapping between authenticated objects and their realm membership. The key field is the authenticated identity as a URI. The URI to realm mapping can be through a fully specified URI which must match exactly or a URI specified as a regular expression to match multiple URIs.

Time Ranges

All of the authorization access control in ENC can be time-restricted. This tab view provides the ability to define a time-range for use by individual access control entries. Entries can either be 'normal weekdays', where the time-range applies to one or more days from Sunday to Saturday, or can be 'special dates', such as Independence Day, etc.

The hours for which the time range is valid are specified as a start and end period in 24 hour format, such as "00:00 - 00:00" for a full 24-hour period. The granularity of the time range is 30 minutes, so each entry should use 00 or 30 as the minute value.

Access Control

This tab provides access to the timed access control entries. Each entry allows you to specify named rules that allow or deny activity (rules designed to deny access have higher precedence than rules that allow). The TACE name is recorded in audit entries and also displayed by the utility command when simulating accesses to test rule-sets. Therefore, it is recommended that you use reasonably descriptive names for each rule where appropriate.

The access control entry can control a single event or be aggregated to control multiple events within a single rule. For each rule, we have a protected resource - the secured object - and an accessing object - the security principal.

IP Addresses

This tab provides the IP address white-list table. Each entry can either be a single IP address or an IP address range specified by a pattern matching expression. The infrastructure machines will only accept connections from machines with the specified addresses.

Events

The ENC infrastructure defines a series of events which equate to operations that require an authorization check. Most of these events can be set in a TACE to control which security principals are allowed to do what to whom and when. In most cases, if the authorization component refuses the access request, the physical connection will be terminated. The name lookup and agent connect events are exceptions to this rule.

We now briefly describe each of the events in turn. For each event, the "secured object" entry defines the protected resource and the "security principal" entry defines the requesting resource.

Network Connection

Secured object: The ENC node receiving the connection.

This is the only event that is not controlled within a TACE rule; therefore the target of the operation is implicit. All access to the infrastructure is controlled by the IP address white-list. Only nodes or IP ranges listed in the IP address white-list are allowed to connect to the ENC infrastructure nodes. The secured object in this instance is always the target ENC node. The white-list currently applies to all ENC infrastructure nodes.

Authenticated Connection

Secured object: The ENC node accepting the connection.

Security principal: The authenticated identity of the connected ENC node.

All nodes must authenticate once they have established a network connection to a partner ENC node. This event is generated once a successful authentication sequence has been completed. The accepting ENC node calls the authorization API with the authenticated URI of the connecting node to see if the operation is allowed.

The access control entry for this event can specify the target as either the literal computer identity (from authentication), a pattern matching expression to address a sub-group of computers, or a realm name.

Server Registration

Secured object: The ENC Gateway Manager node.

Security principal: The authenticated identity of the ENC Gateway Server node.

When an ENC Gateway Server successfully establishes an authenticated connection to its manager, it sends a registration message asking to register as a server. The ENC Gateway Manager will then call the authorization component to see if the server is allowed to register with this manager. This is to stop unauthorized ENC Gateway Servers being placed into the ENC virtual network.

The access control entry for this event can specify the target as either the literal computer identity (from authentication), a pattern matching expression to address a sub-group of computers, or a realm name.

Router Registration

Secured object: The ENC Gateway Server handling the request.

Security principal: The authenticated identity of the ENC Gateway Router node.

When a router successfully establishes an authenticated connection to its server, it too sends a registration message asking to register as a router. The ENC Gateway Server will perform a local authorization check to see if this operation is allowed, and then passes the request on to the ENC Gateway Manager for further authorization.

The access control entry for this event can specify the target as either the literal computer identity (from authentication), a pattern matching expression to address a sub-group of computers, or a realm name.

Manager Router Registration

Secured object: The ENC Gateway Manager node.

Security principal: The authenticated identity of the ENC Gateway Router node.

This event is generated when a server forwards on a router registration message. The ENC Gateway Manager calls the authorization component to see if the router is allowed to join the ENC virtual network.

The access control entry for this event can specify the target as either the literal computer identity (from authentication), a pattern matching expression to address a sub-group of computers, or a realm name.

Server Client Registration

Secured object: The ENC Gateway Server handling the request.

Security principal: The authenticated identity of the ENC Client node.

This event is generated when an ENC Client node registers to an ENC Gateway Server node. The server performs a local authorization check, and then passes the registration request up to the ENC Gateway Manager for an authoritative answer.

The access control entry for this event can specify the target as either the literal computer identity (from authentication), a pattern matching expression to address a sub-group of computers, or a realm name.

Manager Client Registration

Secured object: The ENC Gateway Manager node.

Security principal: The authenticated identity of the ENC Client node.

This event is generated when an ENC Gateway Server node forwards on an ENC Client registration message to the ENC Gateway Manager.

The access control entry for this event can specify the target as either the literal computer identity (from authentication), a pattern matching expression to address a sub-group of computers, or a realm name.

Host Listen

This event is not currently implemented. The event is an agent local authorization check to see if the ENC agent is allowed to create a listening connection.

Host Connect

This event is not currently implemented. The event is an agent local authorization check to see if the ENC agent is allowed to create an outgoing connection.

Agent Connect

Secured object: The security identity of the target ENC node.

Security principal: The authenticated identity of the requesting ENC Client node.

This event is generated at the ENC Gateway Manager node whenever an ENC agent wishes to connect to another ENC agent node.

The access control entry for this event can specify the target as either the literal computer identity (from authentication), a pattern matching expression to address a sub-group of computers, or a realm name.

Agent Connect to Router

Secured object: The security identity of the ENC Gateway router node.

Security principal: The authenticated identity of the requesting ENC Client node.

This event is generated at the ENC Gateway Router node when an ENC agent connects to the router to establish a virtual connection to another ENC agent node.

The access control entry for this event can specify the target as either the literal computer identity (from authentication), a pattern matching expression to address a sub-group of computers, or a realm name.

Name Lookup

Secured object: The security identity of the target ENC node.

Security principal: The authenticated identity of the requesting ENC Client node.

This event is generated at the ENC Gateway Manager node when an ENC node wishes to perform a name lookup operation to convert from a symbolic host name to an ENC private address.

The ENC Gateway Manager initially extracts the target DNS name from the name lookup request, and converts this into one or more client records (thus allowing duplicate host-names across realms, but not within). These client records are passed though to the authorization component to decide if the name lookup request should be allowed (or not). A client record consists of the known DNS name and the authenticated identity of the object.

The access control entry for this event can specify the target as the literal computer identity (from authentication); a realm name; or a pattern matching expression to address a sub-group of computers or even multiple-realms.

Management Access

Secured object: The security identity of the target ENC node.

Security principal: The authenticated identity of the requesting ENC Client node.

This event is generated when an ENC client connection requests management information from the target ENC gateway.

The management information can include data about all ENC virtual connections hosted by an ENC server, so only approved nodes must be given access.

Connection Sequence

This section covers the common functionality that all ENC nodes have to perform in order to participate in the ENC virtual infrastructure. The common functionality is split into three distinct phases: physical connection, authentication, and finally, authorization.

Physical Connection

All nodes are required to be listed in the IP Address white-list table to be allowed to connect to the target ENC node in the first instance. On each connection established to an ENC node, the authorization component is called to check if access should be allowed or denied. If denied, the connection will be terminated immediately.

Authentication

Once a network transport connection has been established, both peers in the conversation will utilize the TLS protocol to authenticate to each other, validate that the authenticated identity is trusted via a trusted third-party certification authority, and that the identity is currently valid.

Authorization

Subsequent to the authentication phase, the authenticated identity is passed through to the authorization component for the 'Authenticated Connection' event check. The secured object for this event is the target ENC node. An access rule to allow (or deny) this operation can be specified with the individual computer as the secured object, a group of computer names as specified via a pattern matching expression, or via realm membership.

Any failures in the above sequence will be audited by the security auditing subsystem, if the appropriate category or messages are enabled. The auditing component can also be configured to record all successful operations as well.

Each ENC node, whether it is a server, router, or client agent, all perform registration to the nodes they are connecting to. A separate event is defined for each registration type as only ENC Gateway Server nodes should be allowed to perform a Server registration operation; only ENC Gateway Routers should be allowed to perform a Router registration, and so on.

Dependent on your infrastructure, you can create individual access control entries for each event and/or each secured object or you can group together events and computers within a realm for more coarse-grained access control.

ENC Virtual Connections

Now all physical ENC infrastructure nodes are operating normally, we consider the operating behavior of the ENC virtual network. In the default state, no connections or name lookups are allowed through the network unless there are explicit access control entries to allow this. Even computers that are joined together within a realm mapping have no automatic right to see or connect to each other.

When an ENC agent node wishes to communicate with another ENC agent node, the first operation to happen is usually a name lookup event. In most cases, there will only be one registered machine with this given name and it will usually be within the same realm as the requesting machine so would be covered by a blanket access control rule that allows all ENC nodes within a given realm to contact and lookup other members of its realm. In rarer circumstances, there may be two or more machines with the same fully qualified name. In this event, we need to disambiguate the name lookup by ensuring that we can only dereference computers within the realm(s) that the requesting object is also a member of. This is designed to ensure that data leakage across realms cannot happen unless explicitly allowed by an access rule.

If the authorization component allows the name lookup request, the IP address of the virtual ENC host is returned to the ENC Client agent. The ENC Client will then issue an Agent Connect request to the ENC Gateway Server/Manager. Again, the ENC Gateway Manager will look up the secured identity associated with the address of this request, and call the authorization system for permission for the operation to occur.

If permission is granted for the connection, both agents - the peers of the virtual communications circuit - will connect to ENC Gateway Routers to finalize the connection. Again, this connection is authenticated and authorization to access the router is required.

Example for Rule Setting

This example uses the command line utility file definition, from encUtilCmd, to describe the authorization rules, but it is analogous for the DSM Explorer; the rule sets are very similar.

It is possible to generate a simple set of rules, similar to those described below, using the encUtilCmd utility and its 'create' command. This also provides the ability to generate a test script at the same time to exercise the rules.

The following realms are used in this example:

[infrastructure]

This is the realm used for containing all of the infrastructure nodes (managers, servers, routers, and so on). The ENC infrastructure is managed by Forward, Inc. In this example, we bracket the realm name to make it stand out, but there is no requirement to do so; all realms names are equal. All of the infrastructure computers have certificate names with a common Relative Distinguished Name (RDN) of DC=forwardinc,DC=com.

[dsm]

This is an example realm holding all of the computers that make up the DSM infrastructure. We make a contextual distinction between the ENC infrastructure and the DSM infrastructure to make delineation between realms cleaner. All of the DSM computers have certificates names with the RDN of DC=forward-dsm,DC=com.

east

This is an example realm holding all of the computers from the 'east' company. All of the east computers have certificates with the RDN of DC=east,DC=com.

west

This is another example realm holding all of the computers from the 'west' company. All of the west computers have certificates with the RDN of DC=west,DC=com.

In this example, the ENC nodes, whilst they are DSM agent nodes as a minimum as well, are treated as stand-alone devices, which are separate from the DSM nodes. In the DSM ENC environment, the usual requirement is that DSM realm nodes can see and connect to all nodes within individual realms, and that realm agents can connect to nodes in the DSM realm, but members of a managed realm cannot see, or connect to, members of another managed realm.

You must now start defining authorization rules to allow the infrastructure to communicate and also for the realm computers to connect and utilize the virtual network. In the first instance, you must declare the realms to allow them to be used and cross-referenced.

The following is an extract for the authorization rules file: the realm section. It defines the four realms named above.

```
realm
{Name "[infrastructure]" Notes "ENC infrastructure realm"}
{Name "[dsm]" Notes "The DSM infrastructure realm"}
{Name "east" Notes "East Inc. Contact is admin@east.com"}
{Name "west" Notes "West Inc. Contact is admin@west.com"}
end
```

The next step is to define the mapping between certificate URIs and the realms themselves. This example uses pattern matching for all entries.

```
URIMapping
{URI ".*,DC=forwardinc,DC=com" Enabled "1" Type "Pattern" Realm "[infrastructure]"}
{URI ".*,DC=forward-dsm,DC=com" Enabled "1" Type "Pattern" Realm "[dsm]"}
{URI ".*,DC=east,DC=com" Enabled "1" Type "Pattern" Realm "east"}
{URI ".*,DC=west,DC=com" Enabled "1" Type "Pattern" Realm "west"}
end
```

You will deal with the IP address white-list next. In this example, you are allowing two public IPv4 subnets to access the ENC infrastructure.

```
IPAddWhiteList
{IPAddress "130\.119\..+" enabled "1" Type "Pattern"}
{IPAddress "141\.202\..+" enabled "1" Type "Pattern"}
{IPAddress "131\.119\..+" enabled "1" Type "Pattern"}
end
```

The last item to create before you progress to the individual access control entries is an active time-range. For the purposes of this example, the time range is active for all weekdays and covers all twenty-four hours of a day.

```
TimeRange
{Name "all-days" enabled "1" Hours "00:00 - 00:00" Type "normal" Weekdays "sunday -
saturday"}
end
```

Now you have all the basic elements you need to proceed with the access rules; you can concentrate on the access control entries themselves. In this example, you will mainly use individual access control entries for clarity. In real-world situations, it can be simpler and more efficient to combine several rules into a single rule.

Following is a single access control entry for example purposes only. For all the rules we now discuss, they should be defined as follows - between the TimeACL and end tags - or created in the configuration UI.

This rule, named AC-[infrastructure]-[infrastructure], defines an entry that allows all members of the infrastructure realm to access and authenticate to other members of the infrastructure realm. It references the 'all-days' time range you previously defined so will be active all day, every day.

```
TimeACL
{Name "AC-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow" TimeRange
"all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType "realm"
SecObj "[infrastructure]" Events "AuthenticatedConnection"}
...
end
```

You must add similar rules for the other realms; in this case, '[dsm]', 'east' and 'west'. The rules will be identical to those above but with the security principal changed to that of these other realms, as below.

```
{Name "AC-[dsm]-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "[infrastructure]"
Events "AuthenticatedConnection"}
{Name "AC-east-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[infrastructure]"
Events "AuthenticatedConnection"}
{Name "AC-west-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[infrastructure]"
Events "AuthenticatedConnection"}
```

You now define some more infrastructure entries. These entries have comments with them to show their purpose. As mentioned before, these could have all been rationalized into a single entry with the Events field set to “ManagerRegisterServer ServerRegisterRouter ManagerRegisterRouter ManagerRegisterAgent”. A benefit of keeping the rules separate is that the verification tools and auditing logging within the ENC subsystems will use the unique rule name when recording why an operation was allowed or disallowed.

```
; This entry allows all infrastructure nodes to be able to register a server to the
manager.
{Name "MRS-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow" TimeRange
"all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType "realm"
SecObj "[infrastructure]" Events "ManagerRegisterServer"}
;
; This entry allows all infrastructure nodes to be able to register a router to the
server.
{Name "SRR-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow" TimeRange
"all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType "realm"
SecObj "[infrastructure]" Events "ServerRegisterRouter"}
;
; This entry allows all infrastructure nodes to be able to register a router to the
manager.
{Name "MRR-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow" TimeRange
"all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType "realm"
SecObj "[infrastructure]" Events "ManagerRegisterRouter"}
;
; This entry allows all infrastructure nodes to be able to register a client to the
manager.
{Name "MRA-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow" TimeRange
"all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType "realm"
SecObj "[infrastructure]" Events "ManagerRegisterAgent"}
```

Now you must declare the ability to register with the infrastructure nodes for the DSM and managed realms. The following entries provide this configuration.

```
{Name "SRA-[dsm]-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "[infrastructure]"
Events "ServerRegisterAgent"}
```

```
{Name "SRA-east-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[infrastructure]"
Events "ServerRegisterAgent"}
```

```
{Name "SRA-west-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[infrastructure]"
Events "ServerRegisterAgent"}
```

The ENC Gateway routers also require authorization configuration for all nodes that will be connected to, and routed through, them. The following entries define this.

```
; These entries allow all DSM nodes to be able to connect to routers in the
infrastructure realm.
{Name "RAC-[dsm]-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "[infrastructure]"
Events "RouterAgentConnect"}

; These entries allow all agent nodes from the named realm(s) to be able to connect
to routers in the infrastructure realm.
{Name "RAC-east-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[infrastructure]"
Events "RouterAgentConnect"}
{Name "RAC-west-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[infrastructure]"
Events "RouterAgentConnect"}
```

You have now enough configuration data to allow all ENC nodes from the DSM and managed realms to be able to connect, authenticate and register with all of the nodes in the ENC infrastructure. The next step is to allow name lookup and agent connection functionality. The following entries do this.

There are mirror rules for all nodes: the managed realms are allowed to lookup the names of all DSM ENC-connected computers. And the DSM ENC-connected computers are allowed to look up all members of the managed realms. Rules and the mirror rules must be explicitly specified as shown below.

Note that there are no rules to allow 'east' to see 'west'; and conversely, there are no rules to allow 'west' to see 'east' , so look ups across the realms will not be possible. This namespace separation is vital to the secure operation of the virtual network.

```
; These entries allow all agent nodes from the named realm(s) to be able to perform
lookups of ENC members in the DSM realm.
{Name "NL-east-[dsm]" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType
"realm" SecPrinc "east" SecObjType "realm" SecObj "[dsm]" Events "ManagerNameLookup"}
{Name "NL-west-[dsm]" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType
"realm" SecPrinc "west" SecObjType "realm" SecObj "[dsm]" Events "ManagerNameLookup"}

; These entries allow all DSM nodes to be able to perform lookups of ENC members in
the named realms.
{Name "NL-[dsm]-east" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType
"realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "east" Events "ManagerNameLookup"}
{Name "NL-[dsm]-west" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType
"realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "west" Events "ManagerNameLookup"}
```

The following entries allow the agents to connect to/from the DSM and managed realms. Again, these entries could have been combined with the previous rule set, but the separation allows for more detailed logging and troubleshooting of rules.

```
; These entries allow all agent nodes from the named realm(s) to be able to connect
to ENC members in the DSM realm.
{Name "ACN-east-[dsm]" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType
"realm" SecPrinc "east" SecObjType "realm" SecObj "[dsm]" Events "AgentConnect"}
{Name "ACN-west-[dsm]" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType
"realm" SecPrinc "west" SecObjType "realm" SecObj "[dsm]" Events "AgentConnect"}

; These entries allow all DSM nodes to be able to connect to ENC members in the named
realms.
{Name "ACN-[dsm]-east" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType
"realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "east" Events "AgentConnect"}
{Name "ACN-[dsm]-west" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType
"realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "west" Events "AgentConnect"}
```

That concludes the example rule set.

How do I? and Other Questions

This section tries to anticipate likely questions and to provide a concise answer.

I am using the special all-realms membership (*), but time ranges are not being honored; why?

The * match marks the computer object as a member of all realms and also implies that it is a "super-user". An object with super-user access can perform all operations so the authorization subsystem always allows the specified operation regardless of time restrictions or access restrictions, a super-user realm can do anything - connect anywhere, lookup anything, and so on. Note that use of the super-user type is audited with a warning in the system application log.

Is there a way I can check rules before I apply them?

Yes, use the ENC utility command encUtilCmd and the 'verify' command. This allows you to simulate all of the events listed previously. Please refer to the encUtilCmd reference guide for detailed instructions on how to use the application.

I have to create a lot of rules! Is there a simpler way?

Again, yes, use the ENC utility command encUtilCmd. The 'create' command allows you to create a rule set for multiple realms and will define a basic set of rules that reflects the approach in this document section. You can also create a test script at the same time, which will verify all of the created rules using simulated identities. You can then modify the generated rules to use the real security identities, and tailor other areas to your specific requirements.

Auditing Events

The ENC Gateway internally audits events on the inter-node connections and generates audit information in the operating system event log. It can also optionally be sent to the Event Management system or a plain file. Audit events are grouped into categories covering errors, connections, security, and so on. Events can be enabled or disabled individually or by categories.

By default, all audit categories are disabled except for the error category, although all messages are enabled within their categories. This is to avoid the event log from being swamped with ENC events. The administrator should enable events when required when troubleshooting or monitoring the operation of the system.

Audit events can be enabled by enabling the corresponding category or they can all be enabled by setting a single parameter.

Note also that by default, all audit configuration data is locally managed but can be easily switched to centrally managed using the policy editor in the DSM Explorer.

For a complete list of event categories, see the "ENC Gateway and Client Auditing Policy Group" topic in the Configuration Policy section of the *DSM Explorer Help*.

Installation and Configuration of ENC Gateway Components

The installation of the ENC Gateway functionality is supported through the installer of CA IT Client Manager; currently for Windows operating environments only.

The configuration of the ENC Gateway components is done through parameters in the configuration store (comstore) and pushed out as a managed configuration policy.

ENC Gateway capability is disabled by default, as it is assumed that the majority of CA IT Client Manager installations are within company networks and do not need to traverse the Internet or internal firewalls.

Note: If you intend to run a web server such as IIS or Apache on the same computer as an ENC Gateway Server, they must be configured so that they do not try to open the same ports. By default, ENC listens on port 80 and 443. IIS and Apache also listen on port 80. Finally, IISadmin listens on 443. If a port conflict occurs and ENC is unable to listen, it will raise a corresponding event in the system event log.

ENC and SSA Configuration

The configuration of ENC components is done through common configuration parameters and pushed out through managed configuration policy. If the configuration policy for ENC or SSA is changed, this may cause SSA PMUX and CAM to be restarted. For more information about the ENC configuration policies, see ENC Gateway Policy Group in the Configuration Policy section of the *DSM Explorer Help*.

How to Enable the ENC Client

By default, the DSM installer copies the files for the ENC Client to disk but does not make them active. If you decide to activate the client at a later date, there are a number of steps to perform which are conveniently handled by the encUtilCmd utility program.

To enable the client, execute the following commands:

```
//if required by the network environment
encutilcmd client -proxy_http [proxy_socks] -proxy_host full_proxy_server_name
-proxy_port proxy_port_number
        -user username -password password

encUtilCmd client -state enabled -server Name_of_Gateway_Server [-port n]
caf start
```

Note: Enabling the client will have the side effect that both CA Message Queuing (CAM) and the Secure Socket Adapter Port Multiplexer (SSA PMUX) will be restarted. This is because ENC integrates with both of these components and a restart is required to make them "ENC aware."

Deployment in an ENC Environment

To successfully deploy software in an ENC environment, that is, with a firewall in the middle, the following preconditions must be met:

- The Infrastructure Deployment component of CA ITCM requires that both the DMPrimer and the dmkeydat.cer file (deployment certificate) must be present on the target computer.

  For details on how to achieve this, see the Manual Installation of the Infrastructure Deployment Primer Software (see page 237) and Provide the Deployment Management Security Key to a Primer Installation (see page 238) sections.

- The ENC Client component must be running and operational on the target computer. The ENC Client component is installed with the basic hardware inventory component and is made operational by setting its configuration.
- The Infrastructure Deployment policy options, Use host names and Do not ping target during scan, must be set to True.
- The Infrastructure Deployment policy option Always deploy primer must be set to False. The reason for this is that in an ENC environment the target is likely to have a firewall, so the primer cannot be deployed by the usual methods and an alternative must be used.

ENC Deployment Scenarios

The scenarios described in this section are expected to be the most common in which the ENC Gateway functionality is employed. They are based on the pilot scheme, the branch office, and the IT outsourcer.

In the outsourcer scenarios, companies of various sizes have outsourced the management of their desktops and servers to a specialist IT management company. CA IT Client Manager is being employed to do the usual technical management tasks, but needs the ENC Gateway functionality to work across firewalls and the Internet. An outsourcing company may, of course, be handling all scenarios at once, and multiple times.

Other scenarios are possible, of course.

In each scenario, the steps required to install and configure the system are described and the results expected.

The ENC deployment scenarios considered in the following sections include:

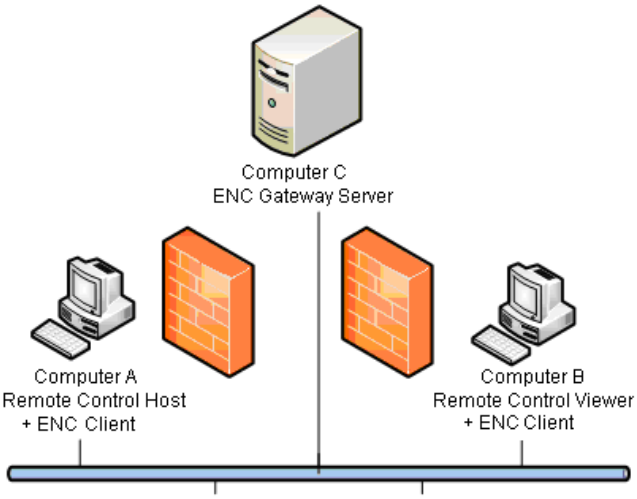
- Scenario 1: The Pilot Scheme (see page 452)
- Scenario 2: The Branch Office (see page 456)
- Scenario 3: Small Outsource Client Company (see page 459)
- Scenario 4: Medium Outsource Client Company (see page 460)
- Scenario 5: Large Outsource Client Company (see page 461)

ENC Deployment Scenario - The Pilot Scheme

This scenario is expected to be the first that an organization deploys and is intended to give experience on how the system works. It also serves as a simple example to help understanding the ENC Gateway.

This scenario is based simply on three computers, two are agent computers behind Windows personal firewalls and the third is an ENC Gateway Server that provides connectivity.

The following illustration shows the layout of the pilot scheme scenario:



In this scenario, computer A is running a Remote Control Host, computer B is running a Remote Control Viewer, and computer C is running an ENC Gateway Server. Computer B cannot connect to computer A because it is behind a firewall. All computers are running ENC Clients which are connected to the ENC Gateway Server on computer C. It is computer C that provides connectivity from computer B to A. The setup is unmanaged by a domain manager because we want the scenario to be as simple as possible.

To set up a small ENC Gateway network, follow these steps:

On Computer A:

1. Enable the Windows firewall.
2. Start a custom install of CA ITCM. Select "Remote Control" and "Agent."
3. When the installer asks for the address of the scalability server, accept the preset default value. When the installer asks you if that is OK (since there is no server), click Yes. This allows an unmanaged installation to work.
4. Click the ENC Client button to start configuring the client. Enter the address of computer C for the client's server address.
5. Click the Remote Control button and select only "Install host functionality."
6. When installation completes, do not start CA ITCM but instead execute the following commands:

   ```
   ccnfcmda -cmd setparametervalue -ps itrm/rc/host/managed -pn centralizedsecurity -v 0
   ```

   ```
   ccnfcmda -cmd setparametervalue -ps itrm/rc/host/managed -pn standalone -v 1
   ```

7. Start CA ITCM using the "caf start" command.

On Computer B:

1. Enable the Windows firewall.
2. Start a custom installation. Select "Remote Control" and "Viewer".
3. No scalability server specification (proceed as on computer A).
4. Configure an ENC Client in the same way as on computer A.
5. Click the Remote Control button and select only "Install Viewer functionality."
6. When installation completes, do not start CA ITCM but instead execute the following command:

   ```
   ccnfcmda -cmd setparametervalue -ps itrm/rc/viewer/managed -pn managedmode -v 0
   ```

7. Start CA ITCM using the "caf start" command.

On Computer C:

1. Verify that the windows firewall is disabled.
2. Start a custom installation. Clear all products. On the custom installation dialog, clear everything except "ENC Gateway" and "Agent."
3. No scalability server specification (proceed as on computers A and C).
4. On the dialog for configuring the ENC Gateway, select all three roles: Manager, Server and Router.
5. Do not start up CA ITCM on this computer right now. The security for the Gateway server is not configured yet and will reject all connections from clients. To configure ENC security, we can create a text file containing a rule that allows anyone to connect. The file is then imported into the common store for the server to pick up.

   Important! Note that this is just an example. In a real production environment, you would never use rules that allow open access!

6. Create a text file called defrules.txt, containing the following text:

```
[authz]
RulesVersion=5

REALM
{Name "ENC" Notes "The default realm to which everyone belongs"}
end

TimeRange
{Name "all-days" enabled "1" Hours "00:00 - 00:00" Type "normal" Weekdays "sunday
- saturday"}
end

TimeACL
{Name "policy1" enabled "1" RuleType "allow" Events "AuthenticatedConnection
ManagerRegisterServer ServerRegisterRouter ManagerRegisterRouter
ServerRegisterAgent ManagerRegisterAgent ManagerNameLookup AgentConnect
RouterAgentConnect ManagementAccess" TimeRange "all-days" SecPrincType "realm"
SecPrinc "ENC" SecObj "ENC" SecObjType "realm"}
end

URIMapping
{URI ".+" enabled "1" Type "pattern" Realm "ENC"}
end

IPAddWhiteList
{IPAddress ".+" enabled "1" Type "pattern"}
end
```

7. Import this rule file using the encUtilCmd command, as follows:

```
encUtilCmd import -i defrules.txt -fl
```

   The ENC Gateway Server now has a rule that allows all connections.

8. Finally, install ENC certificates on all computers. For more information, see Setting Up Certificate Services for Use by ENC Gateway (see page 466).

To test the scenario, perform the following steps:

1. On computers A and B start up CA ITCM using the command "caf start". Do not start up computer C yet because we want to test without ENC Gateway functionality.
2. Start up the host configuration dialog by selecting it from the system tray on computer A. Select the Users tab and verify that the local administrator is a user of Remote Control on that computer.
3. On computer B, start up the viewer and try to connect. This should be blocked by the firewall on computer A.
4. Start up CA ITCM on computer C. After a few minutes, check that the ENC Clients have registered with the ENC Gateway Server using the "encclient status" command. This should report that the client has registered successfully and is ready.

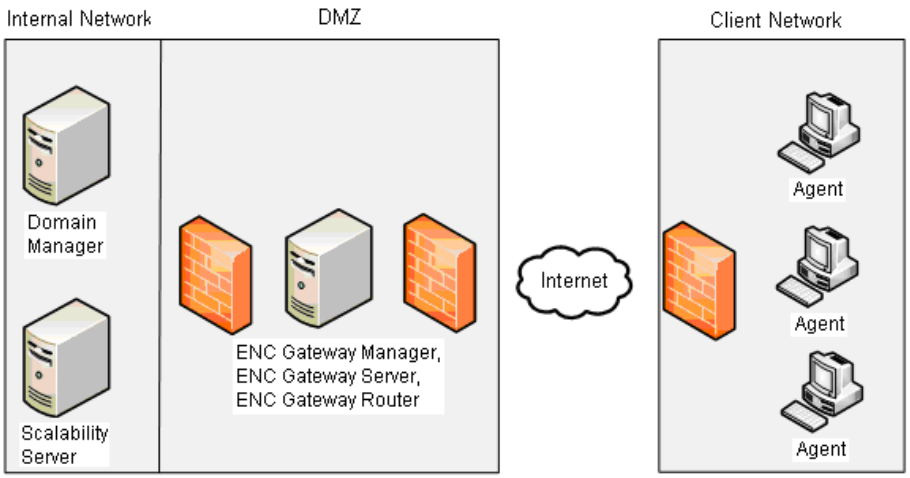
5. Repeat the connection attempt; it should now work. All data is being routed via computer C. The "encclient status" command should report that a connection is in progress via computer C.
6. You can adjust the rules by modifying the defrules.txt file and reimporting, but using the encUtilCmd command with the -o option to override the existing rules. This allows experimentation with different authorization rules so you can get a feel for the system.

   (For the detailed description of the encUtilCmd utility program and all its options, see the *EncUtilCmd Command Reference*, which you can find in the *CA Bookshelf* under the Reference Guides category.)

ENC Deployment Scenario - The Branch Office

In this scenario, the parent company maintains the domain manager and scalability server on the main office network (internal network). The branch office has a LAN with DSM agents installed on their computers (client network). Both offices are protected by firewalls and connected to the Internet.

The following illustration shows the network layout in a sample branch office deployment scenario:



In this scenario, it is assumed that all computers in the network, including the ENC Gateway Server computers, have at least a DSM agent installed.

The DMZ (demilitarized zone) allows connectivity from the internal network into the DMZ but no further. Computers in the DMZ can connect out to the Internet but not to the internal network.

The required deployment and configuration steps in this scenario are as follows:

- Deploy the ENC infrastructure in the main office (internal network)
- Deploy DSM agents to the branch office (client network)
- Configure the agents in the branch office to report to the main office scalability server

In the main office network the following activities apply:

- Create a DMZ in the main office network, if not already present. This is required because the ENC Gateway Servers have to be visible to the branch office, which is assumed to connect in over the public Internet.
- Install a DSM domain manager, scalability server, agents and ENC Clients as required in the parent network
- Install a DSM agent, an ENC Client, Manager, Server, and Router on a computer in the main office network DMZ. Configure the agent to register with the scalability server in the internal network.
- Install ENC certificates on all ENC Gateway-aware computers, as described in the Certificate Management (see page 466) section. This covers computers in the internal network and the DMZ. These are required for ENC Gateway authentication.
- Install ENC certificates on the DMZ computers.
- Do not start up the ENC Gateway Servers just yet. At this point, the ENC Gateway Server is configured with no authorization rules and so will reject all connections. This means, that the DSM infrastructure in the DMZ cannot contact the domain manager in the main office network and thus cannot receive configuration policy containing the authorization rules.
- Open the DSM Explorer and configure the security policy you require for ENC. Configure the ENC Gateway with a security policy. This must cover access for computers in the main office network as well as those in the branch office. At the moment, however, this cannot be sent to the ENC Gateway Servers from the domain manager because there is a catch-22, that is, the computer cannot receive a policy until it registers with the domain manager, and it cannot register until it gets a policy which defines the authorization rules that allow it to connect to the domain manager.

- To fix this, the ENC Gateway Server has to be “bootstrapped” with rules sufficient to allow a connection to the domain manager. Once established, the domain manager can send the real policy to override the bootstrap policy.

  First, the real policy must be entered into the configuration policy on the domain manager. This can be done using one of two methods:

  1. One method is to open the DSM Explorer and configure the security policy you require for ENC using the configuration policy editor. The GUI provides a custom dialog to help compose the rules.
  2. The alternative method is to compose a text file with your default rules and import them in bulk using the encUtilCmd utility. (For the detailed description of the encUtilCmd and all its options, see the *EncUtilCmd Command Reference* which you can find in the *CA Bookshelf* under the Reference Guides category.) Note that encUtilCmd also provides a means of verifying the rules before you make them “live”.

  At minimum, these rules should allow the DSM infrastructure in the main office network to contact and register with the ENC Gateway infrastructure in the DMZ.

  We suggest that you compose the rules using the second method, as the rules file you create can then be used on both the domain manager and the ENC server computers. The GUI can be used for future modifications to the policy.

  Apply the rules to the domain manager using the “encUtilCmd importdb” command. This adds the rules to the DSM configuration database. Once there, they can be delivered through the usual policy mechanism once the ENC server computers connect.

  Apply these rules to the ENC Gateway Server in the DMZ using the "encUtilCmd import" command. This will bootstrap the server with authorization rules and allow the computer to contact the domain manager and register.

  Start CA IT Client Manager on the ENC Gateway Servers so that they pick up the new rules and allow ENC connections to proceed

- By default, the configuration policy in the domain manager is set to locally managed to prevent accidental overwriting by a blank policy. Set this to centrally managed. When CA IT Client Manager registers successfully, the initial default rule will be overwritten by the policy sent down from the domain manager.
- Wait 10 minutes, and then check that the computers in the DMZ have now registered and are visible in the GUI.
- If no computers are visible, it may be that the default rules are incorrect or the new policy has cut off access. To diagnose this, examine the NT application event log on the ENC Gateway Servers.

In the branch office the following activities apply:

- Install the required DSM agents on each computer in the branch office network. The ENC Gateway functionality is installed by default but needs to be configured. Configure the clients to register with the ENC Gateway Server in the main office DMZ network. Since the ENC Gateway is not yet working between the main and branch office, DSM deployment cannot be used. Instead, the installation can be done using a number of methods that depend on how many computers are affected, for example:
  - Manual installation from DVD, if only a few computers are to be installed
  - Installation of a package on user logon from a NT domain logon script.
  - Installation of a temporary domain manager and scalability server within the branch office network. This can be done using a real or virtual machine that is sent to the branch. Use the deployment feature of CA IT Client Manager to send out the agent package. Once deployment is complete and all agents are registering with the domain manager in the main office, the temporary domain manager in the branch office is removed.
- Check that the computers in the branch office register, by checking the All Computers group in the GUI back in the main office.
- Perform the usual validation tests employed by your organization to ensure that CA IT Client Manager is fully functional.

ENC Deployment Scenario - Small Outsource Client Company

The small company scenario is very similar to the branch office except that more security is required. Since the outsourcer may be looking after many companies, more control needs to be imposed on the connectivity allowed between nodes in each company network. In addition, access from one outsource client to another must be secured. Normally, one client would not be allowed to see the computers in another. This is handled by the support for realms in ENC Gateway authorization.

The computers in the outsourcing company must be able to connect with the client's computers. This requires the outsourcer ENC Gateway Manager to be configured with authorization rules that allow the following:

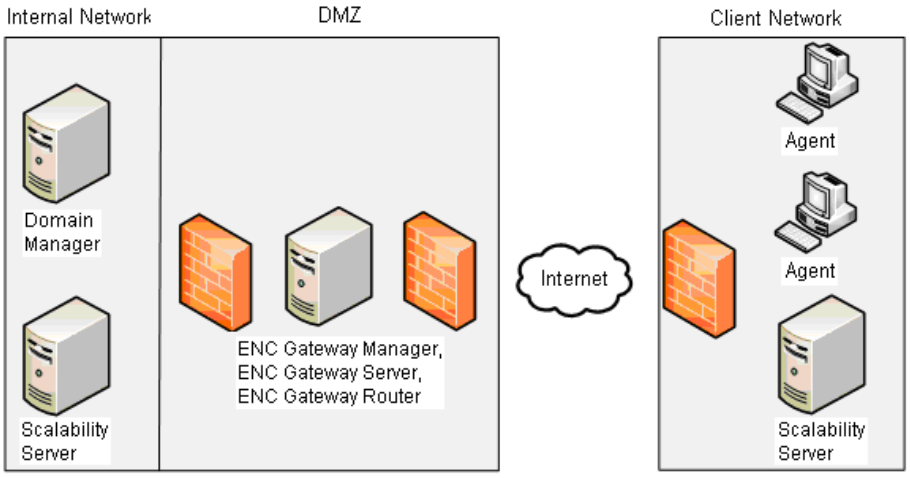
- Registration from computers in the client network.
- Connections from computers in the client network to computers in the outsourcer network, and conversely
- Connections between different client realms are denied.

Configuring and setting up CA ITCM is similar, but security area management must also be configured to handle the security requirements (see the "CA ITCM Security Features" (see page 375) chapter).

ENC Deployment Scenario - Medium Outsource Client Company

In this scenario, the client has enough computers to warrant their own scalability server.

The following illustration shows the network layout in a sample medium outsource client company deployment scenario:



The agents in the client network register with the scalability server there. The scalability server connects to the domain manager in the outsourcer network through an ENC Gateway connection. The deployment steps are very similar to the small company scenario except for the agent configuration. In this scenario, the DSM agents are configured to register with the "in-house" scalability server.

In this medium outsourcer scenario, ENC will typically not be on the end point computers. In this case this means that direct connections will not work unless ENC is configured and running on the end point computers. Direct connections are used for the following communications:

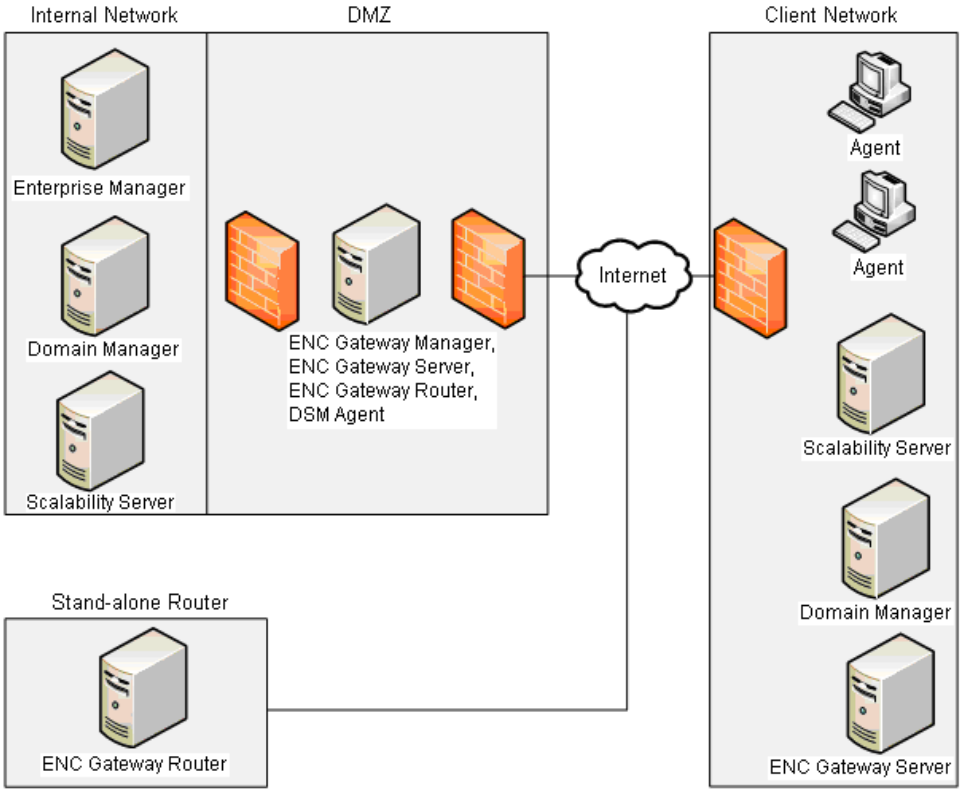
- Remote control host - view connection
- Instant diagnostics from DSM Explorer to agent
- Software catalog from agent to manager
- DTS notifications

ENC Deployment Scenario - Large Outsource Client Company

In this scenario, the company is large enough to have its own domain manager as well as a number of scalability servers and an ENC Gateway Server.

The outsourcing company maintains an enterprise manager that is to be linked to the client's domain manager.

The following illustration shows the network layout in a Large Outsource Client Company ENC Gateway deployment scenario:



Once the client domain manager is installed, it can be used to deploy DSM agents as usual within the client.

The policy can be configured locally using the client's domain manager to allow the client ENC Gateway Server to accept ENC connections from the client computers.

The enterprise manager will replicate its database to the domain manager by using the database provider itself. This cannot be done through an ENC Gateway connection. To make this work, the firewalls must be configured as described in the existing Microsoft or Oracle published best practice.

The computers in the outsourcing company must be able to connect with the client's computers. This requires the outsourcer ENC Gateway Manager to be configured with authorization rules that allow the following:

- Connections from the client's ENC Gateway Server
- Registration from computers in the client network
- Connections from computers in the client network to computers in the outsourcer network and conversely

Stand-alone ENC Gateway Routers

Additional ENC Gateway Routers may also be deployed for resiliency or scalability. These ENC Gateway Routers can be installed elsewhere on the Internet or at branch offices.

The deployment steps for stand-alone ENC Gateway Routers are as follows:

- Install a DSM agent and an ENC Gateway Router and configure it to register with the ENC Gateway Server in the outsourcer office. The router can, of course, be configured to register with any other suitable ENC Gateway Server.
- At the domain manager, add suitable authorization rules to the policy intended for the stand-alone router computer. The rules must allow the router in the realm that it resides in to connect and register.
- Install a suitable certificate on the router computer.
- Startup CA ITCM on the router computer. The router should then register with the ENC Gateway Server. Check the event log for this.

  Note: To see these events, you need to set the configuration parameter itrm/common/enc/audit/enabled to 1. In the configuration policy this will appear as "Enable All". This enables auditing of all ENC events. This lets you see more clearly the activity in the ENC system. By default, only those events in the "error" category are enabled. To restore auditing back to normal, set the configuration parameter to 2 ("Enable by Category").
- Once the ENC Client on the router computer registers, the CA ITCM infrastructure will be able to accept the policy and therefore install authorization rules for the router. Once the router has picked up the authorization rules, it will be able to act as a router for other computers in the ENC Gateway network to connect.

Stand-alone ENC Gateway Servers

Similar considerations as for stand-alone ENC Gateway Routers apply to stand-alone ENC Gateway Servers. The difference is that the authorization rules are those suitable for a server role, that is, they allow the operations that a Gateway Server can perform as opposed to those that a Gateway Router can perform.

Internet Proxy Support

If an ENC Client's path to an ENC Gateway Server is blocked by an internet proxy, then it must be configured to connect through that proxy. The ENC Gateway supports SOCKS4, SOCKS5, and HTTP proxies. Authentication can be configured by an explicit user name and password or impersonation of the logged on user. The client can also use current Internet Explorer settings to locate the proxy.

The properties to be set are located in the policy node 'common components/enc/client'.

To configure a SOCKS proxy, set the parameters as follows:

- SocksProxyAddress and SocksProxyPort to identify the proxy computer
- SocksProxyAuthType to define the type of authentication to be used (basic or secure)
- SocksProxyImpersonate, which allows the client to use the credentials of the logged on user. Of course, this means that the client cannot connect unless someone is logged on
- SocksProxyUsername and SocksProxyPassword, if you want to use explicit credentials to authenticate with the proxy
- SocksProxyDiscovery, if you want the ENC Client to automatically locate the proxy using IE settings. In this case, you would usually have SocksProxyImpersonate set

To configure a HTTP proxy, set the same parameters except that "HTTP" is substituted for "Socks" in the parameter names.

Note: Proxy configuration can also be set using the encUtilCmd utility. This is useful when the computer in question is cut off from managed policy by the firewall but obviously needs policy settings in order to connect.

Restrictions on Using CA ITCM Through ENC Gateway

There are a number of restrictions on the features in CA IT Client Manager (CA ITCM) when used through an ENC Gateway connection. These restrictions include:

- Wake-on-LAN (WOL) cannot work through the ENC Gateway because the ENC Gateway supports only TCP connections, whereas WOL uses UDP.
- Some features of Instant diagnostics do not work because they rely on non-ENC Gateway-aware components provided with the operating system, for example, FTP.
- Service location cannot work because it uses UDP.
- Reporter cannot work as it accesses the MDB directly.

- Software delivery (SD) jobs through the ENC Gateway may take up to 10 minutes to be triggered. This is because SD will try to use the IP address of the target when it registered, but this will fail because IP addresses are not valid over different networks. The SD scalability server will retry the job every 10 minutes, alternating between the FQN and IP of the target. The FQN will work with the ENC Gateway because it uses the FQN of ENC Gateway-enabled computers to uniquely identify them.
- Some components within CA ITCM use SQL Server or Oracle client side components to make direct management database (MDB) connections. These connections are not ENC-enabled, hence, if these connections pass over firewalls, you should use the recommended Microsoft or Oracle method of traversing the firewall.

  The following list provides details of scenarios and DSM components where direct MDB access is made; additionally, the specific client side components used for SQL Server and Oracle are given:

  - **Domain manager to and from the enterprise manager**

    MDB replication between the domain manager and the enterprise manager uses direct connections and bulk copy.

    Client side components:

    For SQL Server: SQL Native Client and bcp Utility

    For Oracle: OCI API and SQL*Loader

  - **Engine to the domain manager and the enterprise manager**

    The engine makes direct database connections when communicating with the domain manager and the enterprise manager.

    Client side components:

    For SQL Server: SQL Native Client and bcp Utility

    For Oracle: OCI API and SQL*Loader

  - **Reporter to the domain manager or the enterprise manager**

    The reporter makes direct database connections to generate reports.

    Client side components:

    For SQL Server: SQL Native Client and bcp Utility

    For Oracle: OCI API and SQL*Loader

  - **Web Console to the domain manager or the enterprise manager**

    The Web Console component makes a JDBC connection to the database.

    Client side components:

    For SQL Server: JDBC

    For Oracle: JDBC

- **Contents Import/Export Utility**

  The Contents Import/Export Utility makes direct database connections when synchronizing DSM data with a remote Oracle or SQL Server MDB.

  Client side components:

  For SQL Server: SQL Native Client and bcp Utility

  For Oracle: OCI API and SQL*Loader

Using the encUtilCmd Utility

The encUtilCmd utility is a program designed to implement various ENC Gateway utility functions. However, this section deals only with one use case of encUtilCmd.

For the detailed description of the encUtilCmd command and all its options, see the *EncUtilCmd Command Reference* which you can find in the CA Bookshelf under the Reference Guides category.

The encUtilCmd utility in addition to other functionality will handle the problem of configuring ENC Gateway security.

This use case considers a problem that appears after the installation of a scalability server, which will be in the locked down state. The domain manager is unable to make a direct connection to the scalability server because there is a firewall in the way. So this method cannot be used to distribute the policy to the scalability server. The domain manager cannot use the ENC Gateway to contact the scalability server because the scalability server will reject all connection attempts. It is this policy that defines who can connect to the scalability server.

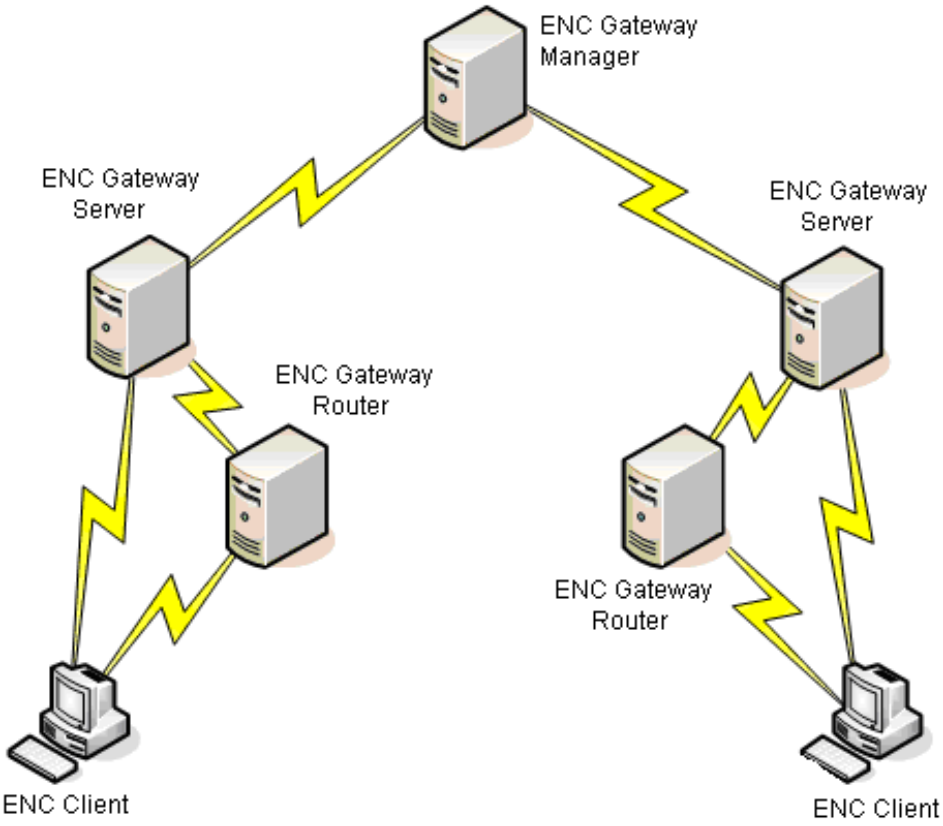
To solve this problem, you can define some rules in a text file and import this file on the ENC Gateway Server using the encUtilCmd command.

Certificate Management

In the Extended Network Connectivity (ENC) infrastructure, all inter node communications are secured using the standard transport layer security (TLS) protocol. This protocol provides confidentiality, integrity, and mutual authentication.

The authentication portion of the TLS protocol is provided by the use of digital certificates and public-private key cryptography. The confidentiality is provided by symmetric key cryptography.

The following illustration shows the inter node connections between the ENC components in an ENC infrastructure:



All of the inter node connections in the ENC infrastructure are protected by TLS authentication. Authentication is always mutual: the initiator of a connection authenticates to the responder, and the responder authenticates to the initiator. This allows the ENC infrastructure to validate computers connecting to it, and also the ENC Clients to feel secure to whom they are connecting.

X.509 Certificates

Extended Network Connectivity (ENC) uses X.509 version 3 digital certificates for authentication. The certificate profile in use is that of the IETF PKIX working group's RFC 3280 implementation.

The certificates and their associated private keys are obtained through the Microsoft Certificate Store. The certificates should have an Enhanced Key Usage extension that is marked for Server Authentication (1.3.6.1.5.5.7.3.1) or Client Authentication (1.3.6.1.5.5.7.3.2), dependent on the application using it.

A CA ITCM private extension to the Enhanced Key Usage certificate extension can be used to assist in certificate location (1.3.6.1.4.1.791.2.10.8.3). This object identifier (OID) is private to CA Technologies and is internal to the CA OID tree.

No ENC limits are imposed on the RSA key size used in the certificate key pair. The size of keys used is an organization-specific choice, though we recommend a minimum of 1024-bit keys.

Certificate Management Using a PKI Infrastructure

Certificate creation and distribution can be a difficult process. The use of a Public Key Infrastructure (PKI) to automate and augment this process is highly desirable.

Certificate Requirements

The ENC Gateway uses X.509 v3 certificates that are issued for use by the standard TLS 1.0 (SSL 3.1) security protocol. The ENC Gateway can use standard TLS certificates, but also supports an extended key usage extension to allow the ENC subsystem to identify certificates that are primarily for use by the ENC Gateway.

The ENC Gateway searches for the best certificate to load for its identity. On the first pass through, it looks for valid certificates (with associated private keys) that are marked with the CA ENC usage extension (see (1) in the following table) as well as the TLS usage extension for client authentication (2), or server authentication (3), respectively (4).

The following table provides some additional details about the terms marked with (1) to (4) in the above paragraph:

Marker	Information
(1)	CA Technologies has internally allocated an object identifier (OID) to be used in X.509 v3 certificates as an enhanced key usage identifier (see RFC2459 section 4.2.1.13). This OID indicates that the certificate is for use by the ENC security subsystem. ■ The object identifier is “1.3.6.1.4.1.791.2.10.8.3” ■ The object identifiers tag is “OID_PKIX_KP_CA_CMS_ENC_TLS_AUTH” ■ The usage extension can be marked as critical or noncritical. ■ The CA Technologies base OID is “1.3.6.1.4.1.791”, which is IANA registered.
(2)	The OID for TLS client authentication is “1.3.6.1.5.5.7.3.2”
(3)	The OID for TLS server authentication is “1.3.6.1.5.5.7.3.1”
(4)	For ENC Gateway nodes that act as both a client and a server (routers and Gateway servers), the security subsystem can use either a single certificate marked for client plus server authentication, or individual certificates marked as client authentication only and server authentication only, respectively.

If the ENC Gateway does not find appropriate certificates, it repeats the search without the requirement of the CA ENC usage extension.

When you create certificates for use by the ENC Gateway, we recommend that you add the CA extended key usage OID to the certificates; however, the ENC Gateway will operate without.

The CA Technologies-Private Authentication Object Identifier

A CA ITCM private extension to the Enhanced Key Usage certificate extension can be used to assist in certificate location (1.3.6.1.4.1.791.2.10.8.3).

This object identifier (OID) is private to CA Technologies and is internal to the CA Technologies OID tree.

Chapter 13: Integration with CA Service Desk Manager

The integration of CA IT Client Manager with CA Service Desk Manager makes CA IT Client Manager a Service Aware application, meaning that CA IT Client Manager can trigger on certain events of its Managed Assets and create tickets in CA Service Desk Manager.

Ticket creation and workflow in CA Service Desk Manager is controlled by the Service Aware policy, which enumerates a list of problem types. CA IT Client Manager uses problem types to categorize the problem and to address the ticket to be created.

CA IT Client Manager and CA Service Desk Manager provide graphical user interfaces that allow context-sensitive launches of each other for the integration.

This chapter describes setting up and configuring the system and security and authentication aspects. The configuration considerations apply for DSM domain and enterprise managers.

For details on CA Service Desk Manager, for example problem types, see the CA Service Desk Manager documentation set.

This section contains the following topics:

Service Aware Policy

Regarding the integration of CA ITCM with CA Service Desk Manager, the Service Aware policy with the name ManagedAssetEvents is defined. The Service Aware policy is automatically installed when CA Service Desk Manager is installed. CA ITCM uses the problem types available with this policy when tickets are created.

The main parameters of the Service Aware policy are as follows:

Display Name:

Managed Asset Events

Code:

MANAGED_ASSET_EVENTS

Description:

This Service Aware policy is used to process tickets being raised by Managed Assets through Web Services.

In addition to the default problem types of CA Service Desk Manager, the Service Aware policy includes the problem types listed in the following table. CA Service Desk Manager administrators can modify these problem types or extend this list with their own problem types.

Display Name of the Problem Type	Code of the Problem Type	Description of the Problem Type	Priority (5 is the highest)
Asset Event-based Policy high	ASSET_EVENT_ POLICY_H	A managed asset encountered an event-based policy violation of high priority	4
Asset Event-based Policy medium	ASSET_EVENT_ POLICY_M	A managed asset encountered an event -based policy violation of medium priority	3
Asset Query-based Policy high	ASSET_QUERY_ POLICY_H	A managed asset encountered a query-based policy violation of high priority	4
Asset Query-based Policy medium	ASSET_QUERY_ POLICY_M	A managed asset encountered a query -based policy violation of medium priority	3

Display Name of the Problem Type	Code of the Problem Type	Description of the Problem Type	Priority (5 is the highest)
Software Distribution Failure high	SW_DISTR_FAIL _H	A software delivery job encountered a failure of high priority	4
Software Distribution Failure medium	SW_DISTR_FAIL _M	A software delivery job encountered a failure of medium priority	3
Software Distribution Failure low	SW_DISTR_FAIL _L	A software delivery job encountered failure of low priority	2

Ticket Handling

Tickets can be created on domain and enterprise level. The following events may result in a ticket:

- A policy violation is encountered.
- A software delivery job fails.
- An administrator creates a ticket interactively through a pop-up menu in the context of a computer.

To avoid ticket flooding, the following rules restrict the creation of new tickets:

- Only one ticket is created for each policy. A ticket is newly created when the first policy violation is encountered. For any subsequent violation of the same policy, a log is appended to the ticket.
- Only one ticket is created for each software job. A ticket is newly created when the first failure of the software job is encountered. For any subsequent failure of the same software job, a log is appended to the ticket.

For more information on ticket handling see the CA Service Desk Manager documentation.

Associating Discovered Assets with Owned Assets

CA ITCM creates tickets in the context of discovered assets, for example, computers or users. When a ticket is created, a discovered asset is mapped to an owned asset, which is known in CA Service Desk Manager. This allows CA Service Desk Manager administrators to navigate and report on relationship between tickets and owned assets.

Context Launch Between CA ITCM and CA Service Desk Manager

The following table gives an overview of the supported context launches between the DSM Explorer or the DSM Web Console and the CA Service Desk Manager Web GUI.

From	To	In Context of	Context
Explorer / Web Console	CA Service Desk Manager Web GUI	Software job	Ticket being created on job failure
Explorer / Web Console	CA Service Desk Manager Web GUI	Asset policy	Ticket being created on policy violation
CA Service Desk Manager Web GUI	Explorer / Web Console	Ticket detail	Software job
CA Service Desk Manager Web GUI	Explorer / Web Console	Ticket detail	Asset policy

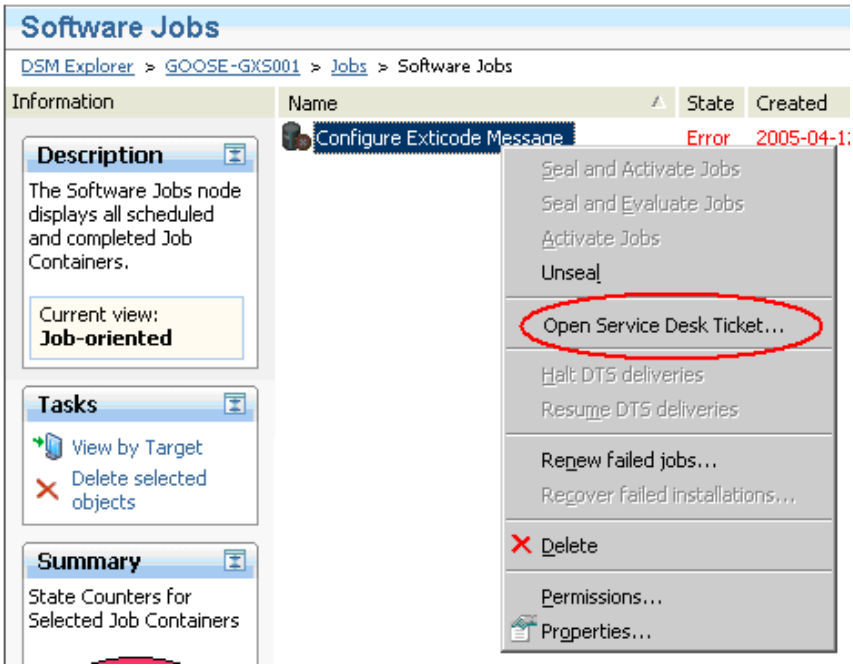
Context Launch from CA ITCM to CA Service Desk Manager

CA ITCM provides user interfaces that allow you to launch CA Service Desk Manager in the following context:

- a software job failure (see page 475)
- an asset policy violation (see page 476)

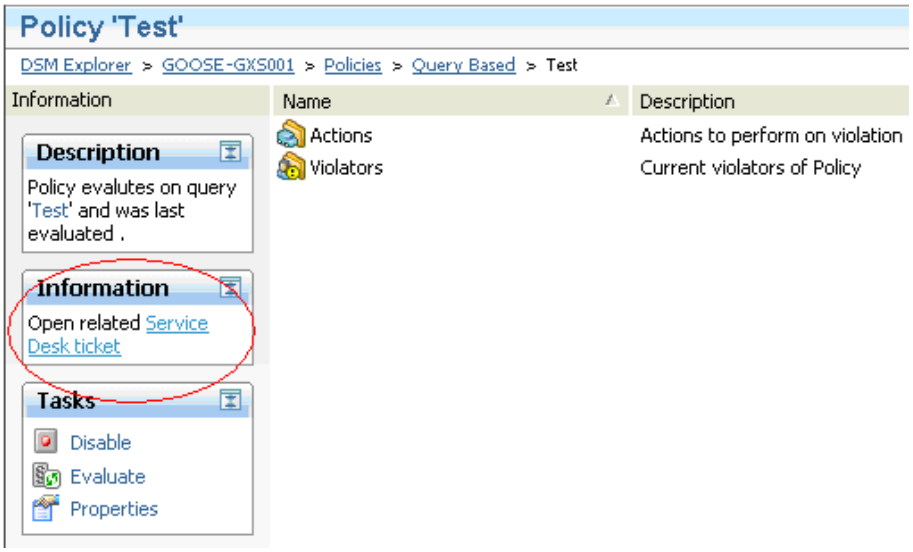
Ticket Details in Context of a Software Job Failure

Software jobs that have failed and raised a CA Service Desk Manager ticket provide a context menu entry Open Service Desk Ticket, which you will see when right-clicking the failed software job. Selecting Open Service Desk Ticket launches the CA Service Desk Manager Web GUI.



Ticket Details in Context of an Asset Policy Violation

When a policy is CA Service Desk Manager enabled, an additional hyperlink Open related Service Desk ticket appears in the Information column of the DSM Explorer. Selecting this hyperlink launches the CA Service Desk Manager ticket detail screen of the ticket, which was initially generated by a violation of this policy.



Ticket Creation in Context of a Managed Asset (ad hoc)

CA Service Desk Manager tickets are created interactively by clicking the Create Service Desk ticket action in the Quick Launch portlet:

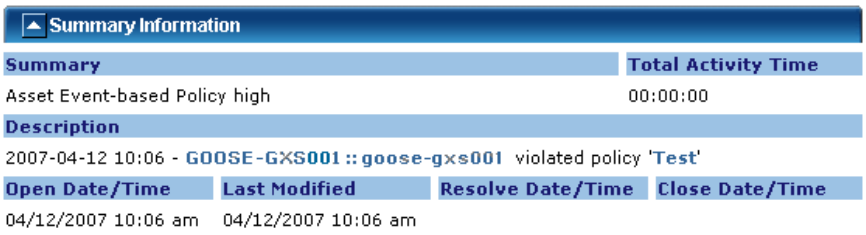
The Quick Launch portlet is located on the Homepage tab, which opens when you select the managed asset on the DSM Explorer.

The Create Ticket method is also available as a command in the asset context menu.

Context Launch from CA Service Desk Manager to CA ITCM

The DSM Explorer and the Web Console are launched from the CA Service Desk Manager Web GUI through individual URLs.

The hyperlink, which launches the DSM Explorer or DSM Web Console, appears in the Description field in the Summary Information of the CA Service Desk Manager ticket:



Note: As the DSM Explorer is started using the dsmgui.exe command, the Explorer needs to be installed on the CA Service Desk Manager machine that is running the CA Service Desk Manager Web GUI.

Setting Up CA Service Desk Manager and CA ITCM

The CA Service Desk Manager setup automatically installs the Service Aware policy for CA ITCM and the predefined problem types for ticket creation. The name of the Service Aware policy is ManagedAssetEvents. The predefined problem types can be modified or enhanced by the CA Service Desk Manager administrator at any time.

Further, CA Service Desk Manager creates a proxy account for CA ITCM, System_MA_User, which is configured with a defined set of privileges, and associates it with the Service Aware policy.

The CA ITCM setup automatically creates a configuration policy for the integration with CA Service Desk Manager. The configuration policy is installed on the Common Configuration (CCNF) manager under the following path name:

```
/Default Computer Policy/DSM/Service Desk Integration/default
```

To enable integration, the CA ITCM administrator needs to set up the configuration policy using the Common Configuration manager GUI.

The configuration policy parameters encompass the following areas:

- A switch indicating if CA Service Desk Manager integration is enabled
- Secure Logon parameters to CA Service Desk Manager Web Service
- The URL to the CA Service Desk Manager Web Service

Prerequisite for In-context Launching of CA Service Desk Manager

The CA Service Desk Manager integration supports context-sensitive launches from the DSM Explorer to the CA Service Desk Manager Web GUI. These launches require that you have appropriate access permissions granted in CA Service Desk Manager. Therefore, the user account (user ID and password) with which you are logged in to the DSM Explorer must also be created as a contact in CA Service Desk Manager.

If your CA ITCM user account is unknown in CA Service Desk Manager, you see a log-in screen when you try to launch the CA Service Desk Manager Web GUI.

Prerequisites for CA Service Desk Manager Integration with Multiple Engines

If you are using multiple engines to evaluate policies, the CA Service Desk Manager integration must be activated for all systems an engine is running on, which means the following prerequisites must be met on each of these systems:

- An agent is installed and running.
- The configuration policy that enables the CA Service Desk Manager integration has been dragged-and-dropped onto this agent.
- The .p12 certificate file is imported (if the managed method is used).

Prerequisites for CA Service Desk Manager Integration with Enterprise Manager

To activate the CA Service Desk Manager integration on an enterprise manager, the following prerequisites must be met on the enterprise manager:

- An agent is installed and running, and is connected to one of the linked domain managers.
- The configuration policy that enables the CA Service Desk Manager integration has been dragged-and-dropped onto this agent.
- The .p12 certificate file is imported (if the managed method is used).

About CA ITCM and CA Service Desk Manager Integration

The following considerations are important for you to know as they may affect your CA ITCM and CA Service Desk Manager integration scenarios:

- Software delivery job from an enterprise manager which is "Service Desk enabled" (see page 480)

Software Delivery Job from Enterprise Manager that is Service Desk Enabled

The following applies to the scenario where CA ITCM and CA Service Desk Manager integration is performed on an enterprise manager.

A software delivery job launched from the enterprise manager that is Service Desk enabled does not create a Service Desk ticket, if it fails because DTS plug-ins are stopped on the enterprise manager or the domain manager.

Secure Logon to the CA Service Desk Manager Web Service

The CA ITCM administrator can select between two methods for a secure logon to the CA Service Desk Manager web service:

- A simple logon method that requires a user name and password (not-managed method)
- A managed logon method based on public/private keys and an eTrust PKI encryption

User name/password and public/private key authentication are not available out of the box. A separate configuration step is required after both CA Service Desk Manager and CA ITCM have been successfully installed.

The secure logon method is specified through the sdlogonmanaged parameter in the CA ITCM configuration policy (comstore). The default value of this parameter is Managed, which means that login happens through a certificate and encryption/decryption based on eTrust PKI. The value Notmanaged means that the user logs in using user name and password.

How You Configure Secure Logon

To configure secure logon, the CA ITCM administrator must perform the following configuration steps:

1. Select method of authentication.
2. If you choose the not-managed method, perform the following actions:
   - Create a respective operating system account for CA Service Desk Manager.
   - Configure CA ITCM accordingly through a configuration policy.
3. If you choose the managed method, perform the following actions:
   - Create X.509 certificate with a private key and expose it with a PKCS#12 file. Administrators can use the CA Service Desk Manager utility pdm_pki for this purpose, or supply their own certificates.
   - Import the created policy file into CA ITCM with the CA ITCM utility cacertutil.

User Name and Password Method (Not-managed)

The parameters sdusr and sdpwd of the configuration policy are used for the user name and password, respectively.

CA Service Desk Manager setup automatically loads the contact System_MA_User for use by CA ITCM, and associates this with the CA ITCM Service Aware policy ManagedAssetEvents.

That is, the default value of sdusr is System_MA_User.

To enable user name and password as the logon method, the CA Service Desk Manager administrator must perform the following actions:

- Create an operating system user.
- Edit the contact of the System_MA_User and place the operating system user name in the System login field.

  (By default, system login is equal to System_MA_User.)

The CA ITCM administrator must update the CA ITCM configuration policy to the according contact name and password that was created in CA Service Desk Manager.

Administrators are allowed to create and make use of contact different from System_MA_User. Therefore, they need to change the configuration in CA Service Desk Manager and the CA ITCM configuration policy synchronously.

Certificate or eTrust PKI Method (Managed)

CA Service Desk Manager setup automatically loads the contact System_MA_User for use by CA ITCM and associates this contact with the CA ITCM Service Aware policy ManagedAssetEvents.

To use the certificate (eTrust PKI) as the logon method, the CA Service Desk Manager administrator must perform two steps:

- Create a PKCS#12 file (see page 482).
- Import the PKCS#12 file into the CA ITCM configuration file (see page 483).

Create a PKCS#12 file

Administrators may supply their own keys through a PKCS#12 file. For example, the administrator may use third-party Certificate Authorities for this purpose.

To create a PKCS#12 file, perform the following steps using the CA Service Desk Manager utility (command) pdm_pki:

1. Create a public/private key pair.
2. Associate the public key with the CA ITCM policy in the CA Service Desk Manager database.
3. Create an X.509 certificate with the private key and expose it with a PKCS#12 file.

The pdm_pki utility creates a PKCS#12 file in its working directory with the file name MANAGED_ASSET_EVENTS.p12.

The pdm_pki command has the following format:

```
pdm_pki -p MANAGED_ASSET_EVENTS [-l certificate_file] [-f]
```

-p

Defines the policy code. In this case, the value MANAGED_ASSETS_EVENTS must be used.

-l

Loads a certificate from a file instead of creating a new one.

-f

Forces the replacement of an already existing key.

Import the PKCS#12 File into the CA ITCM Configuration File

To import the PKCS#12 file into the CA ITCM configuration file (comstore), use the CA ITCM utility cacertutil as described in the following way.

The cacertutil command to import the PKCS#12 file in the CA ITCM configuration file (comstore) has the following format:

```
cacertutil import -i:certificate_file
    -ip:MANAGED_ASSET_EVENTS -t:MANAGED_ASSET_EVENTS
    -l:global
```

-i

Identifies the certificate file name.

-ip

Identifies the pass-phrase.

-t

Specifies the identity tag.

-l

Identifies the user.

Settings in the Configuration Policy

Configuration settings for the CA Service Desk Manager integration are specified in the parameter section sdintegration of the CA ITCM configuration file (comstore.xml). Parameters in the configuration file are set up to be centrally managed through a common configuration (CCNF) policy.

The following parameters are used for CA Service Desk Manager integration.

SdIsEnabled

Indicates whether CA Service Desk Manager integration is enabled. If the value of SdIsEnabled is True, CA Service Desk Manager integration is enabled. If the value is False, integration is not enabled.

Default: False

SdEnd

Identifies the URL to the CA Service Desk Manager web service.

Default: http://*myhost*:8080/axis/services/USD_R11_WebService

Replace *myhost* with the appropriate server address of your CA Service Desk Manager web service. Port 8080 is the default.

SdLogonManaged

Indicates how logon to CA Service Desk Manager web service is controlled. If the value is Managed, logon is controlled through PKCS#12 certificate. If the value is Notmanaged, logon is controlled through the user account and password.

Default: Managed

SdUsr

Defines the user account for the logon to the CA Service Desk Manager web service. This parameter is used only when SdLogonManaged is set to Notmanaged.

Default: System_MA_User

SdPwd

Defines the password for the logon to the CA Service Desk Manager web service. This parameter is used only when SdLogonManaged is set to Notmanaged.

Note: In addition to the SdUsr account, the account of the currently logged on user is important. When an ad hoc ticket is created from the DSM Explorer GUI in the context of a managed asset, this account is referred to as the creator of the ticket in CA Service Desk Manager. When a ticket is created in the context of Asset Management or Software Delivery, the ticket creator is always the Administrator.

Default: *Empty*

SdPolicy

Identifies the name of the CA Service Desk Manager Service Aware policy to log into. This parameter is used only when SdLogonManaged is set to Notmanaged. A PKCS#12 certificate being used with the managed logon already includes a policy description that will always override this value. If this parameter is not specified, the default CA Service Desk Manager policy is selected.

Default: MANAGED_ASSET_EVENTS

SdThrottle

Specifies whether network and CPU throttling is enabled. If the value is True, throttling is enabled. If the value is False, throttling is disabled.

Default: False

SdTimeout

Specifies timeout of calls to CA Service Desk Manager web service. The value can be altered to force a timeout on send, receive, and connect. Positive values indicate seconds before timeout, for example, the value 20 specifies timeout after 20 seconds. Negative values indicate milliseconds, for example, the value -200 specifies timeout after 200 milliseconds.

Default: 0 (Infinite)

Chapter 14: Troubleshooting

This section contains the following topics:

CIC Connection Release Error

The CA Content Import Client (CIC) can sometimes fail to release its connection to the Oracle MDB resulting in the following error in the CIC log:

```
[CCMain] WARN  [com.ca.sccc.dbm.CCDBManager] - Failed to uninitialize MDB connection pool for domain 'xxx'
```

DSM Engine Crashes When the Database is Stopped

Symptom:

When I stop the database for maintenance, for example, to take a backup, the engine processes sometimes crash.

Solution:

Verify that you have stopped all the engine processes before you stop the database for maintenance.

Note: If an engine process crashes during the database maintenance, restart the engine process after you restart the database.

Prerequisites for SXP Packager on Windows 8

If you tried creating packages using SXP Packager on the computer, verify that.NET framework 3.5 is installed and enabled on the Windows 8 or Windows Server 2012 computer using the following steps:

Windows 8:

Click Control Panel, Programs, and Features, Turn Windows features on or off. For more information, see http://msdn.microsoft.com/en-us/library/hh506443.aspx.

Windows Server 2012:

Install .NET Framework 3.5 using the Add Roles and Features Wizard. For more information, see http://technet.microsoft.com/en-us/library/hh83180.aspx.

Opening the Exported Reports

The exported files are in Unicode format. To view the files in an application that does not support Unicode, change the encoding to ANSI before opening the file.

Alert Collector Fails to Connect to the Specified Manager

Symptom:

During the Alert Collector installation, when I run the Alert Collector status command, the Alert Collector shows the following message:

Unable to connect to the specified manager.

Solution:

When you install the Alert collector on a standalone server that is configured to connect to either the EM or DM, and fails to connect to the manager. The alert collector connects to the manager the first time to determine the manager type (whether EM or DM). When an invalid role is specified, the manager type is used to validate the specified role and switch to the default role.

Verify whether the CAF runs and works on the stand-alone server and the manager. Alert Collector fetches the required info and works properly. This status message is displayed when the manager of the alert collector is changed and alert collector is relaunched. The same steps apply to fix the issue.

Alert Collector Fails to Connect to the Database

Symptom:

On uploading the alerts to the alert collector, I do not see the uploaded alerts in WAC using the *AlertCollector* status command shows the following message:

Unable to establish a connection to the database.

Solution:

Ensure that the alert collector on a standalone server connects with the database, by verifying the database server connectivity or installing the associated 32-bit DB client tools (such as SQL or Oracle clients) on the machine.

DSM Explorer does not Display Prompt Window in Meeting Mode Connection

Symptom:

When I open DSM Explorer in a domain manager, right click the agent, and establish a meeting mode connection, the application does not display the prompt window.

Solution:

Verify that the libatk-1.0.so.0 package is installed on the agent.

Issues with Changing the Boot Server Configuration from tftp to Share Access Mode in Cluster Setup

Symptom:

When I change the Boot Server configuration from tftp to Share access mode in Cluster setup, I get the following error:

ERROR: trying to create camenu share
ERROR: trying to create sxpsetup share

Solution:

You can set Share access mode as boot server configuration without any errors in CA ITCM application cluster by configuring a Remote Scalability server.

Problem with Size Details of ITCM and CIC Components on the Add/Remove Programs

Symptom:

After I install or upgrade to CA ITCM Release 12.8; Control Panel, Add/Remove Programs does not display the size estimate of CA ITCM, Content Import Client (CIC), Patch Manager, and other CA ITCM components.

Solution:

Obtaining and displaying the size in Control Panel, Add/Remove Programs is a property of Windows OS and not of InstallShield. This behavior occurs due to a change in the functionality with how Microsoft calculates the estimated size on Windows. Size of each installed component is estimated using the OS algorithm. This algorithm can vary in different versions of windows; impacting the display of CA ITCM size estimates.

To populate the size estimates, you can perform the following steps:

Follow these steps:

Microsoft exclusively uses *EstimatedSize* registry key to populate the estimated size value in Add/Remove Programs. To populate the size estimates, you can manually edit *EstimatedSize* registry key in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{PRODUCT_CODE}. See Microsoft documentation for more information.

Error and Delay in Connecting to Technical Support

Symptom:

When I try to access the technical support page from the CA ITCM about screens, I see a script error after some delay.

Solution:

Press Yes and the technical support page appears after some delay. Note this delay is specific to Internet Explorer 7 only.

SE-Linux Support for CA ITCM Components

Linux systems, with the SE-Linux security system enabled, require specific SE-Linux settings for the following CA ITCM components:

DSM Web Services and Web Console

Installation of the CA ITCM Web Services and Web Console is successful on systems with SE-Linux set to the enforcing mode. However, to work with these components, switch to the **permissive** mode in the following manner:

Follow these steps:

- Open the file '/etc/selinux/config' in a text editor.
- Change the flag SELINUX=enforcing to SELINUX=**permissive.**
- Reboot the system.

Junk Text Appears on the Japanese Installer UI

Valid on Japanese Linux

Symptom:

When I launch the installer in Japanese on Linux, the text is shown as junk on the UI.

Solution:

Launch the product installer in command line mode or use silent installation using the response file.

Issue with the Strings at Command Prompt

Valid on Windows and Linux

Symptom:

When I run commands in a localized environment, I see issues with the strings at Command Prompt.

Solution:

To fix the command prompt strings issue, do the following changes:

(For Windows)

This problem occurs when the default code page of the environment is not supported.

For example, when default code page for German and French is 850; Command Prompt strings appear erratically. Note that, for German and French, CA ITCM supports *code page 1252.* You can reset the code page at the environment settings by running the following command:

```
chcp  1252
```

(For Linux)

You can reset the Language parameter in the the following way:

1. Navigate to the *cd\etc\sysconfig* folder, open *i18n.*
2. Modify the Lang parameter in the following way:

   Example:
   (For German) Lang=de_DE.UTF-8

   (For French) Lang=fr_FR.UTF-8

Error While Loading Shared Libraries on a Newer 64-bit Linux OS

Symptom:

Some of the DSM features (such as cfSysTray, remote control connection, dsm properties) do not work properly on newer 64-bit Linux operating systems. For example, when I run cfSystray, the following error message appears:

[root@hostname]# cfsysTray show
cfSysTray: error while loading shared libraries: libgtk-x11-2.0.so.0: wrong ELF class: ELFCLASS64.

Solution:

DSM is a 32-bit application and requires 32-bit version OS libraries. DSM commands failed because the 64-bit Linux operating system does not include 32-bit OS libraries. By default, these libraries are not installed on the newer 64-bit Linux operating systems.

To install the required libraries, see CA Support or contact your system administrator.

Agent Installation on Solaris Fails with an Error

Symptom:

The agent installation on Solaris 10 failed with the following error in the log file:

ld.so.1: setup: fatal: libCstd.so.1: version `SUNW_1.4.2' not found (required by file /opt/CA/DSM/capki/setup)
ld.so.1: setup: fatal: libCstd.so.1: open failed: No such file or directory Killed
/opt/CA/DSM/capki/setup install caller=CAITCM verbose env=all failed with return code = 137
11:43:58 !! Script executed with error: 137
Script or command "capki/pkiInst" failed with exit code 137.
Reason:The script or command encountered a problem.
Action: Find further details in the installation log file /opt/CA/SharedComponents/installer/log/ca-dsm.log.

Solution:

The agent installation on Solaris 10 failed because the libCstd library version is incompatible. To resolve this problem, install the Solaris OS patch 119964-12 or later.

Remote Control on Windows 8 Secure Mode

Symptom:

Remote Control on Windows 8 and Windows Server 2012 supports all the connection modes except Secure control mode.

Solution:

A solution is in progress and planned for our next major release.

Unable to Connect to MDB

Symptom:

While I install CIC, Installer stops with the following error message:

Unable to Connect to MDB. Please check MDB credentials.

Solution:

Ensure that MDB credentials comply to the password policies. CIC supports alpha-numeric characters and the following special characters in MDB password:

SQL

~ ! # $ * ( ) _ + - { } [ ] ? / @

Oracle

$ _

- Reset the MDB password and Installer runs successfully.

For more information about MS-SQL and Oracle database password policy, visit the respective company websites.

DSM Manager Fails to Start after CAM Upgrade

When installing CA ITCM 12.8, CA Message Queuing (CAM) is typically upgraded during the installation process. If the DSM manager fails to start because it cannot connect to CAM, stop the version of CAM that is currently running or reboot after the CA ITCM installation.

Logs in Temp Folder are Deleted

Symptom:

When I install CA ITCM on the computer where Remote Desktop Services are configured, the logs in the temp folder are deleted after the user logs off or when the machine is restarted.

Solution:

Do the following:

- Navigate to *Remote Desktop Services, Remote Desktop Session Host, Do not delete temp folder upon exit* of the computer.
  - If the status is set to Enabled, temporary folders per session of the user are retained when the user logs off from a session.
  - If the status is set to Disabled, temporary folders are deleted when a user logs off, even if the administrator specifies otherwise in the Remote Desktop Session Host Configuration tool.
  - If the status is set to Not Configured, Remote Desktop Services deletes the temporary folders from the remote computer at log-off, unless specified otherwise by the server administrator.

Note: Path to Remote Desktop Services varies from OS to OS version.

MDB Installer Hangs if ORACLE_HOME Variable or ca_itrm Password Is Set Incorrectly

If the ORACLE_HOME environment variable is set incorrectly, the MDB installer hangs during an unattended install, reinstall, or upgrade. Either set the ORACLE_HOME variable correctly or remove the value in this environment variable. The value for ORACLE_HOME is then picked up from the response file.

If you have entered an incorrect ca_itrm password during a reinstall or upgrade (either interactive or unattended), the MDB installer hangs. Verify that the correct ca_itrm password is entered.

Named Instance and Port ID Installation Error

An installation error can occur on Microsoft SQL Server due to the named instance and port ID properties. Verify that you specify the correct port ID.

Response File Contains Unused Entries

The generated response file and the install.rsp template contain the following Microsoft SQL entries: ITRM_DBSQLPORT=1433 and ITRM_SQLADMINUSER=sa. These entries are unused and ignored by the MDB installer.

Synchronization Error from SQL MDB to Oracle MDB Target

Symptom:

When I perform synchronization from a source with MDB on SQL server to a target with MDB on Oracle 11g, the following error is displayed in the engine logs for ITCM R12.5 SP1:

RecImpl_Ado |RecImpl_Ado.cpp |001371|ERROR | FieldLng encounters an undefined VT type =5 for 14

RecImpl_Ado |RecImpl_Ado.cpp |001373|ERROR | FieldLng encounters an undefined VT type =0

Solution:

Apply the testfix RO43621. Follow the instructions the testfix readme.

Synchronization Error on a Target MDB on Oracle

Symptom:

When I perform synchronization with a target MDB that is on Oracle, the following error message is displayed in the engine log file:

```
ERROR  | ERROR:OCIStmtExecute() failed
```

Solution:

Apply the testfix RO43619. Follow the instructions the testfix readme.

Unified Logon from Web Console Fails on Standalone WAC

Symptom:

When I access the Unified Logon feature of Web Console from a supported browser on Windows 2008 and above, log in fails and prompts me to perform an explicit logon.

Solution:

Follow these steps:

1. Verify that the Domain Controller is on windows 2008 or above with the following local policy setting:
   - Network access: Sharing and security model for local accounts: Classic
   - Network access: LAN manager authentication level: Send LM and NTLM Responses
   - Network security: Verify that the minimum session security for NTLM SSP based (including secure RPC) clients is set to 'no minimum'
2. Verify that the Domain Manager is on windows 2008 or above and set the local policy as given in step 1.
3. Verify that the Registry of the Domain manager is on windows 2008 or above and disable the loopback check box:
   Follow these steps:
   a. Click Start, Run.
   b. Type regedit. Click OK.
   c. In Registry Editor, locate and click the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
   d. Right-click LSA and point to New. Click DWORD Value.
   e. Type DisableLoopbackCheck. Press ENTER.
   f. Right-click DisableLoopbackCheck. Click Modify.
   g. In the Value data box, type 1. Click OK.
4. Verify the settings of the browser (IE or Firefox) on the User's Box.

   Note: For more information about browser settings for unified logon, see Configure Browser Settings for Unified Logon topic in the *Web Console Help*.
5. If the browser is on the server class machine, follow the local policy settings given in step 1.

High CPU Utilization after DSM Manager Upgrade

Symptom:

After upgrading DSM Manager to the current release, CPU utilization becomes high due to old crypto modules running with tomcat 7 and JRE 1.7.

Solution:

This problem occurs when you upgrade ITCM only with DSM Manager and not upgrading the Patch Manager. Upgrade the Patch Manager to the current ITCM release.

Infrastructure Deployment Fails if a Windows 2012 Virtual Machine is Involved

Symptom:

infrastructure deployment fails if one of the following in a Windows 2012 virtual computer.

- Domain Manager
- Scalability Server
- Target Computer

Solution:

Follow the VMware Knowledge Base entry: Possible data corruption after a Windows 2012 virtual machine network transfer (2058692).

Appendix A: Automation Service Configuration File

The automation service configuration file contains configuration parameters that automated migration uses for various tasks. Although all the parameters are described in this section, some parameters are only informational. We recommend that you do not change the parameters that are only informational.

Note: An integer value in the automation.config file must not contain or be surrounded by spaces. When you specify an integer value in the automation.config file, verify that there is no space, within and around the value. Any space in the integer value can result in the malfunctioning of the automation service.

AssessmentServiceEPR

Defines the end point URL of assessment service. This parameter is only informational.

ITCMEPR

Defines the end point URL of CA ITCM web service. This parameter is only informational.

ITPAMEPR

Defines the end point URL of CA IT PAM web service. This parameter is only informational.

AutomationServiceEPR

Defines the end point URL of automation service. This parameter is only informational.

JNI_BIN_PATH

Defines the JNI path to get comstore values. This parameter is only informational.

DEFAULT_MANAGER

Defines the name of the default manager for Web Console and CA ITCM web services. This parameter is only informational.

WipeAndReloadProcess

Defines the path to CA IT PAM process definition for Wipe and Reload migration. Change this parameter only if you have customized the process definition.

MachineReplacementProcess

Defines the path to CA IT PAM process definition for Machine Replacement migration. Change this parameter only if you have customized the process definition.

MaxNumberOfITPAMInstances

Defines the maximum number of CA IT PAM instances that automation service can run concurrently. Depending on load your CA IT PAM server can handle, you change this value.

Note: Automation service creates one CA IT PAM instance per computer in the migration job.

ProcessLaunchInterval

Defines the time interval (in seconds) between the creation of CA IT PAM instances.

TimeOutForOSIMJobs

Defines the timeout period (in seconds) before which the computer must start the OSIM job. After the timeout period, the OSIM jobs are canceled and OS migration job fails for the computer.

WaitForBootServer

Specifies that the activation of the OS installation waits until a boot server picks up the target and reports to the domain manager.

WaitForOSImage

Specifies that the activation of the OS installation waits until the required OS and Boot image is available on the assigned boot server.

WakeOnLAN

Specifies whether the boot server must wake up the target computer before OS installation.

Reboot

Specifies whether the boot server must force the reboot on the target computer before activating installation, if set to true.

ContainerPriority

Defines the priority for software job containers created for migration job.

DeliveryCalender

Specifies the name of the delivery calendar you want to use. Leave this parameter blank, if you do not want to use a delivery calendar.

IgnoreJobCalendarsOnTargetComputers

Specifies whether the job option, Ignore job calendars on target computers, must be set when a RAC container is created. If this policy is set to False, calendars are not ignored at target computers. If True, calendars are ignored at target computers.

JobsTriggerSS

Specifies that the scalability server must initiate and execute the job at the scheduled time.

RemoveInstallationHistory

Specifies that the existing installation records will be deleted, thus preventing the job from failing with a status of Already Installed, before the install process is activated.

RunFromSS

Specifies whether the job check program of the target computer must release communication with the server during execution of the job. When the job has finished, the agent reconnects to the server to report job status.

TimesRelativeToEM

Specifies that the activation time specified must be interpreted as universal time. The time deviation configured on each domain manager is considered for converting the time received into the local system time.

UseDeliveryCalender

Specifies whether to use the delivery calendar for the job.

SoftwareBlackList

Defines the list of software packages that are used to exclude computers from OS migration job. The computers that have any of these software packages installed are automatically excluded from OS migration.

MaximumDelayOfJobContainer

Defines the time for which the job container waits for additional computers after adding the first computer before it seals the container. Additional containers are automatically created, if necessary.

MaxNumberOfTargetsPerJobContainer

Defines the maximum number of target computers per job container. After the job container reaches this limit, the container is closed and a new job container is created for remaining computers.

LastTargetInContainerOptimization

Specifies whether to activate the job container immediately, when there are no targets left in the migration job. The container is activated immediately even if the targets in the container is less than the number specified in MaxNumberOfTargetsPerJobContainer and without waiting for MaximumDelayOfJobContainer time. This parameter is only informational.

Default: True

RenamePackageName

Defines the rename software package used for renaming the computers. This parameter is only informational.

RenamePackageVersion

Defines the version of the rename software package used for renaming the computers. This parameter is only informational.

RenameProcedure

Defines the rename software package procedure used for renaming the computers. This parameter is only informational.

AutomationJobScheduleInterval

Defines the time delay (in seconds) for which the automation services waits before scheduling the next automation job.

AutomationJobSchedulerBatchSize

Defines the number of targets scheduled by automation service before checking the ITPAM instance status for the scheduled targets and updates the status as Migration Successful or Migration Failed. Depending on the load on the CA IT PAM server and how frequently you want to update the status of the target, you can change this value.

Log4j Properties

Defines the following log4j properties:

– log4j.rootLogger

– log4j.appender.A1

– log4j.appender.A1.layout

– log4j.appender.A1.layout.ConversionPattern

– log4j.appender.A1.MaxFileSize

– log4j.appender.A1.MaxBackupIndex

For example, you can change the following parameters to change the log level, the file size, or the number of log files created:

log4j.rootLogger=ERROR, A1

Note: Change this value to DEBUG or INFO to change the log level accordingly.

log4j.appender.A1.MaxFileSize=5000KB

log4j.appender.A1.MaxBackupIndex=1

Note: For more information about the Log4j properties, see the documentation of org.apache.log4j.PropertyConfigurator.

Appendix B: Ports Used by CA IT Client Manager

The following tables describe in detail the port usage of the various DSM components. These tables are comprehensive and contain duplication in order to provide a complete picture for each component.

This section contains the following topics:

General Considerations of Port Usage

In general, for the majority of intercomponent communications across the network, CA ITCM only requires two ports to be opened, specifically UDP port 4104 for (typically light) message-based traffic and TCP port 4728 for (typically bulk) stream traffic.

By default, remote communications through CA Message Queuing (CAM) will use UDP over port 4104, as documented in the following tables. You can configure CAM to use TCP for remote communications (in some circumstances this can be preferable), in which case TCP with a source port of ANY and a listening port of 4105 will be used. Remote communications through CAM over TCP is not documented in the tables. CAM is also used extensively for local communications, that is, between components running on the same machine. In this case, TCP on port 4105 is used.

Certain features within CA ITCM can use file shares if configured to do so. In this case, appropriate file share ports must be opened. Specific port numbers will vary depending on the operating environment (platform) and the mechanisms available and configured.

Typical file share ports are as follows:

Windows

Either 139/TCP (old style) or 445/TCP (new style)

Linux and UNIX

2049/TCP (NFS)

Ports Used by the Enterprise Manager

The following tables provide an overview of the ports used for communications from and to the enterprise manager.

Communications from the Enterprise Manager

From	Port	To	Port	Protocol	Product	Description
Enterprise manager	Any	Enterprise manager	4105	TCP	All	Local communications through CAM
Enterprise manager	4104	Domain manager	4104	UDP	All	Communications through CAM across network
Enterprise manager	Any	Directory server	389	TCP	All	LDAP directory access
Enterprise manager	Any	Directory server	636	TCP	All	LDAP over SSL directory access

From	Port	To	Port	Protocol	Product	Description
Enterprise manager	Any	Domain manager	4728	TCP	Software Delivery	DTS file transfer

Communications to the Enterprise Manager

From	Port	To	Port	Protocol	Product	Description
Explorer	4104	Enterprise manager	4104	UDP	All	Communications through CAM across network
Web Browser	Any	Enterprise manager	80	HTTP	All	Web Console access
Web Services Client	Any	Enterprise manager	80	HTTP	All	Access to Web Services API from remote client application
Domain manager	Any	Enterprise manager	4728	TCP	Software Delivery	DTS file transfer
Explorer	File share ports	Enterprise manager	File share ports	UDP	Software Delivery	NOS-based file transfer
Explorer	Any	Enterprise manager	4728	TCP	Software Delivery	NOS-less file transfer
Packager	4104	Enterprise manager	4104	UDP	Software Delivery	Communications through CAM across network

Notes:

- If secure HTTP communications is configured for use by the Web Console and the Web Services components, port 443 (default) would be used for listening on the domain manager or enterprise manager.
- Web Console uses Apache Tomcat. By default, Tomcat is installed and configured to use ports 8090 (startup), 8095 (shutdown), and 8020 (ajp13). However, typically these are used only locally.

Ports Used by the Domain Manager

The following tables provide an overview of the ports used for communications from and to domain managers.

Communications from the Domain Manager

From	Port	To	Port	Protocol	Product	Description
Domain manager	Any	Domain manager	4105	TCP	All	Local communications through CAM
Domain manager	4104	Enterprise manager	4104	UDP	All	Communications through CAM across network
Domain manager	4104	Remote domain engine	4104	UDP	All	Communications through CAM across network
Domain manager	4104	Scalability server	4104	UDP	All	Communications through CAM across network
Domain manager	Any	Directory server	389	TCP	All	LDAP directory access
Domain manager	Any	Directory server	636	TCP	All	LDAP over SSL directory access
Domain manager	4104	Explorer	4104	UDP	All	Communications through CAM across network
Domain manager	Any	Enterprise manager	4728	TCP	Software Delivery	DTS file transfer: distribution order acks
Domain manager	Any	Scalability server	4728	TCP	Software Delivery	DTS file transfer: package transfer

Communications to the Domain Manager

From	Port	To	Port	Protocol	Product	Description
Enterprise manager	4104	Domain manager	4104	UDP	All	Communications through CAM across network
Explorer	4104	Domain manager	4104	UDP	All	Communications through CAM across network
Scalability server	4104	Domain manager	4104	UDP	All	Communications through CAM across network
Web browser	Any	Domain manager	80	HTTP	All	Web Console access

From	Port	To	Port	Protocol	Product	Description
Web Services client	Any	Domain manager	80	HTTP	All	Access to Web Services API from remote client application
Remote domain engine	4104	Domain manager	4104	UDP	All	Communications through CAM across network
Agent	4104	Domain manager	4104	UDP	Remote Control Software Delivery	Communications through CAM across network: SD Catalog, RC Host Auth., RC Viewer GAB
Scalability server	Any	Domain manager	4728	TCP	Software Delivery	NOS-less file transfer: job output files
Enterprise manager	Any	Domain manager	4728	TCP	Software Delivery	DTS file transfer: package transfer
Explorer	File share ports	Domain manager	File share ports	TCP/UDP	Software Delivery	NOS-based file transfer: package registration
Explorer	Any	Domain manager	4728	TCP	Software Delivery	NOS-less file transfer: package registration
Packager	4104	Domain manager	4104	UDP	Software Delivery	Package registration control data
Packager	Any	Domain manager	4728	TCP	Software Delivery	NOS-less file transfer: package registration

Notes:

- If secure HTTP communications is configured for use by the Web Console and the Web Services components, port 443 (default) would be used for listening on the domain manager or enterprise manager.
- Web Console uses Apache Tomcat. By default, Tomcat is installed and configured to use ports 8090 (startup), 8095 (shutdown), and 8020 (ajp13). However, typically these are used only locally.

Ports Used by Infrastructure Deployment

Infrastructure deployment is part of the domain manager. Its port usage is provided in a separate section to highlight the fact that these ports need to be open only if or while infrastructure deployment is used.

The ports mentioned in the following tables (excluding port 7) are used to push out the infrastructure deployment primer from the domain manager. If a customer is willing to install the primer manually or does not want to use infrastructure deployment at all, the ports will not need to be opened up. It is not necessary to open all ports for all targets. The ports do not need to be left open; they need to be opened only during the deployment period.

In addition, the customer can open up a subset of MS Share/telnet and FTP/SSH ports depending on the communications mechanisms used.

Communications from the Domain Manager

From	Port	To	Port	Protocol	Product	Description
Domain manager	Any	Target	7	TCP	All	Echo Request. Used during target scan. Usage of this port can be disabled through an appropriate setting in the configuration policy
Domain manager	File share ports	Target	File share ports	TCP UDP	All	Windows NOS-based file transfer of primer package. Using ADMIN$
Domain manager	Any	Target	135	TCP	All	Windows RPC call to start primer install
Domain manager	Any	Target	21	TCP	All	FTP-based file transfer of primer package
Domain manager	Any	Target	22	TCP	All	UNIX ssh / secure FTP-based file transfer of primer package. Pushed from the domain manager.
Domain manager	Any	Target	23	TCP	All	UNIX telnet connection used to initiate FTP-based file transfer of primer package on target.

Communications to the Domain Manager

From	Port	To	Port	Protocol	Product	Description
Target	Any	Domain manager	20 21	TCP	All	FTP-based file transfer of primer package

Ports Used by the Scalability Server

The following tables provide an overview of the ports used for communications from and to scalability servers.

Communications from the Scalability Server

From	Port	To	Port	Protocol	Product	Description
Scalability server	Any	Scalability server	4105	TCP	All	Local communications through CAM
Scalability server	4104	Domain manager	4104	UDP	All	Communications through CAM across network
Scalability server	4104	Domain engine	4104	UDP	All	Communications through CAM across network
Scalability server	4104	Agent	4104	UDP	All	Communications through CAM across network: Configuration, SD trigger job check, AM trigger job check
Scalability server	Any	Domain manager	4728	TCP	Software Delivery	NOS-less file transfer: Job output files
Scalability server	Any	Agent	4728	TCP	Software Delivery	DTS file transfer: Package transfer
Scalability server	554	Agent	554	TCP	Software Delivery	RTSP (not secured) for App-V virtual application services
Scalability server	322	Agent	322	TCP	Software Delivery	RTSPS (secured) for App-V virtual application services

Communications to the Scalability Server

From	Port	To	Port	Protocol	Product	Description
Domain manager	4104	Scalability server	4104	UDP	All	Communications through CAM across network
Domain engine	4104	Scalability server	4104	UDP	All	Communications through CAM across network
Agent	4104	Scalability server	4104	UDP	All	Communications through CAM across network
Agent	Any	Scalability server	4728	TCP	All	NOS-less file transfer Backup data transfer
Agent	File share ports	Scalability server	File share ports	TCP	Software Delivery	NOS-based file transfer
Domain manager	Any	Scalability server	4728	TCP	Software Delivery	DTS file transfer: Package transfer
Agent	554	Scalability server	554	TCP	Software Delivery	RTSP (not secured) for App-V virtual application services
Agent	322	Scalability server	322	TCP	Software Delivery	RTSPS (secured) for App-V virtual application services

Ports Used by the Boot Server

The boot server is part of the scalability server. Its port usage is provided in a separate section to highlight the fact that these ports need to be open only if OS Installation Management (OSIM) features are used.

Communications to the Scalability Server

From	Port	To	Port	Protocol	Product	Description
Target	68	Scalability server	67	UDP	Software Delivery	Bootstrap Protocol Client – bootpc
Target	Any	Scalability server	69	UDP	Software Delivery	Trivial File Transfer (TFTP)

From	Port	To	Port	Protocol	Product	Description
PXE target	Any	Scalability server	4011	UDP	Software Delivery	(optional) Alternate Service Boot – altserviceboot.binl (PXE) If port 4011 is not available, port 67 is used instead.
Target	File share ports	Scalability server	File share ports	TCP/UDP	Software Delivery	NOS-based file transfer

Ports Used by the Engine

The following tables provide an overview of the ports used for communications from and to an engine.

Communications from the Engine

From	Port	To	Port	Protocol	Product	Description
Any engine	Any	Any Engine	4105	TCP	All	Local communications through CAM
Any engine	Any	Content server	443 or 5250	TCP	All	Software signature download from CA Content web site
Any engine	Any	Directory server	389	TCP	All	LDAP directory access: Directory sync, Queries, Reports
Any engine	Any	Directory server	636	TCP	All	LDAP over SSL directory access: Directory sync, Queries, Reports
Any engine	Any	SMTP server	25	TCP/UDP	Asset Management	Sending email on policy violation
Domain engine	4104	Scalability server	4104	UDP	All	Communications through CAM across network

From	Port	To	Port	Protocol	Product	Description
Remote domain engine	4104	Domain manager	4104	UDP	All	Communications through CAM across network
Remote enterprise engine	4104	Enterprise manager	4104	UDP	All	Communications through CAM across network

Communications to the Engine

From	Port	To	Port	Protocol	Product	Description
Enterprise manager	4104	Remote enterprise engine	4104	UDP	All	Communications through CAM across network
Domain manager	4104	Remote domain engine	4104	UDP	All	Communications through CAM across network. Notifications, for example, ad hoc query evaluation
Explorer	4104	Any engine	4104	UDP	All	Communications through CAM across network
Scalability server	4104	Domain engine	4104	UDP	All	Communications through CAM across network

Ports Used by the Agent

The following tables provide an overview of the ports used for communications from and to agents.

Communications from the Agent

From	Port	To	Port	Protocol	Product	Description
Agent	Any	Agent	4105	TCP	All	Local communications through CAM
Agent	4104	Scalability server	4104	UDP	All	Communications through CAM across network
Agent	Any	Scalability server	4728	TCP	All	NOS-less file transfer Backup data transfer

From	Port	To	Port	Protocol	Product	Description
Agent	4104	Domain manager	4104	UDP	Remote Control Software Delivery	Communications through CAM across network: SD Catalog, RC Host Auth., RC Viewer GAB
Agent	File share ports	Scalability server	File share ports	TCP	Software Delivery	NOS file transfer
Agent	554	Scalability server	554	TCP	Software Delivery	RTSP (not secured) for Microsoft App-V streaming communications
Agent	322	Scalability server	322	TCP	Software Delivery	RTSPS (secured) for Microsoft App-V streaming communications

Communications to the Agent

From	Port	To	Port	Protocol	Product	Description
Explorer	4104	Agent	4104	UDP	All	Instant Diagnostics (DSM component info) SD trigger job check AM trigger job check
Scalability server	4104	Agent	4104	UDP	All	Communications through CAM across network: Configuration SD trigger job check AM trigger job check
Scalability server	Any	Agent	4728	TCP	Software Delivery	DTS file transfer: package transfer
Packager	Any	Agent	3001, 3002	UDP	All	DSM service locator
Explorer	Any	Agent	4728 *)	TCP	Remote Control	RC Viewer to RC Host
Scalability server	554	Agent	554	TCP	Software Delivery	RTSP (not secured) for Microsoft App-V streaming communications
Scalability server	322	Agent	322	TCP	Software Delivery	RTSPS (secured) for Microsoft App-V streaming communications

Notes:

- *) in the table indicates that the Remote Control Host will also listen on TCP port 798 if legacy Remote Control Viewer support is enabled.
- A scalability server may be running on the same computer as a domain manager.

Ports Used by the Packager

The following tables provide an overview of the ports used for communications from the Software Management Packager.

Communications from the Packager

From	Port	To	Port	Protocol	Product	Description
Packager	4104	Enterprise manager	4104	UDP	Software Delivery	Package registration control data
Packager	Any	Enterprise manager	4728	TCP	Software Delivery	NOS-less file transfer: package registration
Packager	4104	Domain manager	4104	UDP	Software Delivery	Package registration control data
Packager	Any	Domain manager	4728	TCP	Software Delivery	NOS-less file transfer: package registration
Packager	Any	Agent	3001, 3002	UDP	All	CA ITCM service locator

Ports Used by the DSM Explorer and Reporter

The following tables provide an overview of the ports used for communications from the DSM Explorer and DSM Reporter and to the DSM Explorer.

Communications from the Explorer and Reporter

From	Port	To	Port	Protocol	Product	Description
Explorer	Any	Explorer	4105	TCP	All	Local communications through CAM, Notification messages
Explorer	4104	Enterprise manager	4104	UDP	All	Communications through CAM across network

From	Port	To	Port	Protocol	Product	Description
Explorer	4104	Domain manager	4104	UDP	All	Communications through CAM across network
Explorer	4104	Agent	4104	UDP	All	Instant Diagnostics (DSM component info) SD trigger job check AM trigger job check
Explorer	4104	Any engine	4104	UDP	All	Communications through CAM across network
Explorer	Any	Agent	4728	TCP	Remote Control	RC Viewer to RC Host
Explorer	File share ports	Enterprise manager	File share ports	UDP	Software Delivery	NOS-based file transfer: package registration
Explorer	Any	Enterprise manager	4728	TCP	Software Delivery	NOS-less file transfer: package registration
Explorer	File share ports	Domain manager	File share ports	TCP UDP	Software Delivery	NOS-based file transfer: package registration
Explorer	Any	Domain manager	4728	TCP	Software Delivery	NOS-less file transfer: package registration

Communications to the Explorer

From	Port	To	Port	Protocol	Product	Description
Domain manager	4104	Explorer	4104	UDP	All	Communications through CAM across network
Enterprise manager	4104	Explorer	4104	UDP	All	Communications through CAM across network

Ports Used by the ENC Gateway

The following table provides an overview of the ports used for communications by the ENC Gateway functionality.

From	Port	To	Port	Protocol	Product	Description
ENC Client	Any	ENC Gateway Server	443	TCP	All	ENC Client registration, connection requests, listen requests.
ENC Client	Any	ENC Gateway Server	80	TCP	All	Communications through CAM across network
ENC Gateway Server	Any	ENC Gateway Server	443	TCP	All	ENC Gateway Server registration, relay of client requests to ENC Gateway Manager, relay of data between connected ENC Clients
ENC Client	Any	Internet Proxy	1080	TCP	All	Communications through proxy
ENC Client	Any	Internet Proxy	80	TCP	All	Communications through proxy

Ports Used by Quarantine of AMT Asset

CA IT Client Manager (CA ITCM) supports the Intel Advanced Management Technology (AMT). In this context an AMT quarantine policy is introduced, which is a circuit breaker feature adding a filter for incoming and outgoing network traffic on AMT devices.

The quarantine policy provides a new management state for the AMT-enabled asset. We can temporarily lock down this asset while performing advanced management on CA ITCM. The quarantine policy closes all normal inbound and outbound traffic, except for the ports used by AMT devices and CA ITCM for communication, that is, the Intel AMT asset in quarantine can be fully managed by CA ITCM.

The quarantine policy affects ports as follows:

- AMT Send/Receive ARP traffic from AMT computer (port 67)
- AMT Send/Receive data traffic on AMT ports (ports 16992-16995)
- CA ITCM Send/Receive on port 4104

  CA ITCM Send/Receive on port 4105

  CA ITCM Send/Receive on port 4728
- Support port for DHCP Service where port 53 is open for Receive.
- Support port for DNS Service where port 63 is open for Send/Receive.

MDB Port Usage

The default ports used for MDB communications are as follows:

- Oracle: 1521
- Microsoft SQL Server: 1433

A database administrator can change the port assignments at the database site.

Appendix C: Software Delivery Procedures for Installation

The installer in CA IT Client Manager provides a set of predefined software delivery (SD) procedures for the installation packages.

This section contains the following topics:

Important Notes on the Uninstall Procedure

Before using the software delivery (SD) agent Uninstall procedure please note the following:

- The SD agent plug-in Uninstall procedure must be sequenced as the last one in the job container, because it is the SD agent plug-in that performs the package uninstallation jobs.
- As the Data Transport Service (DTS) agent plug-in is a separate package on Windows, uninstalling the SD agent does not implicitly uninstall the DTS agent. The DTS agent must be uninstalled through a separate job, but this job can be incorporated in the same job container.

CA DSM Agent + AM, RC, SD Plugin(s) Linux (Intel) ENU

This installation package has the following software delivery procedures predefined:

- Install
- Scan SM Installer installations
- Scan SWD (scans SD proprietary agent db about installed packages)
- Scan SWD: Linux software
- SM Installer: Disable trace
- SM Installer: Enable trace
- SM Installer: Get all traces
- SM Installer: Get latest trace
- Uninstall all of CA ITCM
- Uninstall only all agent plugins

CA DSM Agent + Asset Management Plugin Linux (Intel) ENU

This installation package has the following software delivery procedures predefined:

- Install
- Uninstall all of CA ITCM
- Uninstall only asset management plugin

CA DSM Agent + Basic Inventory Plugin Linux (Intel) ENU

This installation package has the following software delivery procedures predefined:

- Install
- Uninstall all of CA ITCM

CA DMPrimer Linux (Intel) ENU

This installation package has the following software delivery procedures predefined:

- Install
- Uninstall all of CA ITCM

SMPackager (Linux)

This installation package has the following software delivery procedures predefined:

- Install Package
- Reinstall Package
- Uninstall Package

CA DSM Remove Legacy Agent Linux (Intel) ENU

This installation package has the following software delivery procedures predefined:

- Remove all
- Remove AM
- Remove SD

CA DSM Agent + Remote Control Plugin Linux (Intel) ENU

This installation package has the following software delivery procedures predefined:

- Centrally Managed Host Only
- Standalone Agent
- Uninstall all of CA ITCM
- Uninstall only Remote Control plugin

CA DSM Agent + Software Delivery Plugin Linux (Intel) ENU

This installation package includes the Data Transport plugin.

This installation package has the following software delivery procedures predefined:

- Install
- Scan SM Installer installations
- Scan SWD
- Scan SWD: Linux software
- SM Installer: Disable trace
- SM Installer: Enable trace
- SM Installer: Get all traces
- SM Installer: Get latest trace
- Uninstall all of CA ITCM
- Uninstall only Software Delivery plugin

CA DSM Scalability Server Linux (Intel) ENU

This installation package has the following software delivery procedures predefined:

- Disable Boot Server share
- Disable MSILIB share
- Disable NFS share
- Disable Samba share
- Disable SDLIB share
- Enable Boot Server share
- Enable MSILIB share
- Enable NFS share
- Enable Samba share
- Enable SDLIB share
- Install
- Synchronize CCS Calendar
- Synchronize Software Job Records
- Synchronize Software Staging Library
- Uninstall all of CA ITCM
- Uninstall only Scalability Server + Agents

CA DSM Agent + AM, RC, SD Plugin(s) Win32

This installation package has the following software delivery procedures predefined:

- Install
- Uninstall

CA DSM Agent + Asset Management Plugin

This installation package has the following software delivery procedures predefined:

- Detect
- Install
- Local Repair
- Uninstall
- Verify

CA DSM Agent + Basic Inventory Plugin

This installation package has the following software delivery procedures predefined:

- Detect
- Install
- Local Repair
- Uninstall
- Verify

CA DSM Agent + Data Transport Plugin

This installation package has the following software delivery procedures predefined:

- Detect
- Install
- Local Repair
- Uninstall
- Verify

CA DSM Agent + Remote Control Plugin

This installation package has the following software delivery procedures predefined:

- Centrally Managed Complete Agent
- Centrally Managed Host Only
- Detect
- Local Repair
- Standalone Agent
- Uninstall
- Verify

CA DSM Agent + Software Delivery Plugin

This installation package does not include the Data Transport plug-in.

This installation package has the following software delivery procedures predefined:

- Catalog: Add
- Catalog: Remove
- Detect
- Diagnostics: Get configuration and version information (dsmdiag information)
- Install
- Local Repair
- Scan MSI (scans local MSI database about installed packages)
- Scan SM Installer installations (scans SXP packages installed on the agent)
- Scan SWD (scans SD proprietary agent db about installed packages)
- SM Installer: Disable trace
- SM Installer: Enable trace
- SM Installer: Get all traces
- SM Installer: Get history
- SM Installer: Get latest trace
- SM Installer: Get user history
- SM Installer: Get user trace
- Uninstall
- Verify

CA DSM Constant Access (Intel AMT)

This installation package has the following software delivery procedures predefined:

- Install
- Uninstall

CA DSM eTrust PKI

This installation package has the following software delivery procedure predefined:

- Install

CA DSM Explorer

This installation package has the following software delivery (SD)-related procedures predefined:

- Detect
- Install
- Install (without Reporter)
- Install AM
- Install AM (without Reporter)
- Install AM + RC
- Install AM + RC (without Reporter)
- Install AM + SD
- Install AM + SD (without Reporter)
- Install RC
- Install RC (without Reporter)
- Install SD
- Install SD (without Reporter)
- Install SD + RC
- Install SD + RC (without Reporter)
- Local Repair
- Uninstall
- Verify

CA DSM Manager

This installation package has the following software delivery procedure predefined:

- Detect

CA DSM Scalability Server

The scalability server installation package depends on the "CA DSM Agent + Data Transport plugin" package.

The scalability server package has the following software delivery procedures predefined:

- Detect
- Disable Boot Server share
- Disable MSILIB share
- Disable SDLIB share
- Enable Boot Server share
- Enable MSILIB share
- Enable SDLIB share
- Install
- Local Repair
- Synchronize CCS Calendar
- Synchronize Software Job Records
- Synchronize Software Staging Library
- Uninstall
- Verify

CA DSM Secure Socket Adapter

This installation package has the following software delivery procedures predefined:

- Install
- Uninstall

CA DSM Remove Legacy Agent Win32

This installation package has the following software delivery procedures predefined:

- Remove AM
- Remove RC
- Remove SD
- Remove all

Appendix D: Current Certificates Provided by CA IT Client Manager

CA IT Client Manager provides common and application-specific certificates that are listed following. For information on how to work with and customize certificates see "How to Introduce Your Own X.509 Certificates into the Install Image" (see page 216) and "Installation of Application-specific Certificates" (see page 383).

This section contains the following topics:

Common Certificates

The common DSM certificates are listed following.

Default DSM Root Certificate

DN:

CN=DSM Root,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=DSM Root,O=Computer Associates,C=US

Default Basic Host Identity Certificate

DN:

CN=Generic Host Identity,O=Computer Associates,C=US

URI:

x509cert://DSM r11/CN=Generic Host Identity,O=Computer Associates,C=US

Tag:

dsmcommon

Usage:

Basic host identity provision.

Where:

All nodes in the enterprise.

Application-specific Certificates

The application-specific certificates are used for object-level security authorization in the management database (MDB). If you create new certificates, which do not use the default names, you must ensure that you update cfcert.ini with the new URIs before the manager installation or you must create new security profiles with the rights and privileges afforded to the default security profiles.

Please refer to the description of the [Tags] section of the cfcert.ini file (see page 218).

Directory Synchronization Certificate

DN:

CN=DSM Directory Synchronisation,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=DSM Directory Synchronisation,O=Computer Associates,C=US

Tag:

dsm_cmdir_eng

Usage:

To allow the directory synchronization engine job to authenticate to a manager.

Common Server Registration Certificate

DN:

CN=DSM Common Server Registration,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=DSM Common Server Registration,O=Computer Associates,C=US

Tag:

dsm_csvr_reg

Usage:

Scalability server and manager registration to authenticate to a manager.

Configuration and State Management Certificate

DN:

CN=Configuration and State Management,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=Configuration and State Management,O=Computer Associates,C=US

Tag:

csm

Usage:

Authentication of the CSM agent controller.

Software Delivery Agent Mover Certificate

DN:

CN=DSM r11 Agent Mover,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=DSM r11 Agent Mover,O=Computer Associates,C=US

Tag:

dsmagtmv

Usage:

Unicenter Software Delivery agent mover.

Where:

Manager nodes.

Software Delivery Catalog Certificate

DN:

CN=DSM r11 Software Delivery Catalog,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=DSM r11 Software Delivery Catalog,O=Computer Associates,C=US

Tag:

dsmsdcat

Usage:

Software Delivery Catalog.

Where:

Manager nodes, Agent nodes (Windows only).

Notes:

- Software Delivery Catalog certificate has Write (W) permission on Computers and User Profiles. The certificate is present on all Domain Managers and remote Engines.
- Do not change the computer and user profile class permissions of a certifcate on the Domain Manager or any of its remote Engines.
- Do not delete either the default or a user specified software delivery catalog certificate with the same dsmsdcat tag.

Enterprise Access Certificate

DN:

CN=Enterprise Access,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=Enterprise Access,O=Computer Associates,C=US

Tag:

ent_access

Usage:

Enterprise password access.

Domain Access Certificate

DN:

CN=Domain Access,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=Domain Access,O=Computer Associates,C=US

Tag:

dom_access

Usage:

Domain password access.

Reporter Access Certificate

DN:

CN=Reporter Access,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=Reporter Access,O=Computer Associates,C=US

Tag:

rep_access

Usage:

Reporter password access.

Appendix E: Security Area Support Use Cases

This section covers the most important use cases of area support from the user's perspective, and describes how area support functions.

For basic information about security area support and area permissions, see the Security Area Support (see page 410) and Area Permissions (see page 397) sections.

The descriptions of the use cases follow all the same structure, as follows:

Scenario:

Gives a brief explanation of the user scenario. It describes what a user wants to do.

Pre-Condition(s):

Defines what objects are defined before the user is doing the action described in the Action(s) section.

Action(s):

Describes what a user is doing.

Post-Condition(s):

Defines the properties of the objects involved in the scenario after a user has done the previous action.

This section contains the following topics:

Security Area Support for Security Profiles

The security area support for security profiles follows these rules:

- For the Everyone profile it is not allowed to enable or disable area support. Access to any area is denied.
- For the Distributor profile you need full access on the area support security class to enable or disable area support.

Use Case: Installing CA ITCM

Scenario:

A user wants to install CA ITCM.

Pre-Condition:

No previous version of CA ITCM is installed on the computer.

Action:

The user installs CA ITCM.

Post-Conditions:

- Default built-in profiles are installed.
- Area support is disabled (global settings).
- Default area permissions are set to "show all areas."
- The Everyone profile has no access to any area.
- The Administrator profile has full access to all areas and cannot be changed.
- There are no predefined area definitions installed.

Use Case: Upgrading an Existing Installation

Scenario:

A user wants to upgrade an existing installation .

Pre-Condition:

The user has CA ITCM installed.

Action:

The user starts the DSM MDB installation for upgrading the MDB.

Post-Conditions:

- The MDB Schema is changed or upgraded.
- Area support is disabled after the installation.
- The area_aces are created for all existing secured objects where the value is set as specified in the default settings for the area code.

Note: After upgrade all objects are visible in all areas. This is the default configuration.

Use Cases: Security Profiles

The following important user scenarios regarding security profiles are considered in the context of security area support:

- Creating a security profile (see page 540)
- Changing area settings for a security profile (see page 540)
- Deleting a security profile (see page 541)

Use Case: Creating a Security Profile

Scenario:

An administrator wants to create a new security profile.

Pre-Condition:

The security profile does not exist.

Action:

The administrator creates the new security profile where one or more area codes are assigned.

Post-Conditions:

- The security profile is created.
- All security class-level permissions are created for the new security profile.
- The object-level permission is calculated for all existing secured objects. The permissions are calculated for the existing secured objects (including the groups). Object permissions are derived from the class-level permissions.
- The area permissions are created and derived from area permissions assigned to the security profile.

Use Case: Changing Area Settings for a Security Profile

Scenario:

An administrator wants to change the area code assigned for a security profile.

Pre-Condition:

The security profile exists and one or more areas are assigned to the profile.

Action:

The administrator changes the area code for a security profile from the old area code to the new one.

Post-Condition:

The area_aces of secured objects are not changed.

Use Case: Deleting a Security Profile

Scenario:

An administrator wants to delete a security profile.

Pre-Condition:

The security profile exists and one or more areas are assigned to the profile.

Action:

The administrator deletes the security profile.

Post-Conditions:

- The security profile is deleted.
- All permissions information regarding the secured objects and the deleted security profile are also deleted.

Use Cases: Computers

The following important user scenarios regarding computers are considered in the context of security area support:

- Creating a computer manually (see page 541)
- New DSM agent was detected (see page 542)

Use Case: Creating a Computer Object Manually

Scenario:

A user wants to create a new computer object.

Pre-Condition:

The user is a member of one or more security profiles.

Action:

The user creates the new computer object using the DSM Explorer or the DSM command line utility.

Post-Conditions:

- The new computer object is created.
- The area_ace is derived from the security profile and is assigned to the computer object. If the user is a member of more than one security profile, the area_ace of all relevant security profiles are OR'ed and assigned to the secured object.

Use Case: A New DSM Agent Was Detected

Scenario:

A DSM agent was deployed and runs the very first time.

Pre-Condition:

There is no object in the MDB for the new asset.

Action:

No user action. The DSM engine detects the new agent and creates the asset object (inserts into ca_discovered_hardware).

Post-Conditions:

- A new secured object is created.
- The area permissions are assigned as defined on a global level (global configuration parameter).

Use Cases: Asset Groups

The following important user scenarios regarding asset groups are considered in the context of security area support:

- Creating an asset group (see page 543)
- Add a computer to an asset group (see page 544)
- Remove a computer from an asset group (see page 545)
- Changing area permission of an asset group (see page 546)
- Disabling Inheritance and reverting (see page 546)

Use Case: Creating an Asset Group

Scenario:

A user wants to create a new asset group where the user is member of only one security profile.

Pre-Condition:

A group with the same name does not already exist.

Action:

The user creates the new asset group.

Post-Conditions:

- The new group is created.
- A group_ace is created based on the class level permissions for groups.
- An object_ace is created based on the class level permissions for the groups.
- The area_ace is picked up from the security profile where the creation user belongs to. If the creation user is unknown the default area_ace is assigned.

Note: The same is valid for scalability server groups and domain groups.

Use Case: Add a Computer to an Asset Group

Scenario:

A user wants to add a computer to the group where the user is member of only one security profile.

Pre-Conditions:

- The asset group exists.
- The computer exists.

Action:

The user adds a computer to a group; inheritance is enabled for the group.

Post-Conditions:

- The computer is linked to the group.
- If it is not an inheritance group, then nothing is done. If it is an inheritance group, then the object_ace is calculated based on the object_ace of the parent group.
- The area-code is set as follows:
  - If the computer is only a member of only one asset group, the area_ace is the same as the area_ace of the asset group.
  - If the computer is a member of multiple asset groups, the area_aces of the parent groups are OR'ed and assigned to the secured object.

Variants:

If the area permission of the computer is set to creation_user level or global default level before adding to the group, then the area permission is set to the area permissions of the group.

If the area permission of the computer is set to object_level before adding to the group, then the area permissions are not set to group level. The user must use the REVERT function to re-calculate the area permissions to conform to the group.

Area permissions must not change if a permission inheritance is disabled.

Note: The same is valid in case of a dynamic group and the engine doing the group evaluation. In this case the engine links the member to the group.

Use Case: Remove a Computer from an Asset Group

Scenario:

A user wants to remove a computer from an asset group where the user is member of one or more security profiles.

Pre-Conditions:

- The asset group exists.
- The computer exists.
- The computer is member of only one asset group.

Action:

The user unlinks the computer from the asset group; inheritance is enabled for the group.

Post-Conditions:

- The computer is unlinked from the group.
- Area permissions are not updated.
- The security level is set to object level.

Variants:

If the computer is member of more than one asset group and the security level is set on group level, then the area permissions are calculated again (based on the remaining group assignment) and updated.

If the area permission is set on object level the area permission is not updated.

Note: After removing the computer from the asset group the user can use the REVERT function to bring the area permissions of the computer to the creation user level.

Use Case: Changing Area Permission of an Asset Group

Scenario:

A user wants to change the area permissions of an existing asset group.

Pre-Conditions:

- The user is linked to one or more security profiles.
- The asset group exists where permission inheritance is enabled.

Action:

The user uses the Change Permission dialog and links and unlinks one or more areas to the existing group.

Post-Conditions:

- The area_ace of the existing group is changed.
- If it is an inheritance group, the area_ace of the members are updated.

Note: Enabling and disabling permission inheritance does not modify the area permissions.

Use Case: Disabling Inheritance and Reverting

Scenario:

A user wants to disable the inheritance of an asset group and perform a reverting on asset level.

Pre-Conditions:

- An asset group exists where permission inheritance is enabled.
- A computer is linked to the asset group where area permissions are set to object level at link time.

Action:

The user sets permission inheritance of the asset group to disabled and performs a "revert" for the computer object.

Post-Condition:

The object permissions of the computer are reverted to creation user.

Note: Enabling and disabling permission inheritance does not modify the area permissions.

Use Cases: Queries

The following important user scenarios regarding queries are considered in the context of security area support:

- Creating a query (see page 547)
- Running a query (see page 548)
- Running a query in context of Software Delivery (see page 548)

Use Case: Creating a Query

Scenario:

A user wants to create a new query.

Pre-Condition:

The user is member of only one security profile.

Action:

The user creates the new query.

Post-Conditions:

- The new query is created.
- The area_ace of the query is derived from the profile of the creation user of the query.
- The new query includes an additional 'where' condition to make sure the query returns only objects where the creation user has access (same area_ace as assigned to the query itself).
- The object_ace is created based on the class level ace of the security class for queries.

Use Case: Running a Query

Scenario:

A user wants to create a dynamic computer group; the group needs to be evaluated by the engine.

Pre-Condition:

None.

Action:

A user creates a dynamic group; parent group is 'All Computers'.

The user who created the query is different from the user who creates the group.

Post-Conditions:

The evaluation of the group is done by the engine based on the following rules:

- The query is executed.
- Add only those computers as group members that fall in the same area as the user who created the group.

This means that the group area permissions have a higher priority than the area permissions of the group.

Use Case: Running a Query in Context of Software Delivery

Scenario:

A query is evaluated as part of a Software Delivery procedure prerequisite. The evaluation is done by the Task Manager of Software Delivery.

Pre-Condition:

A procedure with a prerequisite is used for installation on a target computer and the global area setting is turned on.

Action:

The Task Manager calls the query evaluation API, passing in the user from the Software Delivery activity object.

Post-Condition:

The query is evaluated in the same context as the user who created the job in the GUI. This means that the query returns only objects in the same area as the user who created the job. If the job was created by a background process where no user context was available then the query evaluation will return all objects as if area support was not enabled.

Use Cases: Software Packages

The following important user scenario regarding software packages is considered in the context of security area support:

- Creating a software package (see page 549)

Use Case: Creating a Software Package

Scenario:

A user wants to create a new software package.

Pre-Condition:

The software package did not exist.

Action:

The user creates the software package using the CA ITCM GUI.

Post-Conditions:

- The software package is created.
- Area permissions are created and the software package is linked to the same areas as the user who created the object.

Use Cases: Software Procedures

The following important user scenario regarding software procedures is considered in the context of security area support:

- Creating a software procedure (see page 549)

Use Case: Creating a Software Procedure

Scenario:

A user wants to create a new software procedure.

Pre-Condition:

The software procedure did not exist.

Action:

The user creates the software procedure using the CA ITCM GUI.

Post-Condition:

The procedure “inherits” the same area permissions as the software package it is included in.

Use Cases: Software Groups

The following important user scenario regarding software groups is considered in the context of security area support:

- Creating a software group (see page 550)

Use Case: Creating a Software Group

Scenario:

A user wants to create a new software group.

Pre-Condition:

The user is a member of one or more security profiles.

Action:

The user creates the new software group using the DSM Explorer (a new node below Software Package Library).

Post-Conditions:

- The new software group is created.
- The area_ace of the software group is derived from the profile of the creation user of the query.
- The objects_ace is created based on the class level ace of the security class for asset jobs.
- A group_ace is also created based on the class level ace of the security profile.

Use Cases: Software Policies

The following important user scenario regarding software policies is considered in the context of security area support:

- Creating a software policy (see page 551)

Use Case: Creating a Software Policy

Scenario:

A user wants to create a new software policy.

Pre-Condition:

The user is a member of one or more security profiles.

Action:

The user creates the new software policy using the DSM Explorer or the CA ITCM command line.

Post-Conditions:

- The new software policy is created.
- The software policy is assigned to an Asset Group.
- The object_ace is derived from the class select ace.
- The area permissions of the software policy are derived from the profile of the creation user of the policy.

Use Cases: Software Jobs

The following important user scenario regarding software jobs is considered in the context of security area support:

- Creating a software job (see page 551)

Use Case: Creating a Software Job

Scenario:

A user wants to create a new software job.

Pre-Condition:

The user is a member of one or more security profiles.

Action:

The user creates the new software job using the DSM Explorer or the DSM command line.

Post-Conditions:

- The new software job is created.
- Object permissions are derived from the class select ace
- The area permissions of the software job are derived from the profile of the creation user of the job.

Use Cases: Asset Jobs

The following important user scenario regarding asset jobs is considered in the context of security area support:

- Creating an asset job (see page 552)

Use Case: Creating an Asset Job

Scenario:

A user wants to create a new asset job.

Pre-Condition:

The user is a member of only one security profile.

Action:

The user creates the new asset job. The asset job can be of any job type like messages, command, and so on.

Post-Conditions:

- The new asset job is created.
- The area_ace of the asset job is derived from the profile of the creation user of the query.
- The objects_ace is created based on the class level ace of the security class for asset jobs.

Use Cases: Engine Tasks

The following important user scenario regarding engine tasks is considered in the context of security area support:

- Creating an engine task (see page 553)

Use Case: Creating an Engine Task

Scenario:

A user wants to create a new engine task.

Pre-Condition:

The user is a member of only one security profile.

Action:

The user creates the new engine task.

Post-Conditions:

- The new engine task is created.
- The area permission of the engine task is derived from the profile of the creation user of the engine task.
- The objects permissions are created based on the class level permission of the security class for asset jobs.

Use Cases: Managing Areas

The following important user scenarios regarding managing areas are considered in the context of security area support:

- First time enabling area code support (see page 554)
- Disabling area code support (see page 554)
- Re-enabling area code support (see page 555)
- Changing the default area permissions (see page 555)
- Adding a new area (see page 556)
- Deleting an area (see page 556)

Use Case: First Time Enabling Area Code Support

Scenario:

An administrator wants to enable the area code for all security profiles and it was disabled in the past.

Pre-Conditions:

- The area code support is disabled and the CA ITCM product has been used already.
- Secured objects and profiles were created while area support was disabled.

Action:

The administrator enables the area code support.

Post-Conditions:

- The area code support is enabled in the MDB.
- The area codes of all profiles are set to default area code as defined when the security profile was created.
- The area codes for the existing secured objects are set to the area codes as defined for the security profile.

Note: This means that an administrator must assign one or more area codes to the security profile explicitly after the first time enabling area code support.

Use Case: Disabling Area Code Support

Scenario:

An administrator wants to disable the area codes for all security profiles.

Pre-Condition:

The area codes are set correct in the MDB.

Action:

The administrator disables the area code support.

Post-Conditions:

- The flag in the MDB is set to disable the area code.
- The area code itself is neither deleted nor changed.

Use Case: Re-enabling Area Code Support

Scenario:

An administrator wants to enable the area code for all security profiles again.

Pre-Condition:

The area codes are set correct in the MDB but the area code support is set to DISABLED.

Action:

The administrator enables the area code support.

Post-Conditions:

- The flag in the MDB is set to enable the area code..
- The area code itself is the same as before the area code support was disabled.

Use Case: Changing the Default Area Permissions

Scenario:

A user wants to change the default area permissions.

Pre-Condition:

The user has CA ITCM installed.

Action:

The user changes the default permissions.

Post-Conditions:

- The default area permissions as stored in the MDB are changed.
- All area permissions where the security level is set to 'default value' are also changed.

Use Case: Adding a New Area

Scenario:

A user wants to create a new area definition.

Pre-Condition:

The user is member of a security profile. The security class to control area support (SEC_CLSID_COM_CONTROL_AREA) allows at least creating a new area.

Action:

The user creates the new area definition.

Post-Condition:

The new area is created.

Use Case: Deleting an Area

Scenario:

A user wants to delete an area definition.

Pre-Condition:

The user is member of a security profile. The security class to control area support (SEC_CLSID_COM_CONTROL_AREA) allows at least deleting an area.

Action:

The user deletes the area definition manually.

Post-Conditions:

- The area is deleted.
- Area permissions are updated that the area does no longer exist.

Use Case: Take Ownership

Take ownership will not change the area permission of any object.

Appendix F: CAF Scheduled Jobs

The complete rules for specifying scheduled jobs that run in the common application framework (CAF) are described following. These jobs cover the running of caf commands at regular or random intervals. For example, there is a standard job which runs the Asset Management agent once a day.

This section contains the following topics:

CAF Standard Jobs and Parameters

CAF is installed with a collection of standard jobs (see CAF Policy Group in the Configuration Policy section of the *DSM Explorer Help* for details).

A job is described by a set of parameters stored in the configuration store (comstore) under the key:

`itrm/common/caf/scheduler/`*`name_of_job`*

The scheduler itself can be enabled or disabled by setting the “enabled” parameter in the above key.

The parameters of a job are as follows:

desc

Defines the job description; this appears in trace logs.

enabled

Indicates whether a job is enabled. Valid values are: 1=job is enabled, 0=job is not enabled and will not run.

type

Specifies the type of job. This determines the time frame in which the job repeats and can be one of these values:

day

Runs the job every few days at a given hour and minute.

hour

Runs the job every few hours at a given minute of the hour.

minute

Runs the job every few minutes.

You can also specify these additional keywords:

now

Executes the job now and at the scheduled intervals thereafter. The word “now” in this context means “when caf starts up”.

If the randomnowtime parameter is set, the job executes within a random number of seconds up to the value of randomnowtime. This is used to ensure that computers that start up together do not all fire their jobs at the same time.

random

Executes the job at the specified time plus a random number of minutes up to the value of the randomminutes parameter. This is used in jobs which involve contacting servers. This helps to spread the load on servers by partially randomizing the time at which agents make contact.

random_hour

Specifies running the job at a random hour within the day. Used with daily schedules.

random_minute

Specifies running the job at a random minute within the hour (which may also be random). Used with daily and hourly schedules.

excludeDays

Specifies the names of the days to be excluded from the schedule: monday, tuesday, and so on. Separate each day by spaces. For example, the setting “monday wednesday” prevents the job from running on Monday and Wednesday.

excludeHours

Specifies the numbers of the hours to be excluded from schedule using a 24-hour clock. Separate each hour by spaces. For example, the setting “1 15” prevents the job from running at 1:00 a.m. and 3:00 p.m.

hour

Specifies the hour at which the job starts using the 24-hour clock. This is used with daily schedules only.

minute

Specifies the minute in the hour at which the job starts. This is used with daily and hourly schedules.

repeat

Repeats every time unit defined by the “type” property. For example, if type is “hour” then “repeat” specifies the number of hours between jobs.

randomnowtime

Specifies a number of seconds. When CAF starts up, a job marked as “now” will run at a random time within this number of seconds.

randomminutes

Specifies a number of minutes. The job runs at the specified time plus a random time up to the value of this parameter.

cmd

Specifies the caf command for executing this job. This is the same as the command line with the exception that the host, user, and password options cannot be used.

CAF Scheduled Jobs Examples

Example: Run the amagent plugin every hour on the hour

```
type=”hour”, repeat=1, minute=0, cmd=”start amagent”
```

Example: Run the amagent every day at 2:30 p.m.

```
type=”day”, repeat=1, hour=14, minute=30, cmd=” start amagent”
```

Example: Run the amagent when CAF starts up and thereafter every day at a random time between 1:00 a.m. and 2:30 a.m. except on a weekend

```
type=”day now random”, hour=1, minute=0, randomminutes=90, excludedays=”saturday
sunday”, cmd=” start amagent”
```

Appendix G: FIPS 140-2 Compliance

This appendix details the use of cryptography in CA ITCM, especially the compliance level with the FIPS 140-2 publication standards.

This section contains the following topics:

FIPS PUB 140-2

The FIPS 140-2 is a security standard that specifies the security requirements for a cryptographic module used within a security system. It is a standard provided by NIST to evaluate and accredit the operation of cryptographic modules through the Cryptographic Module Verification Program (CMVP). The CMVP is run by NIST-approved test laboratories to test and validate cryptographic modules. The modules are tested against the derived test requirements of the FIPS 140-2 standard.

For each security function that is validated and approved for use in FIPS 140-2 accredited mode, an individual certificate under the Cryptographic Algorithm Validation Program (CAVP) is recorded in the FIPS 140-2 approval certificate for the module. The approval certificate lists all security functions that the module provides—both approved and non-approved, and details the functions that can be used in the FIPS 140-2 approved mode of operation.

Each approved module publishes an associated security policy document that details how the module must be operated in order to be compliant with the FIPS 140-2 standard.

Note: Only cryptographic modules can be certified as FIPS 140-2 accredited and approved; applications cannot be, though they can use FIPS 140-2 approved modules in their approved modes of operation.

References

For more information about Cryptographic Module Verification Program, go to the NIST website:

http://csrc.nist.gov/groups/STM/cmvp/

You can view the validated modules at the following URL along with links to their relevant security policies:

http://csrc.nist.gov/groups/STM/cmvp/validation.html

You can find information related to the certificate numbers referenced in this appendix in the above URL.

Supported FIPS Modes

CA ITCM can operate in one of the following modes:

FIPS-Preferred

In FIPS-preferred mode, CA ITCM prefers to use FIPS 140-2 approved security functions; however, when it communicates with legacy CA ITCM components it uses legacy security functions. In this mode, the embedded cryptographic modules are *not* operated in FIPS 140-2 accredited modes as they require the use of non-approved security functions, such as MD5. When operating in FIPS-preferred mode CA ITCM can communicate and interoperate with the previous releases of CA ITCM.

FIPS-Only

In FIPS-only mode, CA ITCM uses *only* FIPS 140-2 approved security functions. There is some non-cryptographic use of non-approved security functions, as detailed in the sections below, but these are not provided by any embedded cryptographic module when in a FIPS 140-2 approved mode of operation. In this mode, CA ITCM can only interoperate with the components that are FIPS-compliant, either in FIPS-preferred or FIPS-only mode.

Note: This appendix focuses on the cryptographic use when CA ITCM is operating in FIPS-only mode.

Cryptographic Module – RSA Crypto

CA ITCM directly uses and embeds the following cryptographic modules:

- RSA Crypto-C ME Version 2.1; CMVP certificate #828

Following is the extract from the security policy of this cryptographic module:

"This Cryptographic Module is classified as a multi-chip standalone module for FIPS 140-2 purposes. As such, the module must be tested upon a particular operating system and computer platform. The cryptographic boundary thus includes the Cryptographic Module running on selected platforms running selected operating systems while configured in "single user" mode. The Cryptographic Module was validated as meeting all FIPS 140-2 level 1 security requirements, including cryptographic key management and operating system requirements. The Cryptographic Module is packaged as a dynamically loaded module or shared library file which contains all the module's executable code. Additionally, the RSA BSAFE Crypto-C ME toolkit relies on the physical security provided by the host PC in which it runs."

Cryptographic Security Functions

The following table provides the cryptographic algorithms from the RSA Crypto-C module that CA ITCM uses for various security functions:

Security Function	Crypto Algorithm	Validation Certificate Number	Comments
Asymmetric encryption and decryption	RSA encrypt or decrypt	Non-approved	Allowed in FIPS 140-2 mode for key transport
Symmetric encryption and decryption	AES CBC	490	FIPS PUB 197 – Advanced Encryption Standard
	Triple-DES	510	FIPS PUB 46-3 - Data Encryption Standards FIPS SP 800-67 - Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher ANSI X9.52 – TDEA approved modes of operation
Hash Functions	SHA-1	560	FIPS PUB 180-3 – Secure Hash Standard
	SHA-256	560	FIPS PUB 180-3 – Secure Hash Standard

Security Function	Crypto Algorithm	Validation Certificate Number	Comments
	SHA-512	560	FIPS PUB 180-3 – Secure Hash Standard
Random Number Generation	PRNG	270	FIPS PUB 186-2 – Digital Signature Standard For more information, see Appendix 3: Random Number Generation For The DSA in the FIPS PUB 186-2 Digital Signature Standard document.
Asymmetric Key Establishment	TLS 1.0	Not Applicable	Allowed by the FIPS 140-2 Implementation Guidance document with FIPS approved cipher suites
	SSH v2	Not Applicable	Allowed by the FIPS 140-2 Implementation Guidance document with FIPS approved cipher suites

Component-Specific Cryptographic Use

This section lists the component-specific cryptographic usage when CA ITCM is operating in the FIPS-only mode:

Inter-node Communications [Session Messaging]

The session messaging component uses the TLS v1.0 protocol for inter-node communications. The chosen cipher suite will be selected by negotiation between the communicating nodes.

In some instances, the session messaging component uses the Key Transport Recipient Information structure as specified in the Cryptographic Message Syntax version 3 (CMS3) as specified in RFC3369.

Stream-based Networking

The stream-based networking component utilizes the TLS v1.0 protocol for inter-node communications. The chosen cipher suite will be selected by negotiation between the communicating nodes.

Remote Control – Local Address Book

The remote control Local Address Book entries are protected by the 3TDES algorithm in CBC mode with randomized IV.

Desktop Migration Manager [DMM]

DMM uses the TLS v1.0 protocol for communication and the AES algorithm with 192 bit keys in CBC mode with randomized IV.

ENC

As the ENC functionality provided in CA ITCM is currently Windows only, it is tightly integrated with the Microsoft SCHANNEL provider; the Microsoft Certificate Store, and therefore the underlying Microsoft Cryptographic provider (RSAENH). For more information about the FIPS status of the Microsoft cryptographic providers, see FIPS-certified Windows Operating Environments (see page 567).

OSIM and Software Delivery

OSIM and software delivery use symmetric encryption provided by the AES algorithm in CBC mode with randomized IV and structured using the Cryptographic Message Syntax version 3 (CMS3) as specified in RFC3369.

Common Object Manager, Common Engine, SMS Extractor

The Common Object Manager, Common Engine, and SMS Extractor components use the 3TDES algorithm in CBC mode with randomized IV.

Platform Virtualization – ESX Module

The ESX module uses the TLS v1.0 protocol for communication with remote VMware ESX nodes.

DTS

The DTS programs use symmetric encryption provided by either the AES or 3TDES algorithms, with varying key sizes, but all using CBC mode with randomized IVs.

CCS

CA ITCM can make use of CA Common Services, which can optionally be installed. For a detailed description of the FIPS compliance level of CA Common Services, review "Appendix B FIPS 140-2 Encryption" of the *CA NSM Administration Guide* provided in the CA Bookshelf.

FIPS-Compliance of Components External to CA ITCM

There are many other uses of cryptography within a machine, external to the CA ITCM applications.

Windows Operating Environments

The Microsoft Enhanced Cryptographic Service Provider [RSAENH CSP] is FIPS-140 certified on various Windows operating environments. For a list of these FIPS-certified operating environments, see http://technet.microsoft.com/en-us/library/cc750357.aspx. This link also details how to enable the local security policy to use FIPS-compliant cryptography. You must configure the local security policy (System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing) for ENC to be FIPS-compliant.

Note: You must carefully consider the impact of operating in FIPS-only mode of operation that is, allowing only FIPS-compliant encryption. For more information, see FIPS 140-2 Support (see page 75).

SQL Server

Microsoft SQL Server, from version 2005 SP1, is FIPS-compliant. For more information about how to configure SQL Server to operate in FIPS-compliant mode, see Microsoft Knowledge Base entry 920955 in http://support.microsoft.com/kb/.

Other Components

CA ITCM is a suite of applications and component modules that provides a business solution. As a software package, CA ITCM also utilizes components and services from other CA groups and third-party providers. Unless otherwise mentioned, none of these components and/or services implement or expose cryptographic capabilities directly to CA ITCM and, therefore, their compliance with FIPS 140-2 certified cryptographic modules is not documented. Refer to supporting documentation from the component providers for any FIPS 140-2 related information.

Additionally, cryptographic operations within operating systems is within the remit of the operating system vendors. Refer to any FIPS 140-2 related documentation from the vendors for FIPS 140 and Common Criteria support, including level of compliance and/or any supported configuration required.

Note: For the most up-to-date list of components shipped with CA ITCM, see compatibility matrix.

Non-approved Use of Security Functions

In some cases, CA ITCM makes use of security functions that are not allowed by the FIPS 140-2 publication. These do not impact the 'normal' operation of CA ITCM in the FIPS-only mode.

Asset Management Agent – Software Signature Scanner

When a software signature contains an "md5" attribute value for a <file> tag, the signature scanner uses a private implementation of MD5 code. The scanner checks whether the MD5 digest of any file found on the agent computer matches the "md5" attribute before it returns a positive result for that signature. MD5 is not used for any cryptographic purposes in the software signature scanner.

Installation

During CA ITCM installation, PKCS#12-based files can be used for certificate and key installation. These files are encrypted using a key derived in a password-based key derivation function (PBKD), such as PBKDF2 from the PKCS#5 v2.0 standard. During installation, these files are extracted and protected using non password-based techniques.

Note: Password-based key derivation (password based key establishment) is explicitly disallowed for the purposes of asymmetric key agreement as specified in section 7.1 of the FIPS 140-2 Implementation Guidance document.

Glossary

application

An *application* is a piece of software, for example, Microsoft Word.

application virtualization

Application virtualization is the encapsulation of an application, separating it from the underlying operating system on which it is executed. At runtime the application is tricked into acting as if it were directly interfacing with the original operating system and all the resources managed by it, but in reality it is not.

centrally managed environment

A *centrally managed environment* is one where the remote control domain manager controls the host settings through computer policies, global address book (GAB) items, licensing of the host agent on the domain, and user permissions. This is the default setting for CA IT Client Manager.

centrally managed host environment

A *centrally managed host environment* is one where either a remote control enterprise or domain manager is responsible for the configuration of the hosts and the authentication of viewer connections. It also manages the address book that users use to find hosts.

Common Configuration Enumeration (CCE)

Common Configuration Enumeration (CCE) is one of the SCAP standards. It contains Standard identifiers and dictionary for system configuration issues related to security. A rule definition in an SCAP data stream can contain references to one or more CCE identifiers, indicating that the rule is a representation of a specific CCE configuration guidance statement or configuration control. For more information, go to http://cce.mitre.org/.

Common Platform Enumeration (CPE)

Common Platform Enumeration (CPE) is one of the SCAP standards. It contains standard identifiers and dictionary for platform or product naming. For example, some elements in XCCDF files can be restricted to only apply to certain platforms and this is done using CPE identifiers. For more information, go to http://cpe.mitre.org/.

Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) is a dictionary of common names (that is, CVE Identifiers) for publicly known information security vulnerabilities. These identifiers make it easier to share data across separate network security databases and tools. CVE is one of the components used in SCAP. See http://cve.mitre.org/ for details.

Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) is one of the SCAP standards. It contains standards for conveying and scoring the impact of vulnerabilities. For more information, go to http://www.first.org/cvss/index.html.

configuration view

A *configuration view* is a customized Windows-only user interface that lets you edit configuration policies that are related to specific components or functionality. Configuration views summarize the relevant policies for a component or function independent of where they are actually located in the hierarchy and the DSM Explorer tree.

connectors

connectors are the links from products that consume connector data to external products, or *domain managers*. Each connector retrieves information from its domain manager and transmits the information through the connector framework to the consuming product for visualization and analysis. Connectors can also enact inbound operations on data in the source domain manager, such as object creation. connectors use a unified connector framework to enable integration with multiple consuming products.

desktop recompose

Desktop recompose is the process of assigning a new golden template to the virtual desktop. Operating systems and applications have to be maintained during their lifetime to fix problems resolved by hot fixes or service packs or to provide new features by new versions. For linked clones, this means the master image, or golden template, has to be updated. Once the updates are completed, the linked clone is recomposed and becomes active. During the recompose operation the related linked clones are linked to this new golden template and are refreshed.

desktop refresh

Desktop refresh is the process of resetting the virtual desktop to its original state. Linked clones track changes to the virtual machine with the clone. To control the storage allocations with the clone, VMware View offers the refresh operation that resets the clone to its baseline and releases all deltas provided for tracking changes. This means that all information stored to the system drive since the creation of clone or its last refresh or recompose is lost. Unlike desktop recompose, the same golden template continues to be used as before the refresh operation.

eXtensible Configuration Checklist Description Format (XCCDF)

eXtensible Configuration Checklist Description Format (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target computers. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. For more information, go to http://nvd.nist.gov/xccdf.cfm.

Federal Information Processing Standard (FIPS)

Federal Information Processing Standard (FIPS) is a security standard that is issued and approved by NIST. It specifies the security requirements that must be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information.

FIPS-certified cryptography module

FIPS-certified cryptography module refer to RSA CryptoC BSAFE module, which is FIPS 140-2 certified.

FIPS-Compliant Cryptography

FIPS-compliant cryptography refers to the use of FIPS 140-2 certified modules, FIPS-approved, and FIPS-allowed techniques and algorithms for cryptography.

FIPS-only

FIPS-only is a mode of operation for CA ITCM wherein only FIPS-compliant cryptography is allowed. In this mode, CA ITCM is not backward compatible with the previous releases of CA ITCM.

FIPS-preferred

FIPS-preferred is a mode of operation for CA ITCM wherein bulk of cryptographic operations are FIPS-compliant, leaving few encryptions in legacy format. In this mode, CA ITCM is backward-compatible with the previous releases of CA ITCM.

golden template

In CA ITCM terminology, the *golden template* is the virtual machine from which virtual desktops are cloned.

guest

A *guest* in generic platform virtualization terminology is the virtual machine and the guest operating system.

guest operating system

The *guest operating system* is the operating system running inside a virtual machine.

health monitoring

Health Monitoring (HM) functionality lets you configure alerts, set threshold values, and monitor the overall health of the CA ITCM infrastructure.

host

A *host* in generic platform virtualization terminology is the physical machine, the host operating system, and the hypervisor.

host cluster

The *host cluster* is the aggregate computing and memory resources of a group of hosts sharing some or all of the same network and storage.

host operating system

The *host operating system* is the operating system running on a physical machine.

hosted virtual environment

A *hosted virtual environment* is the virtualization software that runs on top of a host operating system, that is, the physical machine, host OS, and the hypervisor.

hypervisor

The *hypervisor* is the virtualization software layer simulating physical hardware on behalf of the guest operating system. This term is synonymous with Virtual Machine Monitor (VMM).

instance software state database

The *instance software state database* is a part of the software state database that contains the history of all software jobs executed by the agent running on a non-golden template system, that is, any clones of the golden template.

linked clones

In VMware View, *linked clones* of a master or golden image only refer to the master or golden image but do not include it. Changes to the system during user sessions are not stored to the master image but are kept in delta files with the clone.

location awareness

Location Awareness lets DSM Agent on a computer detect the location of the computer.

master target device

In Citrix XenDesktop, a *master target device* is the base desktop with the OS and required set of applications from which a vDisk is generated.

master vDisk

In Citrix XenDesktop, a *master vDisk* is the initial vDisk generated from the golden template machine.

MITRE

The *MITRE Corporation* is a not-for-profit organization chartered to work in the public interest. MITRE offers the interpreters, source code, schemas, and data files at no cost so that individuals and organizations can build and expand upon them. Ovaldi is one such interpreter that is freely available.

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. The United States (U.S.) National Vulnerability Database (NVD), operated by the NIST, provides a repository and data feeds of content that utilize the SCAP standards. It is also the repository for certain official SCAP standards data. Thus, NIST defines open standards within the SCAP context and defines the mappings between the SCAP enumeration standards.

native virtual environment

A *native virtual environment* is the virtualization software that runs directly on the physical machine, becoming or acting as a host operating system (often minimal), that is, the physical machine and the hypervisor. A synonymous term is "bare metal environment."

non-linked clones

In VMware View, *non-linked clones,* or full clones, are full copies of a master or golden image. The clone includes a copy of the image and all changes to the system during user sessions are stored to this copy.

nonpersistent clones

Nonpersistent clones are virtual desktops from the nonpersistent pool of VMware View user data that are transient out-of-the-box. Once a user logs off, the clone is refreshed and all user data at the system disk are lost.

nonpersistent linked clone virtual desktop

A *nonpersistent linked clone virtual desktop* is a virtual machine that is refreshed or recomposed every time the user logs on, with no persistence for custom installed applications, personalization, and so on.

offline patching

Offline Patching lets you export the patch content and patch files remotely and import to the CA ITCM environment using CA Patch Manager without accessing Internet.

Offline RAC

Offline RAC is a reinstall after crash (RAC) task that is driven by the agent rather than by the manager. Virtual desktops are *recomposed* frequently, that is, whenever the golden template is updated and the disk is reset, any changes to the virtual desktop since the previous reset are effectively voided. For virtual desktops, the agent and not the manager is responsible for the creation of the RAC job container. When the disk reset occurs, the agent initiates an Offline RAC to restore any software that has been deployed to the agent.

Open Vulnerability and Assessment Language (OVAL)

Open Vulnerability and Assessment Language (OVAL) is one of the SCAP standards. It contains standard XML for testing procedures for security related software flaws, configuration issues, and patches as well as for reporting the results of the tests. All the rule checks in the checklists take the form of references to OVAL definitions contained in OVAL files from the SCAP data stream. For more information, go to http://oval.mitre.org/.

Ovaldi

Ovaldi is an OVAL Interpreter developed by the MITRE Corporation. It is a freely available reference implementation created to show how information can be collected from a computer for testing to evaluate and carry out the OVAL definitions for that platform, and to report the results of the tests. The interpreter demonstrates the usability of OVAL Definitions and ensures correct syntax and adherence to the OVAL Schemas.

package format

The *package format* is a property of a software package. Formats include regular and virtual.

package type

The *package type* is a property of a software package. Current types include Generic, MSI, SXP, PIF, and PKG. Package type is not used or altered for the purpose of supporting virtual application packages.

partition

A *partition* is an isolated instance of a host operating system. Partitions do not usually use guest operating systems because they all share the host's operating system.

partitioned virtual environment

A *partitioned virtual environment* is one where multiple instances of the host operating system can run in isolation on the same physical machine. This is not strictly a virtualization technology, but is used to solve the same type of problems.

persistent clones

Persistent clones are virtual desktops from the persistent pool that survive as they are after the user has logged off until they are refreshed or recomposed. VMware View offers out-of the box separate devices for system and user data with the persistent clones. Information stored to the user data device survives any refresh or recompose action while changes to the system disk are lost.

persistent linked clone virtual desktop

A *persistent linked clone virtual desktop* is a virtual machine that is dedicated to a specific user, and the user can request specific software to be added, customize settings, and so on. At each logon the user's customized environment is restored. This persists until the virtual desktop is refreshed or recomposed. At that point, all the software products installed on system drive are lost.

persistent non-linked clone virtual desktop

A *persistent non-linked clone virtual desktop* is a virtual machine that is dedicated to a specific user and is presented to that user at each logon with their custom installed applications, user settings, data, and so on.

platform virtualization

Platform virtualization is the encapsulation of computers or operating systems, hiding their physical characteristics from users and emulating the computing platform at runtime.

provisioned application

A *provisioned application* is an application (regular or virtual) that has been made available for execution on a target computer. The application need not be "installed" locally in order to treat it as provisioned.

regular application

A *regular application* is application software that has not been virtualized and can be installed and executed in a traditional fashion. When talking about releases, patches, and suites, regular applications are implied.

Replication

Replication is an engine task to perform the data replication from Domain Manager to Enterprise Manager and Enterprise Manager to Domain Manager.

sandbox

A sandbox is an application runtime environment that isolates the application from the computer's operating system and resources and also from other applications on the computer. The degree of isolation is usually set to allow the application some access to the operating system resources, such as the documents folder.

scalability server

A *scalability server* is the central server to enable geographical scalability for management tasks. It is a distributed process that is the primary interface for agents.

SCAP data stream

SCAP data stream consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations. An SCAP data stream consists of the XML following files:

- An XCCDF file
- One or more OVAL files
- (Optional) A CPE dictionary file

schema map

A *schema map* is a mapping of the attribute names associated with data objects, such as users, computers, and groups, used in an external directory to those attribute names used by corresponding CA ITCM objects. The fixed and standard set of DSM attribute names is used for querying directories and for formulating complex queries and reports.

Security Content Automation Protocol (SCAP)

The *Security Content Automation Protocol (SCAP)*, pronounced "S Cap", is a method for using the standards such as XCCDF, CCE, CVE, CVSS, CPE, and OVAL to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). More specifically, SCAP is a suite of selected open standards that enumerate software flaws, security related configuration issues, and product names; measure systems to determine the presence of vulnerabilities; and provide mechanisms to rank (score) the results of these measurements in order to evaluate the impact of the discovered security issues. SCAP defines how these standards are combined. The National Vulnerability Database provides a repository and data feeds of content that use the SCAP standards. For more information, go to http://nvd.nist.gov/.

software signature

A *software signature* defines the attributes of a software application, such as the main executable file name, other associated files, size range, version range, creation, and modification dates of the software. All these attributes of a software signature uniquely identify a software application. Software signatures in asset management are created as software definitions. You can create software definitions for a product, release, patch, suite, suite component, or virtual application image. By default, asset management provides predefined software signatures covering the most widely used software in the IT industry.

software type

The *software type* is a property of a software definition. Current types include suite, product, release, patch, and virtual application image.

staged virtual application image

A *staged virtual application image* is a virtual application image that has been discovered in the file system of a computer.

stand-alone environment

A *stand-alone environment* is one where the users of the host and viewer computers locally manage all settings, properties, and licensing of the CA ITCM remote control component. It is set by a Standalone Agent installation. To install it manually, the RC agent setup needs to be called directly.

standalone virtual application

A *standalone virtual application* is a virtual application that has been provisioned in a way where the virtual application image used as the source resides on the system to which it has been provisioned.

streamed virtual application

A *streamed virtual application* is a virtual application that has been provisioned in a way where the virtual application image used as the source resides on a remote system that is different from the system to which it has been provisioned.

streamed virtual application image

A *streamed virtual application image* is a virtual application image that has been discovered to be accessible through the network from a computer. Discovery of streamed virtual application images will usually only be possible if the virtual applications residing inside of the image have been provisioned.

vDisk

In Citrix XenDesktop, a *vDisk*, or virtual disk, is basically an image file with the OS and the required set of applications.

virtual application (VA)

A *virtual applicatio*n is software that has been virtualized.

virtual application image

A *virtual application image* contains one or more virtual applications stored inside a file, possibly with a set of supporting metadata files.

virtual application image definition

A *virtual application image definition* describes the "footprint" for discovering a virtual application image. To discover an image containing one or more included virtual applications (stored inside), regular software signatures must be associated with the virtual application image definition.

virtual application package (VAP)

A virtual application image packaged inside of one or more software delivery packages is referred to as a v*irtual application package*. These packages are used to provision computers with virtual applications.

virtual application staging package

A *virtual application staging package* is a virtual application package used to stage the virtual application image.

virtual application standalone package

A *virtual application standalone package* is a virtual application package used to provision a virtual application in standalone mode.

virtual application streaming package

A *virtual application streaming package* is a virtual application package used to provision a virtual application in streaming mode.

virtual disk

A *virtual disk* is a set of files that forms a file system that appears as a physical disk to the guest operating system.

virtual image

A *virtual image* is a file or set of of files containing the complete definition of a virtual machine, including its hardware specifications and virtual disks. It is the host's file system representation of a guest. A virtual image can be online or offline depending on the running state of the virtual machine it captures.

virtual machine (VM)

A *virtual machine* is an isolated virtualized environment simulating a physical machine. The virtual machine does by definition not include the guest operating system.

virtual patch

A *virtual patch* is the virtual equivalent of a regular patch and has the same basic meaning. The term is used when reporting software inventory for virtual applications (not virtual application images).

virtual release

A *virtual release* is the virtual equivalent of the regular release and has the same basic meaning. The term is used when reporting software inventory for virtual applications (not virtual application images). Note that a provisioned virtual application can use either a staged or streamed virtual application image as source. The virtual applications contained within the virtual application image can themselves be seen as staged but not yet provisioned.

XCCDF profile

An *XCCDF profile* is a policy that is applied to the target computer or compared to the configuration of the target computer. The XCCDF file for each SCAP data stream defines the list of profiles supported. The XCCDF file must have at least one XCCDF profile, which specifies the rules to be used for checking a particular type of system. You can create separate XCCDF profiles for each applicable operational environment in which a system may be deployed.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X