CA IT Client Manager

Remote Control Administration Guide

Release 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 5: Customizing Remote Control 47

Chapter 6: Exporting Recording Files to Video 63

Chapter 7: Diagnostics and Troubleshooting 69

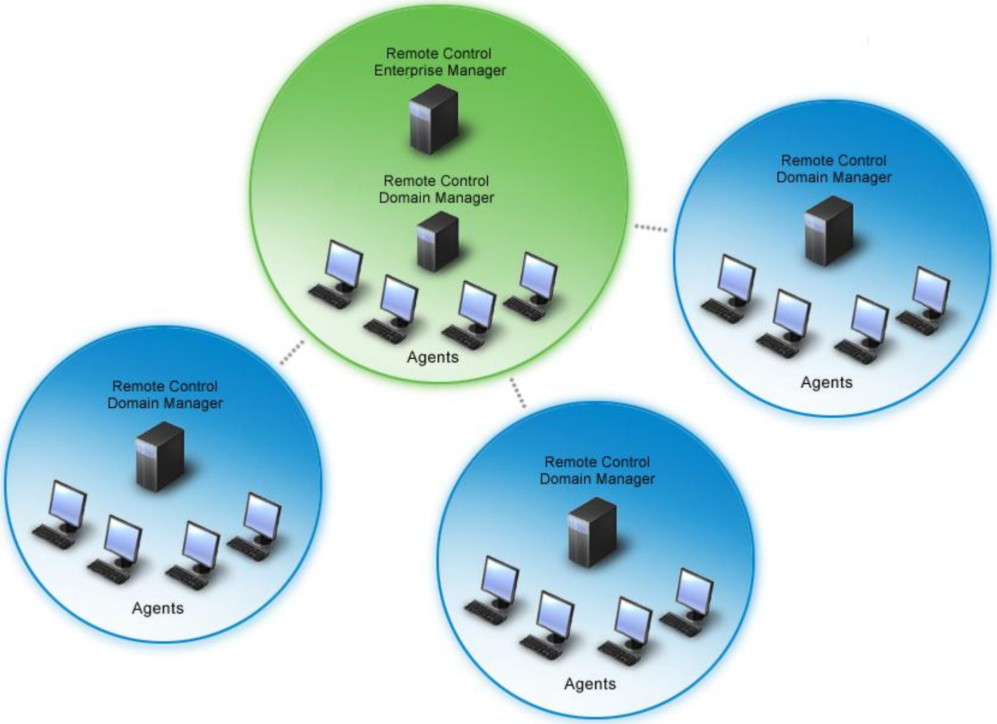
Appendix A: Remote Control XML Files 75

Chapter 1: Welcome to Remote Control

CA IT Client Manager provides a state-of-the-art remote control product, Remote Control, specifically designed for centralized enterprise management. It enables users to view and control Windows, Linux, or Apple Mac OS X (Intel) host agents installed on computers anywhere on the network from the users' local computers. The remote control managers and scalability servers are available only for Windows operating environments.

Remote Control can be used in a variety of situations, from the small privately held company with an owner who wants to work from home to very large enterprises with computers located around the world. It is also very valuable for help desk technicians, who can investigate and solve problems without having to pay a site visit, and for classroom training or meetings.

This guide provides technical assistance for the enterprise administrator, who can configure remote control computer policies and manage user access rights and permissions. You can configure Remote Control administration using a two-tier hierarchy that permits a *domain manager* to inherit policies and remote control permissions from the *enterprise manager*:



Global policies and remote control permissions can be defined and easily propagated to the entire organization from a single enterprise manager. This can be done on a geographic basis, for example, with the enterprise manager in North America and domain managers in North America, South America, Europe, and Asia.

The remote control manager provides the host with information that defines Remote Control security. The agent reports events and status information to the domain manager, and it can also receive commands. The enterprise manager, domain managers, and scalability servers are administered using the DSM Explorer.

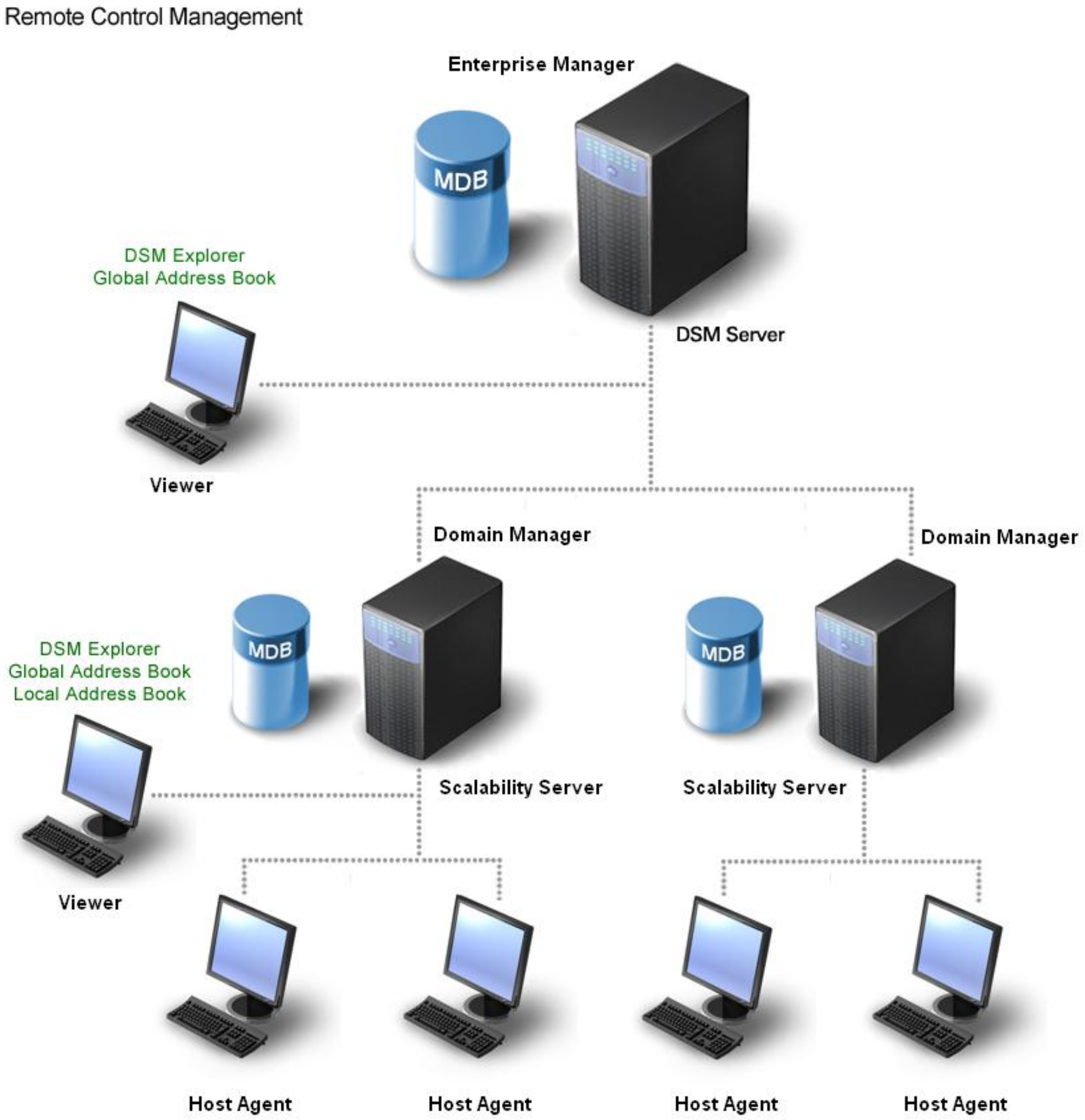
Chapter 2: Architecture

This chapter presents an overview of the architecture of Remote Control, including brief descriptions of its various components and some features.

This section contains the following topics:

Architectural Overview

The following graphic illustrates the basic components comprising the architecture of Remote Control:



Managers

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

The enterprise manager usually runs on a server class computer on the network. It has a number of functions:

- Configuration of the host agents.
- User authentication and permissions, enabling validation of user credentials during the connection process and enforcement of permissions, which control when a user is connected.

An enterprise administrator can configure the enterprise manager using the DSM Explorer. This manager also manages other CA IT Client Manager components, each of which appears as a node in the DSM Explorer tree.

The computer name of the manager appears under the Control Panel, Manager node in the DSM Explorer tree in the left pane. To view the properties of a manager, right-click the manager and click Properties in the context menu.

A *domain manager* is the central point of management for the other CA Client Management Solutions components, including scalability servers and agents. The domain manager has the same functions listed above for the enterprise manager, but it also handles logging of application and security events arising from the operation of the host agent.

You can add a domain manager to the enterprise from the Control Panel, Domains, All Domains node.

Note: For detailed information about common security and working with managers, servers, and domains, see the *DSM Explorer Help* and the *Implementation Guide*.

Scalability Server

The scalability server is a CA ITCM component which resides between the agents and the domain manager. It serves several purposes:

- Collect registration information from agents and pass it to the manager
- Distribute configuration policy from the manager to the agents
- Store agent data

There may be a large number of agents to be managed, too many for a single manager to handle. CA ITCM breaks down this task by distributing groups of agents to multiple servers. The servers then act as intermediaries and relay information to and from the manager.

The scalability server has a collection of directories and files where it stores agent data files. When the agent collects data, it is stored in the server for processing by the DSM engine. The engine is a component whose purpose is to collect information from servers and place it into the domain manager's database. A similar communication takes place when the configuration policy of an agent is modified in the DSM Explorer.

Host

When Remote Control host agents are deployed to target computers in an environment, the computers can be controlled remotely. The Remote Control host runs on the computer that you want to control using the Remote Control viewer component. The viewer connects to the host and establishes a session. The host responds to keyboard and mouse input sent from the viewer and sends a live image of its desktop to the viewer.

You can use the Infrastructure Deployment Wizard to deploy CA ITCM agents, including host agents, and scalability servers in your enterprise. The wizard guides you step-by-step through the process.

Note: For more information, see the Deployment section of the *DSM Explorer Help* and the *Implementation Guide*.

Viewer

The Remote Control viewer provides the means to view and control a remote computer. It lets you connect to a host computer and control its desktop, using your own mouse and keyboard. You can transfer files to and from the remote computer. You can also view and control multiple hosts at the same time. The extent of access, however, is subject to centrally managed user permissions imposed by the remote control manager. This helps to maintain security.

The Remote Control viewer is available from the DSM Explorer or as a stand-alone from the Windows Start menu. It is also available from the Remote Control Host icon in the taskbar, or system tray, if the viewer component is installed along with the host.

Note: You can also launch a web version of the viewer, the RC Web Viewer interface, by double-clicking RCViewer.html in the Program Files\CA\DSM\bin folder.

Global Address Book

The global address book (GAB) contains the address books created by the remote control manager. Users' computer's and protocol information is downloaded to the global address book on the Viewer pane. The global address book is downloaded from the remote control manager and is filtered to contain only the computers to which the user of the viewer has inherited access permissions from the parent address book group. Only the administrator of the remote control manager can edit the address books.

Note: Port numbers are entered automatically in the global address book but manually in the local address book. If a computer changes its primary network address, the host sends the change to the manager so it can update the GAB.

The global address book is available from the Viewer root node. You can define the user of the global address book using the Global Address Book Properties dialog, which is available from the DSM Explorer.

More information:

Users (see page 22)
Configure the Global Address Book (see page 38)
Add Users and User Permissions (see page 40)

Local Address Book

The local address book (LAB) is your personal address book. It contains information about each computer in a customized collection of books that you define. You manage computers by creating an address book hierarchy. You may add, delete, and search for computers using the Local Address Book pane in the Remote Control viewer.

You can also import and export local address books using the rcUtilCmd command line tool. An address book is stored in an XML file. An imported address book either merges its data into an existing local address book or replaces the local address book.

Note: The content of encrypted fields in an address book is locked to the local computer, enabling the content of the address books to be shared between users without compromising security.

Replayer

The Remote Control replayer component lets you play back previously recorded host sessions. It is installed during the CA ITCM installation process and is available from the Remote Control viewer. The replayer can also be launched from the Windows Explorer by double-clicking a replayer *.urc file.

Note: You can also launch a web version of the replayer, the RC Web Replayer interface, by double-clicking RCReplay.html in the Program Files\CA\DSM\bin folder.

Tools

The following command line tools are provided to assist you with various Remote Control administrative tasks:

gui_rcLaunch

Launches the Remote Control viewer when you specify an address, user credentials, and a variety of options. It can also handle legacy hosts and launch the replayer.

Note: The gui_rcLaunch command is not supported in Linux.

Note: For more information, see the Remote Control Viewer and the Remote Control Replayer sections of the *DSM Explorer Help*.

rcUtilCmd

Enables you to export and import local address books.

Note: In Linux and Mac OS X, this program is only used internally by Remote Control.

rcReplayExport

Converts Remote Control proprietary *.urc files into common video formats.

Chapter 3: Implementation

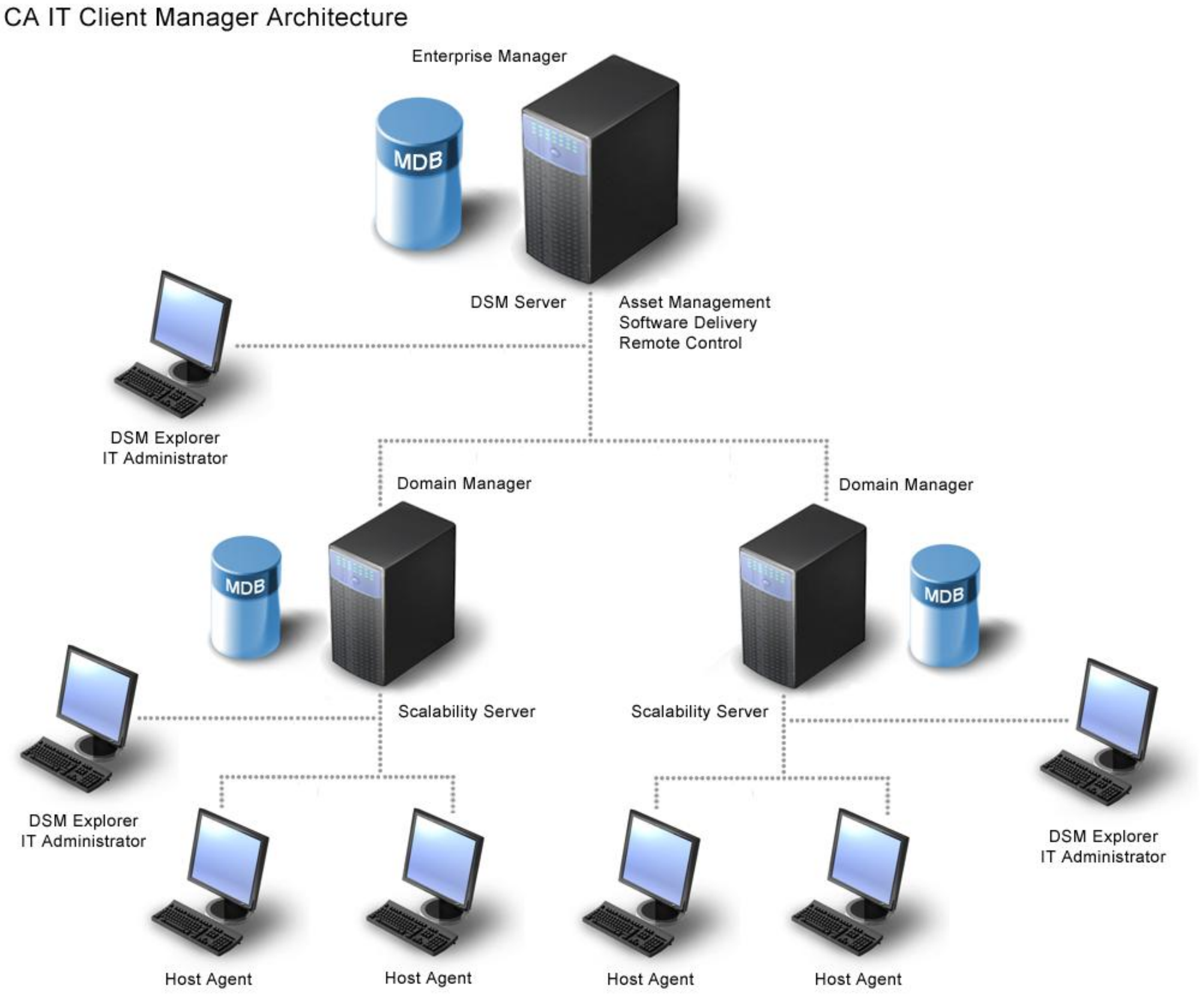
For a more complete understanding of the Remote Control component of CA ITCM, this chapter presents two streamlined implementation models and scenarios for remotely managing assets.

This section contains the following topics:

Centrally Managed Remote Control Configuration

A centrally managed environment is one where the Remote Control enterprise manager controls the host settings through configuration policies, global address book (GAB), licensing of the host agent on the domain, and user permissions. This is the default setting for CA IT Client Manager.

Typically, a centrally managed Remote Control configuration is used for large enterprises with many assets and multiple divisions or regional centers, as illustrated in the following diagram:



Scenario

The scalable two-tier architecture of Remote Control can accommodate any large enterprise. The architecture is robust, since all asset information is managed at each domain manager location and replicated to the enterprise manager.

This implementation model reflects the typical small to mid-size enterprise with multiple divisions or regional offices. A good example is a small, growing community bank with branches in three neighboring but rural towns. The main branch is located in the largest town, and it also serves as the bank's headquarters. The DSM server and enterprise manager are located here, enabling central management of all aspects of the business and monitoring of all bank branches.

There are two bank branches in each of the two other towns. Physically, the two branches in each town are much closer in distance than are the two neighboring towns, so a decision is made to locate a single scalability server and domain manager in each town. The two scalability servers and domain managers manage the day-to-day tasks of both of their respective branches. In reality each domain manager manages more than two PCs or workstations with host agents installed. Typically, a bank has five or six teller stations, several loan officers, and a manager, perhaps even an assistant manager.

Obviously, this scenario is quite simple. In a very large enterprise, with hundreds or thousands of agents, you may have some centrally managed agents configured to use local security. You also may have some stand-alone remote control units. Many large enterprises also use Wake-on-LAN technology and even smart card authentication.

Note: For more detailed information about implementing Remote Control, see the *Implementation Guide*.

Users

The IT administrator in our scenario has the overall responsibility of defining security requirements and managing all IT assets. The Remote Control component provides centralized, policy-based management and extensive security features that streamline administration across the enterprise. It enables IT administrators to access, control, view, manage, and modify remote computers.

The IT technician is responsible for the day-to-day management and maintenance of a subset of an enterprise's IT assets. Whereas the IT administrator is able to connect to all IT assets, IT technicians are only able to connect to those IT assets in their area of responsibility. Remote Control determines access through configuration of agent policy and the use of address books.

Lastly, the host user can decide whether or not a remote connection is allowed if the appropriate policy is enabled.

Note: For more detailed information about implementing Remote Control, see the *Implementation Guide*.

More information:

Configuring in a Centrally Managed Environment (see page 37)
Global Address Book (see page 15)
Local Address Book (see page 16)

Wake-on-LAN

CA ITCM has Wake-on-LAN (WOL) functionality to power up and connect to remote host computers that are switched off, for example, those located in different time zones. The Wake-on-LAN feature is available for single computers, a selection of computers, and computer groups.

Note: The agents should be in the same subnet in order to power up the switched off computers.

From the DSM Explorer, you can perform the following actions:

- Wake up a single PC and establish a connection to the PC
- Wake up an entire group of PCs (for example, a remote office location anywhere in the world) and remotely control multiple computers.

From the Remote Control viewer, you can wake up a single PC in the global address book, start it, and control it. The remote control configuration policy, Register WOL information, must be enabled to remotely power up computers that support WOL from the global address book (this is the default setting). Otherwise, WOL is only available from the DSM Explorer.

Note: For information about powering up one or more remote computers from the DSM Explorer, see the *DSM Explorer Help*.

Power Up a Remote Computer

You can power up and connect to a remote computer from the Remote Control viewer.

To power up a remote computer

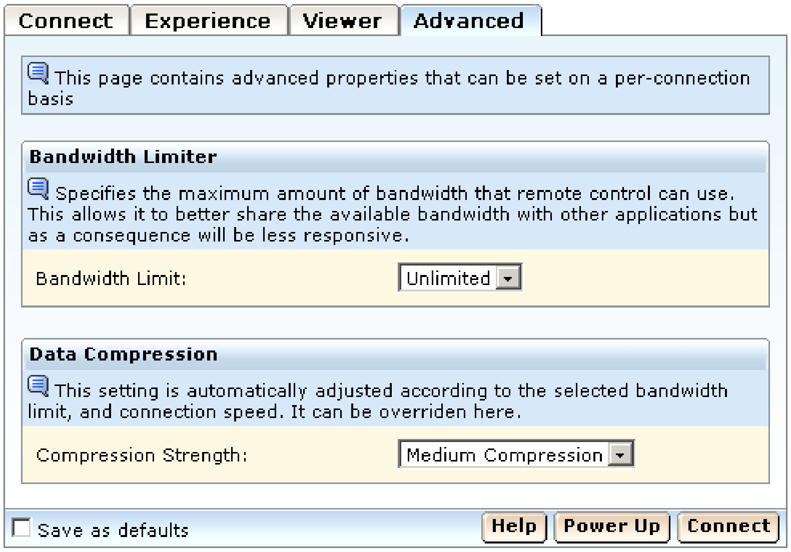
1. Double-click a computer in the global address book, My Favorites folder, or Recently Used folder.

   Alternatively, right-click a computer and click Open.

   The Connection Settings dialog appears.

2. Specify a connection type, address, and user name in the corresponding fields in the Connect tab.

3. Click the Advanced tab and click Power Up:

   This page contains advanced properties that can be set on a per-connection basis

   Bandwidth Limiter

   Specifies the maximum amount of bandwidth that remote control can use. This allows it to better share the available bandwidth with other applications but as a consequence will be less responsive.

   Bandwidth Limit: Unlimited

   Data Compression

   This setting is automatically adjusted according to the selected bandwidth limit, and connection speed. It can be overriden here.

   Compression Strength: Medium Compression

   □ Save as defaults

   Note: If the Power Up button is not visible in the viewer, then WOL information is not registered in the GAB.

   Remote Control attempts to connect you to the host computer using the Wake-on-LAN (WOL) feature, if Wake-on-LAN information is available for the specified computer. It displays a typical Connection Status message during this process.

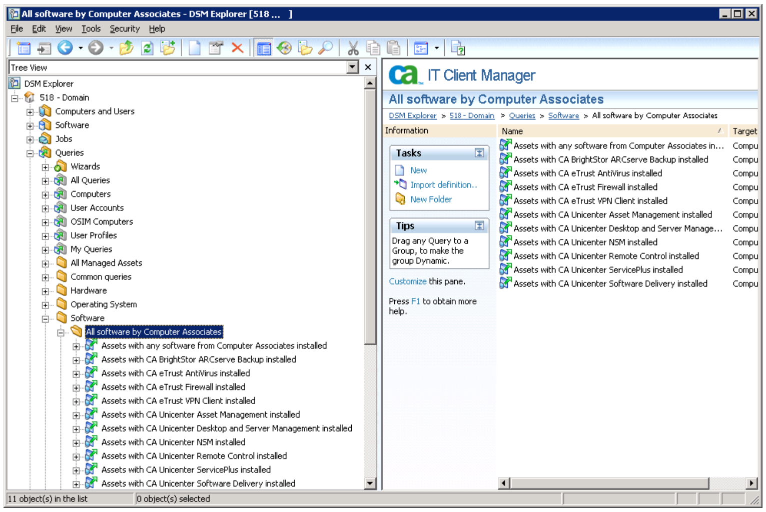
   Note: If you click Connect instead of Power Up, and the connection fails, the viewer determines the reason for the connection failure. If the connection failed because the host could not be contacted, even though the IP address/DNS name was valid, the Connection Status message lets you click the following link, which provides the same functionality as Power Up: "Click here to attempt to turn on the computer remotely, and connect again."

Queries

An essential task for any system containing a database is the ability to retrieve information from the database at any time. This process is called querying. Queries can, for example, be used as basis for the creation of the following:

- Groups of assets and their maintenance
- Policies
- Reports using the DSM Reporter

CA ITCM provides many predefined queries, including Assets with Remote Control Installed, which you can access from the All Queries subfolder or the Software, All Software by Computer Associates subfolder, as shown in this example:



DSM Explorer
518 - Domain
Computers and Users
Software
Jobs
Queries
Wizards
All Queries
Computers
User Accounts
OSIM Computers
User Profiles
My Queries
All Managed Assets
Common queries
Hardware
Operating System
Software
All software by Computer Associates
Assets with any software from Computer Associates installed
Assets with CA BrightStor ARCserve Backup installed
Assets with CA eTrust AntiVirus installed
Assets with CA eTrust Firewall installed
Assets with CA eTrust VPN Client installed
Assets with CA Unicenter Asset Management installed
Assets with CA Unicenter Desktop and Server Management installed
Assets with CA Unicenter NSM installed
Assets with CA Unicenter Remote Control installed
Assets with CA Unicenter ServicePlus installed
Assets with CA Unicenter Software Delivery installed

All software by Computer Associates

DSM Explorer > 518 - Domain > Queries > Software > All software by Computer Associates

Name	Target
Assets with any software from Computer Associates in...	Compu
Assets with CA BrightStor ARCserve Backup installed	Compu
Assets with CA eTrust AntiVirus installed	Compu
Assets with CA eTrust Firewall installed	Compu
Assets with CA eTrust VPN Client installed	Compu
Assets with CA Unicenter Asset Management installed	Compu
Assets with CA Unicenter Desktop and Server Manage...	Compu
Assets with CA Unicenter NSM installed	Compu
Assets with CA Unicenter Remote Control installed	Compu
Assets with CA Unicenter ServicePlus installed	Compu
Assets with CA Unicenter Software Delivery installed	Compu

Drag any Query to a Group, to make the group Dynamic.

Press F1 to obtain more help.

11 object(s) in the list

0 object(s) selected

You can create a new query by selecting the category and clicking New in the Tasks portlet.

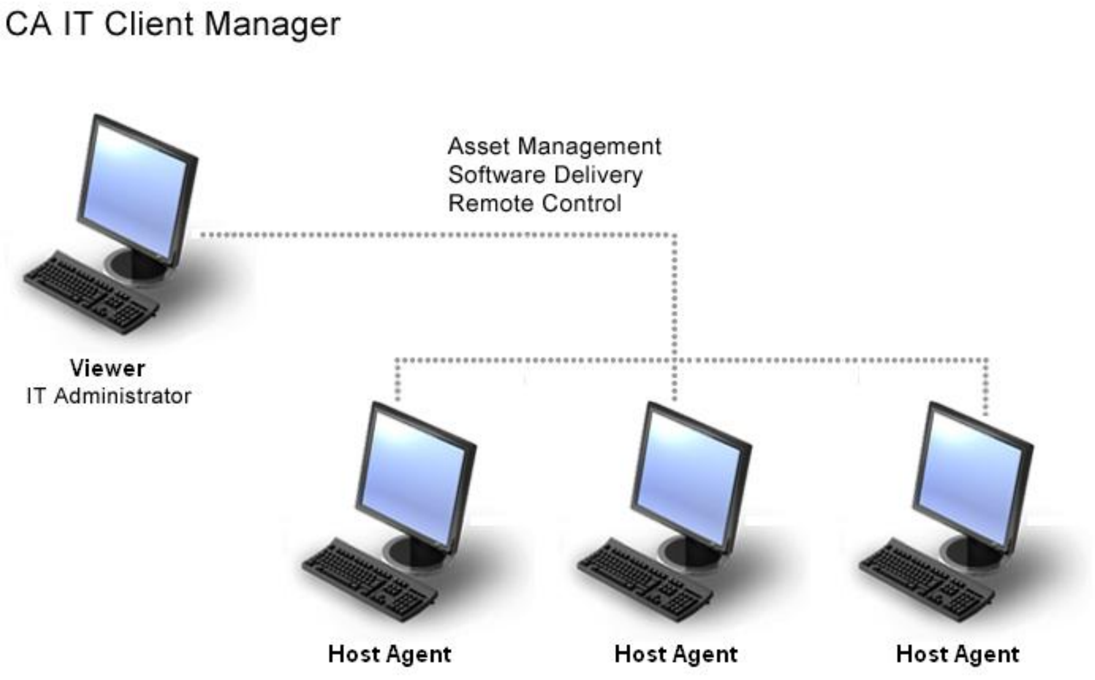
Note: For information about creating remote control session reports, see the *DSM Reporter Help*.

Stand-alone Remote Control Configuration

A stand-alone environment is one where the users of the host and viewer computers manage all settings, properties, and licensing of Remote Control. It is set by a Standalone Remote Control Agent installation. To install it manually, a separate installation wizard, setup_rc, needs to be called directly.

Note: For more information, see the *Implementation Guide*.

Typically, a stand-alone Remote Control configuration is used for smaller companies with fewer assets:



Scenario

This implementation model reflects the typical small, self-contained company with limited assets. A good example is a retail establishment, such as a video rental store or a book store, where the business owner is the IT administrator, president, chief financial officer, and human resources director. The number of PCs or workstations with host agents installed is small, limited to a few cash register stations, PCs for the bookkeeper and order clerk, and perhaps a laptop for the business owner.

Users

Again, the IT administrator in our scenario has the overall responsibility of defining security requirements and managing all IT assets. Access is determined through configuration of agent policy and the use of a local address book. The IT administrator can also deploy stand-alone hosts with preconfigured users and import address books and permissions.

As stated earlier, the host user can decide whether or not a remote connection is allowed if the appropriate policy is enabled.

Note: For more detailed information about implementing Remote Control, see the *Implementation Guide*.

How to Deploy Stand-alone Hosts with Preconfigured Users

On Windows only, you can deploy Remote Control stand-alone hosts with preconfigured users for the Unified Security and Local Security (proprietary) security providers using the Microsoft Installer (MSI).

To configure your installation image to define preconfigured users for these security providers, you must modify the following files on the installation media:

[*Path*]\Program Files\CA\DSM\bin\rcLocalSecurityConfig.xml

Configures the Local Security provider used by default on Windows.

[*Path*]\Program Files\CA\DSM\bin\rcNTSecurityConfig.xml

Configures the Unified Security provider for Windows.

The XML configuration files are compressed on the installation media and cannot be edited directly. Therefore, to deploy stand-alone hosts with preconfigured users, you must do the following:

1. Extract the relevant XML file.
2. Modify the defaultusers parameter in the XML file by adding preconfigured users.
3. Deploy the host agents from the extracted image.

Extract XML Files

You can perform an MSI Administrative install to extract the XML configuration files from the installation media.

To extract the XML files

1. Open a command line window.
2. Change the directory to the WindowsProductFiles_x86\AgentRC folder on the installation DVD.
3. Execute the following command:

   ```
   MSIExec /a AgtRC.msi
   ```

   An installation wizard appears.
4. Enter a suitable location for the extracted files.
5. Click Finish.

   The XML files you need to edit are extracted to [*Path*]\Program Files\CA\DSM\bin for Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008 configuration files.

More information:

Control the Visibility of Viewer and Host Properties (see page 48)
Customizing Remote Control (see page 47)

Modify the defaultusers Parameter in the XML File

Adding preconfigured users for a provider requires modifying the defaultusers parameter in the common paramsection of the extracted XML file.

To modify the XML file on the installation image

1. Locate the common paramsection.

   The following is a copy of the Security configuration file for Windows (rcNTSecurityConfig.xml):

   ```
   <configuration>
   <allusers>
   <paramsection name="itrm">
   <paramsection name="rc">
   <paramsection name="security">
   <paramsection name="providers">
   <paramsection name="common">
   <attribute name="managed">local</attribute>
   <parameter name="defaultusers" value="{winnt:SID=S-1-5-32-544}">
   <parameterinfo name="pi_defaultusers">
   <attribute name="flags">1</attribute>
   <attribute name="desc">Security: List of default users</attribute>
   <attribute name="type">string</attribute>
   </parameterinfo>
   </parameter>
   <parameter name="dll" value="rcCommonSecurity">
   <parameterinfo name="pi_dll">
   <attribute name="flags">1</attribute>
   <attribute name="desc">Security: Shared library providing common security
   functionality.</attribute>
   <attribute name="type">string</attribute>
   </parameterinfo>
   </parameter>
   <parameter name="displayname" value="Unified">
   <parameterinfo name="pi_displayname">
   <attribute name="flags">1</attribute>
   <attribute name="desc">Security: Display name of this security
   provider</attribute>
   <attribute name="type">string</attribute>
   </parameterinfo>
   </parameter>
   </paramsection>
   </configuration>
   ```

2. Modify the default value for the defaultusers parameter. The entry should be a comma-separated list of user names, or NT User Security Identifiers, as shown in the above example. Do not include a space after the comma.

   When done, you can install Remote Control. The default users are automatically created when the host is installed.

Example: Preconfigure Users "one", "two", and "three" on the Local Computer and the Domain Account, "helpdesk"

```
<configuration>
<allusers>
<paramsection name="itrm">
<paramsection name="rc">
<paramsection name="security">
<paramsection name="providers">
<paramsection name="common">
<attribute name="managed">local</attribute>
<parameter name="defaultusers" value="winnt:[DOMAIN]/helpdesk,one,two,three">
<parameterinfo name="pi_defaultusers">
<attribute name="flags">1</attribute>
<attribute name="desc">Security: Shared library providing common security
functionality.</attribute>
<attribute name="type">string</attribute>
</parameterinfo>
<parameter name="dll" value="rcCommonSecurity"><parameterinfo name="pi_dll">
<attribute name="flags">1</attribute>
<attribute name="desc">Security: Name of dll providing NT security.</attribute>
<attribute name="type">string</attribute>
</parameter>
<parameter name="displayname" value="Unified">
<parameterinfo name="pi_displayname">
<attribute name="flags">1</attribute>
<attribute name="desc">Security: Display name of this security provider</attribute>
<attribute name="type">string</attribute>
</parameterinfo>
</parameter>
</paramsection>
</configuration>
```

The Local Security provider supports the same comma-separated list of users. When creating the local security provider users, the user name is also used for the user’s password. It is the responsibility of the system owner to modify these passwords after installation to ensure that the system is secure.

Deploy the Stand-alone Hosts

You can deploy the stand-alone host agents from the extracted image by double-clicking AgtRC.msi.

Importing and Exporting Local Address Books

A local address book (LAB) contains details about computers that can be viewed or controlled by the Remote Control viewer. It can also optionally contain details about login credentials. The Import/Export feature, rcUtilCmd.exe, permits you to share the content of a local address book between users, without compromising security.

More specifically, the local address book consists of an XML file which is tied to a particular user. It may become inaccessible if the file is renamed or relocated; rcUtilCmd.exe makes the necessary modifications to the file so that it can be used in its new location. Additionally, login credentials in the XML file are encrypted using a key unique to the user who is logged on at the time. If an address book is exported to another user, these details cannot be decrypted and they appear blank, because rcUtilCmd.exe does not permit these details to be transferred. An imported address book merges its data into an existing local address book. If required, you can replace the local address book with the imported book.

rcUtilCmd—Export a Local Address Book

The export command lets you export a local address book.

The command has the following syntax:

```
export [exportedbook]
```

exportedbook

> Specifies the name of the file to be exported. This file is the local address book of the currently logged on user. The default is exportedbook.

The rcUtilCmd.exe program creates the default file, rcExportedLAB.xml, in the current working directory.

rcUtilCmd Command—Import an Exported Address Book into the Local Address Book

The import command lets you import an exported address book.

The command has the following syntax:

```
import [-i exportedbook] [-r] [addressBookName] [addressBookDescription]
```

exportedbook

Specifies the same name that is used for the previously exported address book.

Note: You can specify the name without the .xml suffix.

-r

Specifies that the computers already existing in the destination address book will be replaced; otherwise, the replacement definition is ignored.

addressBookName

Specifies the name of a new address book to create or add to the local address book.

addressBookDescription

Specifies the description of the new address book.

The rcUtilCmd.exe program reads *exportedbook* and attempts to add its content to *addressBookName*, creating it if necessary. If *addressBookName* is not supplied, the content is added to a group with the name "Imported Address Book" at the root of local address book.

Where the imported book contains nested books, this structure is maintained in the destination local address book, and the nested content is imported.

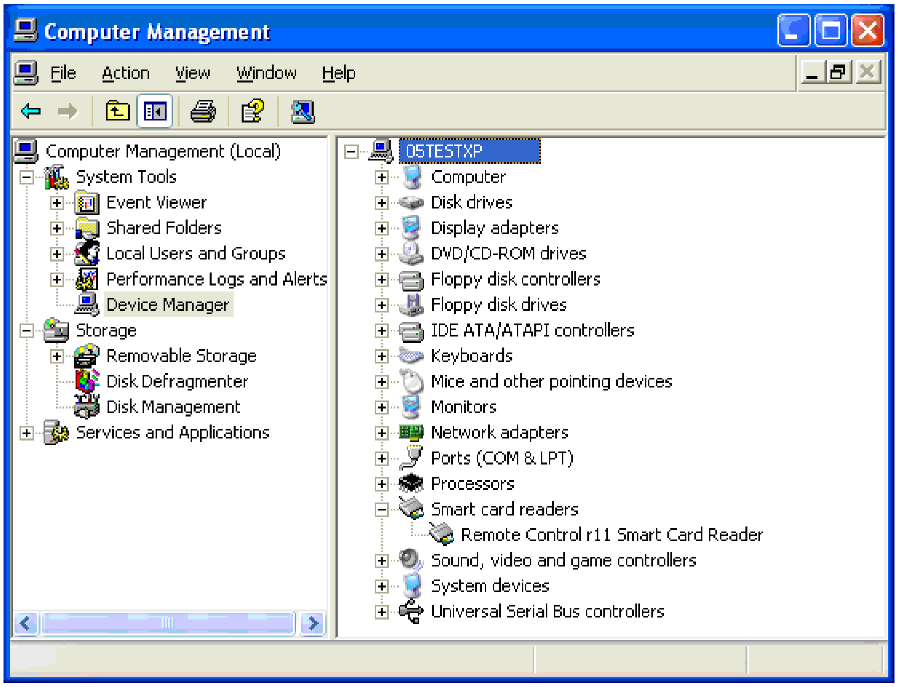
Note: The import is always into the local address book of the currently logged on user.

Smart Card Authentication

A digital certificate can be stored on a *smart card* that includes the user's name, organization, and other identification information. Such smart cards are used to secure mission-critical applications, such as email, web server access, network access, and system login.

CA ITCM supports smart card readers, and Remote Control can now redirect smart card authentication when the user of a Remote Control viewer attempts to log on to the operating system of a remote host computer using their local smart card.

If necessary, a new smart card device is silently installed on the host computer. Thereafter, this device is always visible from the system's Device Manager, even when a session is not connected:



The name of the device does not indicate which viewer is attached. Even after the virtual smart card device has been installed, it is hidden from smart card applications until the viewer user connects their smart card reader for the first time. Therefore, the reader will not appear in the standard smart card insertion UI until the Remote Control viewer has activated it for the first time. The device will remain visible until the computer is rebooted or the device is manually removed.

Note: For more information, see the *Implementation Guide*.

Connect to a Remote Computer Using a Smart Card

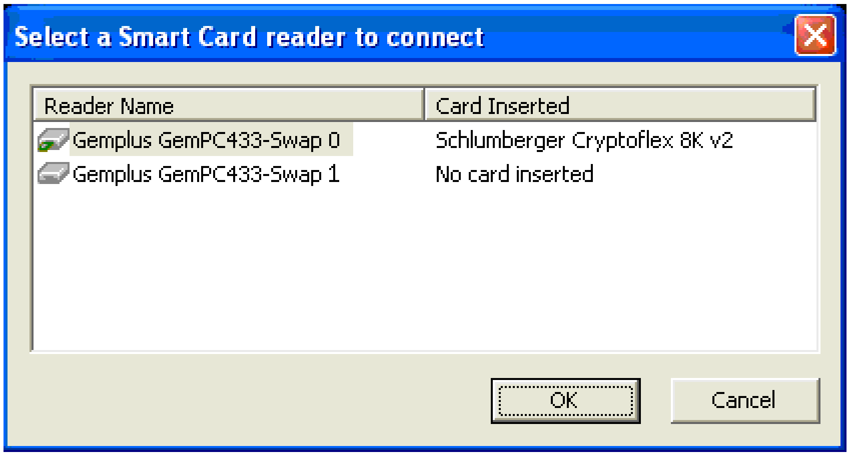
On Windows you can connect to a remote computer from the Remote Control viewer using a smart card.

Note: The remote host computer must support smart card redirection, that is, its Enable smart card redirection configuration policy must be set to True. For more information, see the Configuration Policy section of the *DSM Explorer Help*.

To connect to a smart card reader

1. Access the Remote Control viewer.
2. Connect to a specific remote host computer.
3. Click Connect Smart Card in the Sessions context menu or click the Smart Card toolbar button.

   If only one reader is installed, it is selected automatically. If more than one smart card reader is installed, the Select a Smart Card Reader to Connect dialog appears:



Reader Name	Card Inserted
Gemplus GemPC433-Swap 0	Schlumberger Cryptoflex 8K v2
Gemplus GemPC433-Swap 1	No card inserted

4. Select a smart card reader to connect to the remote host computer.

   To indicate that the smart card reader is connected, the viewer GUI changes slightly—the Disconnect Smart Card menu option is enabled and the corresponding toolbar button is depressed (checked state).
5. Insert your smart card once the smart card reader is connected.

   Applications on the host computer receive the insertion event in the same way they would if a smart card was inserted locally.

Disconnect from a Smart Card Reader

To disconnect from a smart card reader, click Disconnect Smart Card in the Sessions context menu or click the depressed Smart Card toolbar button.

The smart card device is disconnected immediately, but the device driver is not removed and the device is not hidden. To applications using the smart card reader, the virtual device appears as a reader with no card inserted.

Chapter 4: Configuring Remote Control

You can configure stand-alone and centrally managed environments before installation to ensure optimum settings for your environment.

A user's access and associated permissions in the enterprise are managed through address book settings in the DSM Explorer. Create an address book that includes the computers for which you want to grant access using the Add Users task from the Remote Control Permissions pane. Once you add the users or groups that you want to access the computers, you can further control the access by setting permissions for the users or group.

Note: This chapter is for advanced users of Remote Control. Entering incorrect information may result in the product not working properly.

This section contains the following topics:

Configuring in a Centrally Managed Environment

Accessing or controlling the remote machines in Remote Control is managed using *user permissions*. User permissions are configured for groups of computers, not individual computers, through address books. For each address book, the administrator can specify which operations the individual users can perform on the computers in the group (for example, View, Chat, Send Files). By default, an address book inherits its parent's permissions, but you can add to or modify the permissions.

More information:

Users (see page 22)

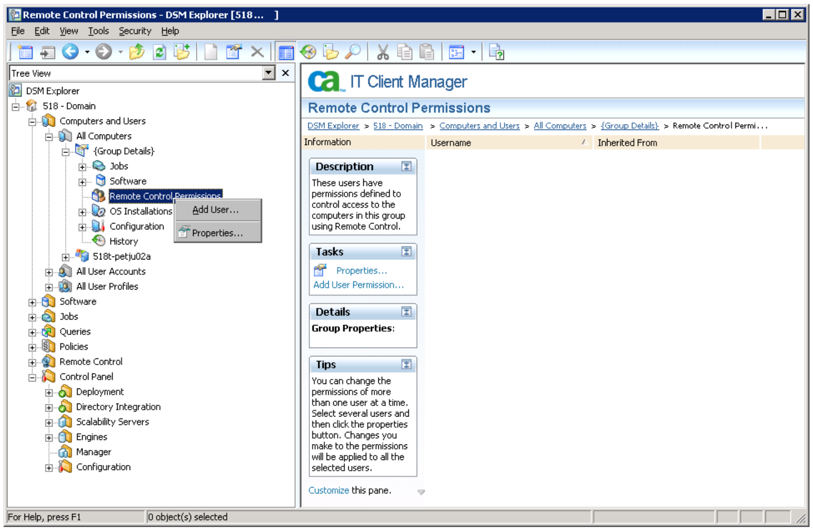
Configure the Global Address Book

You can create and configure a global address book (GAB) using the Address Book Properties dialog.

To create a new global address book group

1. Right-click the Remote Control Permissions node under the Group Details subnode of the appropriate Computer group in the DSM Explorer.

   A context menu appears:

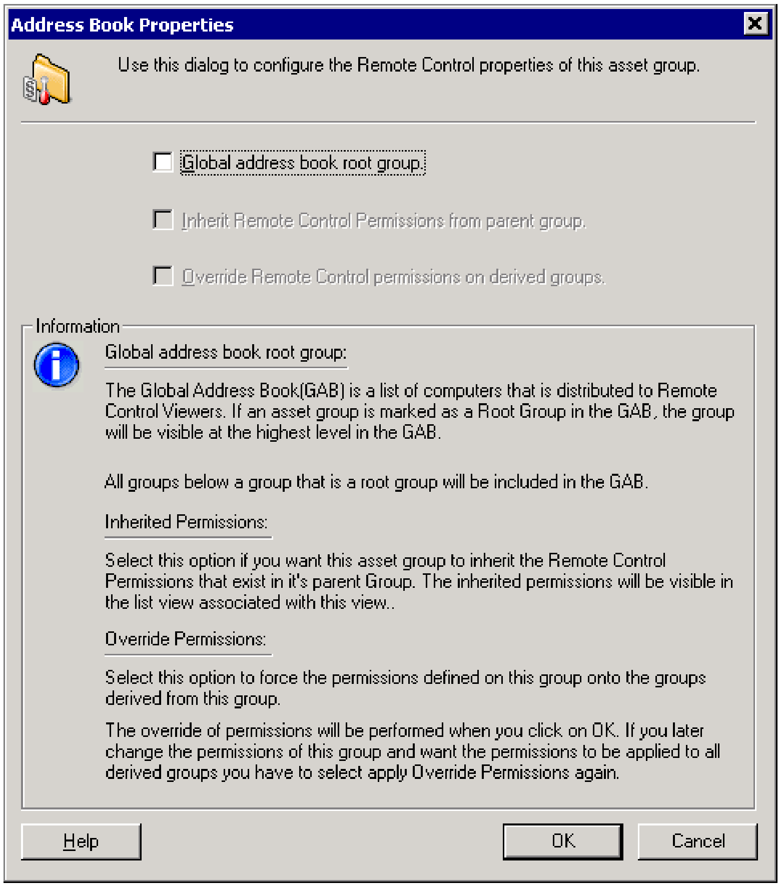


These users have permissions defined to control access to the computers in this group using Remote Control.

You can change the permissions of more than one user at a time. Select several users and then click the properties button. Changes you make to the permissions will be applied to all the selected users.

2. Click Properties.

   The Address Book Properties dialog appears:



Address Book Properties

Use this dialog to configure the Remote Control properties of this asset group.

☐ Global address book root group.

☐ Inherit Remote Control Permissions from parent group.

☐ Override Remote Control permissions on derived groups.

Information

Global address book root group:

The Global Address Book(GAB) is a list of computers that is distributed to Remote Control Viewers. If an asset group is marked as a Root Group in the GAB, the group will be visible at the highest level in the GAB.

All groups below a group that is a root group will be included in the GAB.

Inherited Permissions:

Select this option if you want this asset group to inherit the Remote Control Permissions that exist in it's parent Group. The inherited permissions will be visible in the list view associated with this view..

Override Permissions:

Select this option to force the permissions defined on this group onto the groups derived from this group.

The override of permissions will be performed when you click on OK. If you later change the permissions of this group and want the permissions to be applied to all derived groups you have to select apply Override Permissions again.

3. Select the Global Address Book Root Group option.

   The root group and its members are added to the global address book.

4. (Optional) Select the Inherit Remote Control Permissions from Parent Group option.

5. (Optional) Select the Override Remote Control Permissions on Derived Groups option.

6. Click OK.

   The new global address book group is created.

   Any subsequent changes to the asset group—adding a computer or removing one—are reflected in the global address book.

   All of the user permissions defined in the global address book root are displayed in the Root Address Book Permissions pane. Each asset group that is part of the global address book inherits these permissions by default.

Add Users and User Permissions

Remote control sessions are managed with user permissions and address books. Therefore, you must add users and user permissions for each user account or asset group.

To add a new user permission to an address book group

1. Right-click the Remote Control Permissions node under Group Details and click Add User.

   Alternatively, click Add User Permission in the Tasks portlet of the Remote Control Permissions pane.

   The Add User Permission dialog appears.

2. Select a security authority from the available directories.

   Note: You can add users/groups of ADS, LDAP, and NDS directories, if they are configured.

3. Browse for security principals, that is, users or groups, and select one or more.

   The selected security principal (for example, Administrators) is added to the Names list and a description of the security principal's permissions appears in the Description field.

4. Click Add to add the selected users to the list of security principals.

5. Click OK.

   The selected users have access to all of the computers in the specified computer group.

Note: The first time you add a user and assign permissions, you are in effect creating a new global address book group.

Configure Host Remote Control Permissions

You, as an administrator, can define or modify the type of remote control operations that a user can perform on computers in the current asset group. For example, you may want one user group to have exclusive and secure control permissions for all host computers and other user groups to have more limited control, such as a corporate training user group with shared control and chat permissions only. If users attempt to connect with invalid permissions, the session will be rejected and added to a list of rejected sessions in the Rejected Sessions pane that you can view.

Note: The Rejected Sessions node and corresponding Rejected Sessions pane are only available when the DSM Explorer is connected to a CA ITCM [assign the value for rn in your book] domain manager. If the DSM Explorer is connecting to an older manager, this node will not be available.

To configure the type of remote control operations that a specified user can perform

1. Right-click the user in the Remote Control Permissions pane, and click Properties.

   The User Remote Control Permissions dialog appears.

2. Review the permissions—such as View, Exclusive Control, Shared Control, Chat, Send Files, Record, and so on—that are currently allowed.

3. (Optional) Select a permission, modify its value, and click Change.

   The value of the selected permission is changed.

4. Click OK.

   The specified user's remote control permissions are configured.

Purge Rejected Sessions

You can automatically purge rejected sessions In the Rejected Sessions pane using the Age of rejected sessions to purge policy. This policy enables you to configure a separate purging value for rejected sessions as compared to the value used for purging closed sessions, thereby customizing session retention to match your corporate policy.

To purge rejected remote control sessions

1. Navigate to Control Panel, Configuration, Configuration Policy, Default Computer Policy, DSM, Remote Control, Manager in the DSM Explorer tree.

   The remote control manager policies are displayed in the right pane.

2. Double-click the Age of rejected sessions to purge policy.

   The Setting Properties dialog appears.

3. In the Value field, change the value according to your needs. The default setting is 86400 seconds.

   This purge action occurs during a scheduled session purge, and the Next session purge policy controls the regularity of the session purges.

   Note: The Value field in this dialog is enabled only if you unseal the policy first.

4. Double-click the Next session purge policy.

   The Setting Properties dialog appears again.

5. Optionally, change the default value and click OK.

   The changes are saved.

   Note: Changing these values does not require restarting the management server.

6. Seal the policy for it to be applied to the manager.

Note: For more information about the remote control configuration policies, see the Configuration Policy section of the *DSM Explorer Help*.

Configuring in a Stand-alone Environment

In the Remote Control stand-alone environment, access control is configured by defining permissions on each remote control host within the organization. To configure the users who connect to the host and to set the type of security used in a stand-alone environment, use the Users tab of the DSM Properties - Remote Control dialog. The Users tab also lets you add and delete users, view their properties, and assign permissions. Changes are applied immediately.

Note: The Users tab is only available from the DSM Properties - Remote Control dialog in a centrally managed agent environment when the Centralized security configuration policy is set to False. For more information, see the Configuration Policy section of the *DSM Explorer Help.*

Add Users

Use the Users tab to add and delete users and view their properties. Changes are applied immediately.

To add a new user

1. From the Users tab in the DSM Properties - Remote Control dialog, click the Current Security Provider field and select one of the following options:

   Local

   Permits you to create a user name and password for any user you want to add.

   Unified

   Permits you to select a user from a list of local and domain users previously established by the administrator of the local network.

2. Click Add.

   Remote Control displays the dialog applicable to the type of security provider you selected:

   Local

   Displays the Create New User dialog. Go to Step 4 to continue.

   Unified

   Displays the Add Users dialog with a listing of domains. Go to Step 7 to continue.

3. Enter the user name, the full name of the user, and any noteworthy information in the User Details fields.

4. Enter a password and confirm the password in the Password fields.

5. Click Create.

   The user description appears in the list view of the Users tab. Go to Step 10 to continue.

6. Explore domains and locate the user or groups of users that you want to add.

   Note: Each time you expand the DSM Explorer tree, a message appears requesting you to wait for the user information. The listing is produced almost immediately.

7. Select the user or group of users you want to add.

   The Add button is enabled.

8. Click Add.

   The user or group of users you selected appears in the Users to be added list.

9. Verify your selection and, if correct, click OK.

   The Users tab appears with your selection in the list.

10. Click OK.

    The user or group of users is added, and the user information remains in the Users tab until the user is deleted.

Configure Host Remote Control Permissions

In a stand-alone environment, you can assign permissions to authorized users, defining what the user can do on the host, for example, send and receive files, access the Chat feature, and so on.

To configure user permissions

1. From the Users tab on the DSM Properties - Remote Control dialog, select the user for whom you need to set up permissions.

   Once selected, Remote Control enables the following buttons: Properties, Permissions, and Delete.

   Note: Be sure to click the User Name part of the description to enable these buttons.

2. Click Permissions.

   The Permissions of... dialog displays the following columns so you can view or configure permissions for your user, that is, define what the user can do:

   Permission

   Lists available functions for which you can assign permissions.

   Description

   Provides a brief description of the function displayed on that line.

   Note: The Permissions of... dialog is also available from the My Computer, Properties dialog in a stand-alone environment.

3. Configure permissions by selecting or clearing the check box for each desired function, and click OK.

   The Permissions of... dialog closes and you are returned to the Users tab of the DSM Properties - Remote Control dialog.

4. Click OK.

   The permission settings are saved and the DSM Properties - Remote Control dialog closes.

Note: In a stand-alone environment, a user can be granted permissions to only one computer, that is, the host. Also, in centrally managed and stand-alone environments, these permissions may be overridden by the options set for the host feature configuration.

Chapter 5: Customizing Remote Control

You can customize the locally managed properties and security prior to installation to ensure optimum settings for your environment. Typically, customization is usually only necessary in a stand-alone environment. The settings that control the properties, security, and policy are stored in XML files (see Extract XML Files (see page 28)) that you can edit during an MSI Administrative install.

Note: This chapter is for advanced users of Remote Control. Entering incorrect information in any of the customization procedures may result in the product not working properly.

This section contains the following topics:

Control the Visibility of Viewer and Host Properties

You can control the visibility of each property on the Advanced tab in the Viewer Properties dialog and the DSM Properties - Advanced tab.

To control the visibility of a property

1. Access the appropriate XML file, rcViewerConfig.xml or rcHostConfig.xml.
2. Change the value of the flags attribute for the relevant parameter. Valid values for the flags attribute are:

   0–1

   If set to either of these values, the property does not appear in the Advanced tab.

   2–7

   Indicate reserved values.

   8–9

   If set to either of these values, the property appears in the Advanced tab.

   9–15

   Indicate reserved values.

Example: Hide Compression Property

To prevent overriding the viewer's default compression strength setting, for example, you may want to hide the existence of this property. To remove this property from the Advanced tab, you need to set the flags attribute for the compressionstrength parameter to 0 or 1 in the rcViewerConfig.xml file:

```
<configuration>
<allusers>
<paramsection name="itrm">
<paramsection name="rc">
<paramsection name="viewer">
<paramsection name="managed">
<parameter name="manageripaddress" value=""><parameterinfo
name="pi_manageripaddress">
<attribute name="flags">17</attribute>
<attribute name="desc">Viewer: IP address of the viewer's management
server.</attribute>
<attribute name="type">string</attribute>
</parameterinfo></parameter>
</paramsection>
</paramsection>
.
.
</paramsection>
```

```
      </paramsection>
      </paramsection>
            </paramsection>
   </allusers>
.
.
.
<user>
<paramsection name="itrm">
<paramsection name="rc">

<attribute name="managed">local</attribute>
.
.
.
<paramsection name="general">
<parameter name="migrated" value="no"><parameterinfo name="pi_migrated">
<attribute name="flags">1</attribute>
<attribute name="desc">Viewer: Have the rcViewer settings from RC6 been
migrated</attribute>
<attribute name="type">string</attribute>
</parameterinfo></parameter>
<parameter name="defaultConnectionType" value="2"><parameterinfo name="pi_filter">
<attribute name="count">7</attribute>
<attribute name="string0">View</attribute>
<attribute name="string1">Stealth</attribute>
<attribute name="string2">Shared</attribute>
<attribute name="string3">Classroom</attribute>
<attribute name="string4">Exclusive</attribute>
<attribute name="string5">Secure</attribute>
<attribute name="string6">Meeting</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Viewer: The default connection type to be used by the
viewer.</attribute>
<attribute name="type">enum</attribute>
</parameterinfo></parameter>
<parameter name="computername" value=""><parameterinfo name="pi_computername">
<attribute name="flags">9</attribute>
<attribute name="desc">Viewer: Optional name for this computer: defaults to netbios
name</attribute>
<attribute name="type">string</attribute>
</parameterinfo></parameter>
<parameter name="usealternatesmoothing" value="0"><parameterinfo
name="pi_usealternatesmoothing">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">1</attribute>
<attribute name="desc">Viewer: Uses an alternate smoothing method when shrinking the
view.</attribute>
```

```
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<parameter name="smoothwhenshrinking" value="1"><parameterinfo
name="pi_smoothwhenshrinking">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">1</attribute>
<attribute name="desc">Viewer: Uses a smoothing filter when shrinking the view in
shrink/scale to fit mode.</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<parameter name="smoothwhenmagnifying" value="1"><parameterinfo
name="pi_smoothwhenmagnifying">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">1</attribute>
<attribute name="desc">Viewer: Uses a smoothing filter when stretching the view in
scale to fit mode.</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<parameter name="showsessiontoolbar" value="1"><parameterinfo
name="pi_showsessiontoolbar">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">1</attribute>
<attribute name="desc">Viewer: Display the session toolbar during a viewer
session.</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<parameter name="bandwidthlimiter" value="0"><parameterinfo
name="pi_bandwidthlimiter">
<attribute name="count">9</attribute>
<attribute name="string0">Unlimited</attribute>
<attribute name="string1">4Mbit</attribute>
<attribute name="string2">2Mbit</attribute>
<attribute name="string3">1Mbit</attribute>
<attribute name="string4">512Kbit</attribute>
<attribute name="string5">256Kbit</attribute>
<attribute name="string6">128Kbit</attribute>
<attribute name="string7">64Kbit</attribute>
<attribute name="string8">32Kbit</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Viewer: Limits the maximum network bandwidth usage of
sessions.</attribute>
<attribute name="type">enum</attribute>
```

```
</parameterinfo></parameter>
<parameter name="compressionstrength" value="2"><parameterinfo
name="pi_compressionstrength">
<attribute name="count">5</attribute>
<attribute name="string0">No Compression</attribute>
<attribute name="string1">Light Compression</attribute>
<attribute name="string2">Medium Compression</attribute>
<attribute name="string3">Heavy Compression</attribute>
<attribute name="string4">Extra Compression</attribute>
<attribute name="flags">1</attribute>
<attribute name="desc">Viewer: Viewer data compression strength.</attribute>
<attribute name="type">enum</attribute>
</parameterinfo>
</parameter>
.
.
.
</parameterinfo></parameter>
</paramsection>
</paramsection>
</paramsection>
</paramsection>
</user>
</configuration>
```

More information:

Extract XML Files (see page 28)

Control the Ability to View and Manage Properties

You can control the display of the common configuration policies that are available for centrally managed environments in the Remote Control policy group pane. You can access this from the Control Panel, Configuration, Configuration Policy, Default Computer Policy, DSM node in the DSM Explorer tree.

In some companies it makes sense to simplify the policy view because you may not want to manage some properties. For example, Remote Control offers many categories of events, and a company may not want to track some of these.

Do not manage a property by setting the relevant configuration policy to "locally managed" in the DSM Explorer. Instead, one way to control access to a property is to comment out the property in the XML file using "<!--" and "-->" in the appropriate section, as shown in the following example. This change should only be made on a manager.

Note: For more information about the remote control configuration policies, see the Configuration Policy section of the *DSM Explorer Help*.

Example: Exclude the Host Has Stopped Listening Event

To exclude the general event within agent policy for “A host has stopped listening for connections,” wrap the appropriate section in the rcHostEventsConfig.xml file with the left arrow, exclamation mark, double dash characters (<!--) and double dash, right arrow characters (-->):

Note: We recommend commenting out the setting rather than removing the entry.

```
<configuration>
<allusers>
<paramsection name="itrm">
<paramsection name="rc">
<paramsection name="events">
<paramsection name="hostlogs">
<parameter name="sendeventstomanager" value="1">
<parameterinfo name="pi_sendeventstomanager">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">1</attribute>
<attribute name="desc">Events (Host): Send events to the management
server.</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
</paramsection>
<paramsection name="general">
<parameter name="hostunlocked" value="0">
<parameterinfo name="pi_hostunlocked">
<attribute name="max">1</attribute>
```

```
<attribute name="min">0</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Events (Host): Raise event "A host has been
unlocked".</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<parameter name="hostlocked" value="0">
<parameterinfo name="pi_hostlocked">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Events (Host): Raise event "A host has been
locked".</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<parameter name="hostrebooting" value="0">
<parameterinfo name="pi_hostrebooting">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Events (Host): Raise event "A host has initiated a
reboot".</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<!-- <parameter name="hostnotlistening" value="0"> -->
<!-- <parameterinfo name="pi_hostnotlistening"> -->
<!-- <attribute name="max">1</attribute> -->
<!-- <attribute name="min">0</attribute> -->
<!-- <attribute name="flags">9</attribute> -->
<!-- <attribute name="desc">Events (Host): Raise event "A host has stopped listening
for connections".</attribute> -->
<!-- <attribute name="type">bool</attribute> -->
<!-- </parameterinfo></parameter> -->
<parameter name="hostlistening" value="0">
<parameterinfo name="pi_hostlistening">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Events (Host): Raise event "A host has started listening for
connections".</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<parameter name="hoststopped" value="0">
<parameterinfo name="pi_hoststopped">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Events (Host): Raise event "A host has shutdown".</attribute>
<attribute name="type">bool</attribute>
```

```
</parameterinfo></parameter>
<parameter name="hoststarted" value="0">
<parameterinfo name="pi_hoststarted">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Events (Host): Raise event "A host has started
up".</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<parameter name="error" value="1">
<parameterinfo name="pi_error">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Events (Host): Raise event "A host error has
occurred".</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<parameter name="remotecontrolsessionstopped" value="0">
<parameterinfo name="pi_remotecontrolsessionstopped">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Events (Host): Raise event "A remote control session has
stopped".</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<parameter name="remotecontrolsessionstarted" value="0">
<parameterinfo name="pi_remotecontrolsessionstarted">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Events (Host): Raise event "A remote control session has
started".</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
</paramsection>
<paramsection name="security">
<parameter name="securityvalidatepermissionsfailed" value="1">
<parameterinfo name="pi_securityvalidatepermissionsfailed">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Events (Host): Raise event "A viewer user's request is
denied".</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<parameter name="securityvalidateuserfailed" value="1">
```

```
<parameterinfo name="pi_securityvalidateuserfailed">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">9</attribute>
<attribute name="desc">Events (Host): Raise event "A host-viewer login has
failed".</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
</paramsection>
</paramsection>
</paramsection>
</paramsection>
</allusers>
</configuration>
```

Control Default Values

You can control the default values of locally managed agent and manager policies in Remote Control.

To control the default value, adjust the value setting for each property in the associated XML file. When adjusting type=int properties, make sure the value falls between the Min and Max settings.

Example: Enable Fail Safe Security in Managed Mode

Remote Control can connect to agents if the management server goes offline. By default, this value is set to provide optimum security. To permit help desk technicians to connect to a host when the management server goes offline, adjust the enablefailsafe parameter value to 1 (True) in the rcHostConfig.xml file.

The following are the default values for stand-alone agents:

```
<configuration>
<allusers>
<paramsection name="itrm">
<paramsection name="rc">
<paramsection name="host">
.
.
.
<paramsection name="managed">
<parameter name="deferals" value="1">
<parameterinfo name="pi_deferals">
<attribute name="max">10</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">24</attribute>
<attribute name="desc">Host: Number of deferrals possible when
rebooting.</attribute>
<attribute name="type">int</attribute>
</parameterinfo></parameter>
<parameter name="defertime" value="300">
<parameterinfo name="pi_defertime">
<attribute name="max">3600</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">24</attribute>
<attribute name="desc">Host: Time that a reboot can be deferred (sec).</attribute>
```

```
<attribute name="type">int</attribute>
</parameterinfo></parameter>
<parameter name="checkaddressinterval" value="300">
<parameterinfo name="pi_checkaddressinterval">
<attribute name="max">3000</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">25</attribute>
<attribute name="desc">Host: Time period between checks for changes of the host's
listening addresses and protocols (sec).</attribute>
<attribute name="type">int</attribute>
</parameterinfo></parameter>
<parameter name="registerconnectioninterval" value="30">
<parameterinfo name="pi_registerconnectioninterval">
<attribute name="max">3000</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">25</attribute>
<attribute name="desc">Host: Time period (sec) between attempts to register a host
with the management server.</attribute>
<attribute name="type">int</attribute>
</parameterinfo></parameter>
<parameter name="refreshregistercomputer" value="86400">
<parameterinfo name="pi_refreshregistercomputer">
<attribute name="max">200000</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">25</attribute>
<attribute name="desc">Host: Time period (sec) between attempts to refresh the
registration of a host with the management server.</attribute>
<attribute name="type">int</attribute>
</parameterinfo></parameter>
<parameter name="enablesecuritycache" value="0">
<parameterinfo name="pi_enablesecuritycache">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">25</attribute>
<attribute name="desc">Host: Enable security caching in managed mode.</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
<parameter name="enablefailsafe" value="1">
<parameterinfo name="pi_enablefailsafe">
<attribute name="max">1</attribute>
<attribute name="min">0</attribute>
<attribute name="flags">25</attribute>
<attribute name="desc">Host: Enable fail safe security in managed mode if connection
to manager fails.</attribute>
<attribute name="type">bool</attribute>
</parameterinfo></parameter>
```

```
</paramsection>
</paramsection>
</paramsection>
</paramsection>
</allusers>
</configuration>
```

Localizing the Remote Control Dialogs

Remote Control is available in French, German, and Japanese—plus Korean, Simplified Chinese, and Spanish for agents—but you can also localize it for any other language. The text to be localized is stored in resource files (.dll files), web pages (.htm files), images (.gif), and plain text files.

Many of these files have the ISO language code embedded in the file names or are stored in folders named after the language. For example, the host's strings are stored in rcHostViewer.enu. Common language codes are enu: English (US), fr: French, de: German, it: Italian, no: Norwegian, sp: Spanish, and se: Swedish.

Text Files

The text files containing strings that can be localized are in the Remote Control installation folder and have these names:

- rcHostViewer.enu

  Strings for the host agent and viewer
- rcManager.enu

  Strings for the management server
- rcHostConfig.xml

  Strings for the property descriptions and values

The first two files have the same format as a Windows .ini file, that is, they are divided into sections prefixed with [sectionname] followed by a set of lines in "id=string" format. The identifier *(id*) is simply a name by which the various programs refer to a string. You should never change these identifiers, only the string contents.

For example, the start of the section for the host in rcHostViewer.enu looks like this:

```
#--------------------------------------------------------------------
# The host agent
[rcHost]
IDS_TIMERERROR="Failed to start timer"
IDS_GETADDRESSESTIMERFAILED="Failed to start the timer for checking listening
addresses."
IDS_RC="Remote Control"
IDS_OK="success"
IDS_SERVICEINSTALLED="Service installed successfully"
IDS_SERVICEINSTALLFAILED="Failed to install service"
IDS_SERVICESTATUSFAILED="Failed to get service status"
IDS_SERVICESTOPPED="Service is stopped"
IDS_SERVICESTARTING="Service is starting"
IDS_SERVICESTOPING="Service is stopping"
IDS_SERVICERUNNING="Service is running"
IDS_SERVICECONTINUING="Service is continuing"
IDS_SERVICEPAUSEPENDING="Service pause is pending "
IDS_SERVICEPAUSED="Service is paused"
IDS_SERVICEUNKNOWN="Service status is unknown"
IDS_SVCSTARTFAILED="Unable to start service"
IDS_SVCSTARTING="Service %1$t is starting"
IDS_SVCSTARTED="Service started"
IDS_SVCSTOPFAILED="Unable to stop service"
IDS_SVCSTOPPING="Service %1$t is stopping"
#--------------------------------------------------------------------
```

The strings are quoted. Also, the last example contains the special marker string, "%1$t", which is used by the host to programmatically insert the name of the host service. Some strings may have more than one of these markers. In this case, they are sequentially numbered, for example, "%2$t, %3$t". Some languages may require a different word order than English, so these numbers are used to place the inserted strings in the correct position.

Tools Required

Editing the relevant resource information requires the following tools:

- For .dll files, a resource editor such as that built into many programming environments like Visual C.
- For .htm files, an HTML editor such as Microsoft FrontPage or a plain text editor like Notepad.
- For text files, a text editor such as Notepad.
- For .gif files, an image editor such as Jasc Paint Shop Pro.

How to Localize Remote Control Dialogs

To produce localized Remote Control files, use *one* of the following methods:

Method 1

Make copies of all English resource files and rename them to include the appropriate language code. These copies are then localized. Some additional configuration is also needed to make use of the new files. The advantage of this is that the English version remains available if required. The disadvantage is that there is more work involved.

Method 2

Translate the English (en) versions of these files and Remote Control automatically uses them. Typically, Remote Control searches for files matching your local language and, if it cannot find them, falls back to English. In this case, the English files are used and contain your translations. The advantage of this scheme is that it is simple, but the English version is not available.

The following sections assume that Method 1 is being used to produce localized files.

Changing the Text of the Host Agent’s Dialogs

Translating the host’s dialogs involves editing the following resources:

Host Agent Dialogs

For the typical confirmation, restart, and message dialogs, the host agent reads its strings from the [rcHost] section in rcHostViewer.enu. This section is edited as described previously.

Host Property Dialog

The host’s property dialog reads its strings from the [rcPropDialog] section of rcHostViewer.enu and from the property descriptions embedded in the XML files.

The dialogs themselves are read from rcPropDialog_en.dll. These dialogs have embedded text strings, so you must use a resource editor to change these.

Host Events

The host also optionally reports events to the Windows event log and uses rcEvent.dll to store the event messages. The text strings can be edited in the rcEvents.enu file.

Changing the Text of the Viewer’s Dialogs

Translating the viewer is more difficult than the host because there are more resources to edit. As the viewer uses the EGC framework, both the basic framework and the viewer plug-in must be localized. A basic overview for the plug-in only is provided here.

Translate the EGC-based Viewer

The EGC-based viewer obtains its resources from a number of places:

- Dialogs, web pages, and images are stored in gui_rcview.dll.

  Make a copy of this file including the country code, for example, gui_rcview_se.dll.

- The Viewer Properties dialog is stored in rcPropDialog_en.dll.

  Copy this file with a new name using your country code, for example, rcPropDialog_se.dll. Then use a resource editor to edit the strings on the dialogs that can be localized.

- The viewer reads strings from the [rcPlugin] section of rcHostViewer.enu for message dialogs.

You must configure EGC to use the new gui_rcview.dll file. To do this, create the following registry entries (assuming the Swedish locale, SE):

```
#-------------------------------------------------------------------
[HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\EGC3.0N\Locale\SE]
"HelpFile"="C:\\Program Files\\CA\\SC\\EGC\\egc30enu.chm"
"ResourceDLL"="C:\\Program Files\\CA\\SC\\EGC\\egc30Nres.enu"
[HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\EGC3.0N\Plugins\ITRMRC_DSMVIEW\Lo
cale\SE]
"HelpFile"="C:\\Program Files\\CA\\DSM\\help\\gui_rcview_help_enu.chm"
"MessageHelpFile"="C:\\Program Files\\CA\\DSM\\help\\gui_rcview_msg_enu.chm"
"ResourceDLL"="C:\\Program Files\\CA\\DSM\\bin\\gui_rcview_se.dll"
#-------------------------------------------------------------------
```

A simple way of doing this is to export the existing English entries to a text file, edit them using Notepad, and then import back to the registry.

This example assumes that Remote Control is installed in the default location on the C drive. It still uses the English help files, since you cannot localize these.

Change the Text of the Replayer's Dialogs

The Remote Control replayer uses similar resources to those of the viewer except that they are stored in gui_rcreplay.dll.

To configure EGC to use them, create these registry entries (this example assumes Swedish):

```
#-------------------------------------------------------------------
[HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\EGC3.0N\Plugins\ITRMRC_DSMREPLAY\
Locale\SE]
"HelpFile"="C:\\Program Files\\CA\\DSM\\help\\gui_rcreplay_help_enu.chm"
"MessageHelpFile"="C:\\Program Files\\CA\\DSM\\help\\gui_rcreplay_msg_enu.chm"
"ResourceDLL"="C:\\Program Files\\CA\\DSM\\bin\\gui_rcreplay_se.dll"
#-------------------------------------------------------------------
```

Changing the Text of the Help Files

The help files have a .chm extension (compiled HTML) and, as mentioned earlier, cannot be edited.

Chapter 6: Exporting Recording Files to Video

You can convert Remote Control proprietary *.urc files into common video formats (AVI and WMV), using the Replay Export tool, rcReplayExport.exe. Such recordings can be played when Remote Control is not installed. They can be played on many media player applications and on some DVD players. For example, you may want to compile a library of recordings for helpdesk purposes that detail complicated tasks that users must perform. Users can download and watch these recordings without the need for the Remote Control replayer.

This section contains the following topics:

Prerequisites

To export WMV format files, the Windows Media Format runtime application needs to be installed, if it is not already present. This is available on the installation media, in the WindowsProductFiles_x86\WindowsMedia\wmfdist.exe folder.

Conversion Considerations

The Replay Export tool converts the *.urc files into an uncompressed video stream, which is then fed into a specified video codec for compression. The tool is simply designed to allow conversions of recording files to video without altering any of the default configuration options. However, conversion to video files is a complicated process, and while we only recommend this for experienced users, an array of configuration options is also available to tune the conversion process and get the best results.

The .urc recording file format is specifically tailored to accurately record screen activity and provides excellent quality, with a very small file size. Converting the files to video usually results in a perceptible loss in quality, coupled with an increase in file size. However, some recordings where screen activity is complicated may benefit from conversion.

Video compression is a slow and CPU intensive operation. It may take several minutes to convert a short recording to video. Therefore, you should test conversion on short recordings at first to check that the conversion is optimal.

The AVI file format lets you store uncompressed video. Be aware that uncompressed video files are extremely large (typically at least 1 GB per minute), and therefore not recommended.

Note: As you can now play back *.urc recording files directly in the Windows Media Player without loss in quality, as long as the Remote Control replayer application is installed, you should consider whether this is the best solution for your needs.

Conversion Formats

The recording conversion's main parameters are file format and video compression codec. The file format essentially defines a container for the compressed video data, while the compression codec defines how the video data is compressed. Each file format may only support certain compression codecs. The Replay Export tool supports the AVI and Windows Media Video (WMV) formats. The AVI format supports more compression codecs, but the more modern WMV format is better suited for streaming media downloads.

The Replay Export tool does not install any video compression codecs, but instead utilizes the video compression codecs installed on your computer to compress the video data. You must install suitable codecs to perform video conversion. Windows Media compression codecs, which provide good compression performance, are usually already installed by default with Windows Media Player or DirectX. However, you may also want to install third-party video codecs, such as XviD ©xvid.org and DivX®. Once installed, the Replay Export tool automatically detects the available codecs and chooses the most suitable one for the specified file format as the default setting. If you select a different codec from the Video Compression Codec drop-down list, choose a common compression codec that is widely installed.

To play back the converted video, a user must have installed a media player capable of decoding your selected video compression format. Therefore, it is advisable that you select a codec that is likely to be installed on your target audience's computers. In the case of Windows Media codecs, for instance, while the Windows Media 9 codec may provide the best conversion results, users with older versions of Windows Media Player may be unable to play back converted video without upgrading or downloading additional codec packs. However, many player applications are now able to automatically download codecs over the Internet, as required.

Configuring the Compression Codec

Each compression codec provides its own codec-specific configuration dialog, which should be documented by the codec provider. Therefore, it is beyond the scope of this guide and the online help to describe detailed codec configuration.

In general, the most important factor to consider in video conversion is the bit rate. As a rule, the higher the bit rate, the better the video quality, but the file size also increases accordingly. Many codecs support both Constant and Variable bit rate encodings. CBR encoding is better suited for streaming downloads, where the download bandwidth is known in advance. VBR encoding varies the encoding bit rate to match the level of screen activity. This can result in smaller video files, with no reduction in quality.

VBR encoding works by assessing the level of video activity during the recording to determine what bit rate to use. However, this assessment is usually not tuned to detect activity typical of screen-capture video. Therefore, the quality of some recording conversions may suffer when using VBR encoding.

For best conversion results, we recommend trying several codecs and comparing the quality and file size.

Access the Replay Export Tool

There are multiple methods for accessing the Replay Export tool.

To access the Replay Export tool, choose *one* of these methods

- Right-click a recently recorded or replayed session and click Quick Export.

  Quick Export automatically starts the conversion process using default encoding options and requires no further input.

- Right-click a recently recorded or replayed session and click Export to Video.

  Export to Video invokes the Export Options dialog, enabling you to view or modify the default encoding options before starting the conversion process.

  Note: For detailed descriptions of the Quick Export feature and the Export Options dialog, see the Remote Control Replayer section of the *DSM Explorer Help*.

- Double-click rcReplayExport.exe in the Windows Explorer.

- Use the command line interface.

  For example, the following command converts all of the recording files in the current folder to Windows Media Video format, using the best available codec and default encoding options:

  ```
  rcReplayExport /WMV *.urc
  ```

rcReplayExport Command—Set Export Options

The following syntax lists the command line parameter options for the replay export tool:

```
rcReplayExport [/WMV [/BR bitrate] [/Q quality] [/VBR] | /AVI [/CODEC codec]] [/QUIET]
[/IDLE] [ input file [...]]
```

/WMV

Specifies encoding to WMV format.

/BR *bitrate*

Defines the bit rate for encoding in kilobits per second (must be >= 28kbps).

/Q *quality*

Defines the quality value, which ranges between 1 and 100.

/VBR

Specifies variable bit rate mode.

/AVI

Specifies encoding to AVI format with codec default options.

/CODEC *codec*

Specifies the video codec to use.

/QUIET

Specifies that the progress dialog not be displayed.

/IDLE

Indicates that conversion be performed during idle processor time.

Note: A list of input files can be specified at the end of the command line. The list may contain the wildcards "*" and "?".

Note: If either /WMV or /AVI is specified, the Export Options dialog does not appear.

Examples

This example opens the Replay Export dialog, which is ready to convert all of the recording files in the current folder:

```
rcReplayExport *.urc
```

This example converts all of the recording files in the current folder to Windows Media Video format, using the best available codec and default encoding options:

```
rcReplayExport /WMV *.urc
```

This example converts the test1.urc and test2.urc files to test1.avi and test2.avi, using the Microsoft MPEG-4 Codec V3 compression codec:

```
rcReplayExport /AVI /CODEC “Microsoft MPEG-4 Codec V3” test1.urc test2.urc
```

Chapter 7: Diagnostics and Troubleshooting

This chapter includes information about diagnostic tools and several tips for troubleshooting Remote Control problems.

This section contains the following topics:

Log File Collection Tool dsminfo

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.

Connection Problems

Problem areas for network connections can include those involving physical network connectivity, primary network address configuration, and Remote Control host configuration.

Network Connection Fails

Symptom:

I am having trouble connecting to the network.

Solution:

Use the ping command to detect basic network problems.

Examples

To test the local TCP/IP stack, for example, enter the following command in a command line window:

```
ping 127.0.0.1
```

If you get a response, then the networking software on your computer is working.

To test the connection to a remote computer, enter the following command:

```
ping address of remote host
```

IP Address Fails

Symptom:

Whenever I enter the IP address for my computer, I get an error message.

Solution:

The network adapter may not have an IP address, or the wrong address for your computer is registered to your DNS server.

To test whether either one of these conditions exists, do the following:

1. In a command line window, enter the following command:

   ```
   ipconfig
   ```

   Your local IP address displays.

2. Enter *hostname*.

   Your computer's name displays.

3. To test whether DNS has the correct name for your computer, enter the following command:

   ```
   ping hostname
   ```

   This step echoes the IP address that DNS *thinks* matches your *hostname*. If it differs from what ipconfig returned, then there is a mismatch.

4. To fix a mismatched IP address, enter the following command:

   ```
   ipconfig /renew
   ```

Remote Control Host Status Unknown

Symptom:

How do I determine the current status of my Remote Control host?

Solution:

The Remote Control host program runs under the control of the Common Application Framework (CAF). You can use CAF to determine whether the remote host computer is running by entering the following command:

```
caf status rchost host remote computer address
```

Logon Problems

Logon problems typically result from invalid credentials or the lack of user permissions or incorrect permissions.

Credentials Are Invalid

Symptom:

Whenever I enter my user name and password, I get an error message telling me that this information is invalid.

Solution:

Remote Control uses two methods to validate your credentials. In centrally managed installations with the Centralized security policy disabled, or *stand-alone installations*, the host matches the credentials you enter in the viewer component to a local or domain account on the remote computer. In a centrally managed installation with the Centralized security policy *enabled* (the default configuration), the same process applies but it is done from the computer on which the manager runs.

Note: For more information about the Centralized security configuration policy, see the Configuration Policy section of the *DSM Explorer Help*.

If Remote Control rejects your credentials and you are sure you entered them correctly, check them independently by logging on to the host computer using the following command:

```
net use \\host computer name\c$ /user:username password
```

Connection Permissions Lacking

Symptom:

My credentials were accepted, but I get a message telling me that I lack permissions.

Solution:

If your credentials are accepted but you do not appear to be a valid user, then contact your system administrator, who will assign the correct permissions for your account on the remote host computer.

Reboot Buttons Disabled

Symptom:

Sometimes when Remote Control notifies me that a reboot is pending, I am not able to postpone or cancel the reboot because the buttons are disabled.

Solution:

When Remote Control reboots a computer after a disconnect, a countdown dialog appears which tells you that a reboot is pending. This dialog also has three useful buttons: Reboot Now, Defer, and Cancel. In some circumstances these buttons are disabled.

This happens when more than one user is logged onto the machine, typically using Microsoft Remote Desktop Connection. The reason is that one user cannot be allowed to reboot the machine at random, because that will affect all other users without warning.

Global Address Book Not Fetched

Symptom:

I moved my scalability server to a new domain manager, and subsequently I cannot fetch the global address book from the new manager.

Solution:

The Remote Control viewer gets the network address of the domain manager from which to fetch the global address book from comstore, using the parameter “itrm/agent/units/currentmanageraddress”. This parameter is populated every time the agent registers with its scalability server.

If the scalability server is moved to a new domain manager, that is, registered with a new domain manager and deregistered from the original domain manager, all agents that connect through that scalability server still have this parameter set to the address of the original manager. You need to reregister the agents with the scalability server, because the viewer‘s global address book will not download properly until the agent re-registration has occurred and the above comstore parameter has been correctly populated.

Remote Control Session Fails on a RHEL 5 Agent

Symptom:

When I initiate a secure mode remote control session on an RHEL 5 agent, the following error is displayed:

Esc is already running, but is not responding. To open a new window, you must first close the existing ESC process, or restart the system.

Solution:

Run the following command:

```
yum remove esc
```

Diagnostic Tools

The following diagnostic tools are available in CA IT Client Manager.

Event Log

On Windows, you can view the application event log in the Settings, Control Panel, Administrative Tools, Event Viewer, Application folder. Events are placed there by the Remote Control host, and they may indicate the problem.

On Linux, you can look at the system log.

Trace Log

CA IT Client Manager components write tracing information to files in the following folder:

```
c:\\Program Files\CA\DSM\logs
```

The drive may be different on your computer. You can open the TRC_RCHOST.log to see if there are any error traces.

Technical Support

For assistance, contact CA Support at http://ca.com/support.

Appendix A: Remote Control XML Files

Each CA IT Client Manager component that needs specific initialization will be installed with an XML file. The XML files store the details of the entries that will be generated in the underlying configuration component. This appendix lists the Remote Control configuration XML files.

This section contains the following topics:

Remote Control XML Files

The following lists the Remote Control configuration XML files that exist in the Program Files\CA\DSM\bin directory on the installation media or in the application directory after installation:

File	Comment
rcCAMConfig.xml	**Important!** Do not change defaults unless directed by CA Technical Support.
rcCommonConfig.xml	**Important!** Do not change defaults unless directed by CA Technical Support.
rcHostConfig.xml	Host-specific settings.
rcHostEventsConfig.xml	Host event messages.
rcHostUnmanagedConfig.xml	Stand-alone host-specific settings.
rcLocalSecurityConfig.xml	Local Security provider settings.
rcManagementConfig.xml	Manager and Manager policy settings.
rcManagementEventsConfig.xml	Manager and Manager policy event settings.
rcNTSecurityConfig.xml	Unified Provider settings (Windows and DSM X.509 certificates).
rcProtocolsConfig.xml	TCP protocol settings.
rcRegister.xml	Enterprise registration settings for hosts.

File	Comment
rcSecurityConfig.xml	Host security configuration settings.
rcUnixSecurityConfig.xml	Unified Provider settings (Linux and DSM X.509 certificates).
rcViewerConfig.xml	Viewer-specific settings.

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