



CA Technologies

CA ControlMinder™ Rapid Implementation Guide

SAM JumpBox

Contents

References	3
CA ControlMinder References	3
Tibco References.....	3
Glossary.....	5
Introduction	6
Background	7
Architecture	8
Getting Started.....	9
Configure MS Windows Remote Desktop Services.....	10
Enable Single Sign-On For Terminal Server Connections.....	23
Configure The Enterprise Management Server For Integrated Windows Authentication.....	28
Create A Remote App For CM ENTM	29
Install Session Recording Agent	37
Change The Recording Behavior	40
Install ControlMinder Endpoint Software On The JumpBox.....	44
Protect The Session Recording Agent	54

References

The references related to CA ControlMinder may be found on the CA support web site in both PDF and HTML format.

<https://support.ca.com>

The references related to Tibco are included in the distribution and may be found in both PDF and HTML format in the following folder:

...\AccessControlServer\MessageQueue\tibco\ems\5.1\doc

CA ControlMinder References

- CA ControlMinder Premium Edition Release Notes 12.8
- CA ControlMinder Premium Edition Implementation Guide 12.8
- CA ControlMinder Premium Edition Enterprise Administration Guide 12.8
- CA ControlMinder Reference Guide 12.8
- CA ControlMinder Endpoint Administration Guide for UNIX 12.8
- CA ControlMinder Endpoint Administration Guide for Windows 12.8
- CA ControlMinder selang Reference Guide 12.8
- CA ControlMinder Troubleshooting Guide 12.8

Tibco References

- TIBCO Enterprise Message Service Installation 5.1
- TIBCO Enterprise Message Service User's Guide 5.1
- TIBCO Enterprise Message Service Application Integration Guide 5.1
- TIBCO Enterprise Message Service C and COBOL Reference 5.1



CA ControlMinder Rapid Implementation Guide – SAM JumpBox

Copyright ©2014, CA, Inc. All rights reserved. Microsoft, Windows, Windows Server, Active Directory, SQL Server, Remote Desktop Services, and Internet Explorer are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. ObserveIT is a trademark of ObserveIT Systems, Ltd. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. UNIX is a registered trademark of The Open Group. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

This document is for your informational purposes only. CA Technologies assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document “*as is*” without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.

Glossary

CA	formerly Computer Associates – now CA Technologies
CM	ControlMinder (formerly Access Control)
ENTM	Enterprise Manager
EP	Endpoint (server)
JB	JumpBox
MS	Microsoft Corporation
MSADS	Microsoft Active Directory Server / Services
MSSQL	Microsoft SQL/Server
OEM	Original Equipment Manufacturer
OIT	ObserveIT
OS	Operating System
RIA	Rapid Implementation Architecture
RIG	Rapid Implementation Guide
SAM	Shared Account Manager (formerly PUPM)
UNAB	UNIX Authentication Broker
W2K3	Windows 2003
W2K8	Windows 2008

Introduction

CA ControlMinder Premium Edition provides an extensive range of features and functions that may be used to provide a complete access control enterprise security solution, or may be used separately to provide a subset of the overall enterprise security.

This document presents a straight-line implementation guide that may be used to configure a separate Microsoft Windows NT server as a JumpBox (JB) for use in the CA ControlMinder Shared Account Management (SAM) security model.

The implementation consists of configuring a stand-alone Microsoft Windows 2008 server to act as the SAM JB and creating an application based on the server configuration that may be distributed to users to provide a convenient connection for JB access.

The JB configuration involves enabling and licensing Microsoft Terminal Services, enabling single sign-on for Microsoft Terminal Server connections, configuring the CA ControlMinder Enterprise Manager (ENTM) to support Integrated Windows Authentication, installing and configuring CA Session Recording agent, and installing CA ControlMinder to provide server-centric protection for the CA Session Recording components. CA Session Recording is an OEM implementation of ObserveIT's leading session management and recording solution that is seamlessly integrated into CA ControlMinder Shared Account Management.

Please note that, as currently configured, the SAM JB is only supported to be hosted on a Microsoft Windows 2008 server.

Background

CA ControlMinder Shared Account Management (SAM) is a function that provides password management functions for service accounts.

In the simplest form, SAM is a password vaulting facility that securely manages highly encoded endpoint passwords, and provides various methods of securely delivering those passwords to the user for direct input, or through an automatic connection model whereby the user never has direct access to the password.

SAM also provides a means to automatically change application passwords for ODBC, JDBC, Scheduled Tasks and command line enabled applications.

Finally, SAM supports an integration point with Observe IT to provide video-like recording and replay of endpoint activities through either Microsoft Remote Desktop Protocol (RDP), web interfaces for Oracle or Microsoft SQL/Server or the PuTTY SSH application.

In order to use the automatic endpoint connection features of SAM, it is necessary to have access to a system that has the required support utilities available. The following table presents the automatic connection type and required components. Please note that the list in the table is current as of the time of this document but may change as new endpoints are supported.

Table 1 – Automatic Logon Access List

Connection Type	Required Components
Windows	Microsoft RDP
UNIX	PuTTY (SSH, TELNET)
MS SQL Server	Microsoft SQL Management Studio
ORACLE Web	Microsoft Internet Explorer
FTP	FTP application (ftp.exe)
Juniper NetScreen	Microsoft Internet Explorer
Nokia IPSO	Microsoft Internet Explorer
Reflection	Reflection application (Rx.exe) – X-11 server

The primary advantage of using a SAM JB is that all of the components listed in the table may be installed in one location instead of being installed and maintained on several hundred individual desktop or notebook systems. Similarly, only one installation of the CA Session Recording agent is required to be installed, so that reduces administrative overhead, as well.

Architecture

The architecture of the SAM environment with the JB in play is shown in Figure 1, below. In this figure we have the ENTM, the JB and representative endpoints.

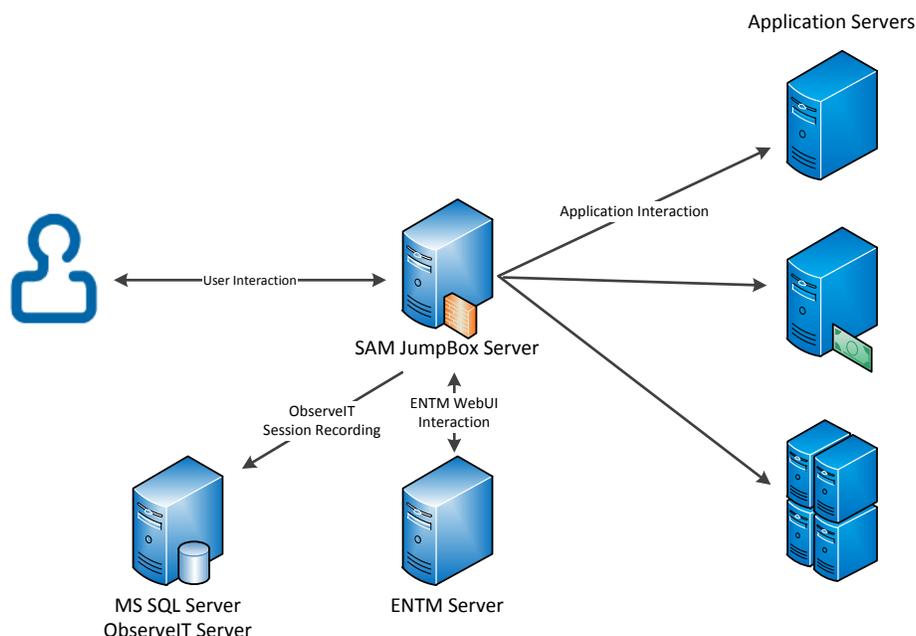


Figure 1 – SAM JumpBox Overview

In the standard SAM model, the user connects to the ENTM Server using a web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Google Chrome. If the user is simply checking out an account password then the password is displayed in the user's browser, or written to the clipboard for non-viewable pasting into an application. If the user is using one of the automatic connection models listed in Table 1 then an Active-X control is executed in the user's local browser that loads the target application and enters the relevant credentials transparently to the user. As mentioned previously, this model requires each of the desired target applications to be present on the user's computer, and this increases overhead and may lead to security exposures since the user is typically sitting outside of an enterprise firewall.

In the SAM JB model, everything works exactly the same as the standard model with the only exception being that all of the components are collocated and execute on the SAM JumpBox Server. The user reaches the SAM JB using RDP with Integrated Windows Authentication and from that point forward it appears that the each application is running locally on the user's computer when in fact each application is running on the SAM JB directly. And since all of these items are collocated it is possible to put the SAM JB behind an enterprise firewall, thus increasing security for otherwise exposed application components.

Getting Started

First, a few notes...

- This guide is not a replacement for the CA ControlMinder official documentation.
- It is expected that the implementer of this the CA ControlMinder SAM JumpBox has a working knowledge of Microsoft Windows NT operating system and of the CA ControlMinder ENTM and SAM functionality.
- It also is required that that the customer be licensed for CA ControlMinder, CA Session Recording, Microsoft Remote Desktop Services, and any other licensing required by other third-party software.
- The guide does not provide the implementation steps for CA ControlMinder or CA Session Recording. It is expected that those are implemented and functional prior to beginning this implementation.
- It is expected that the SAM JumpBox, the end user systems and CA ControlMinder ENTM are all configured to use the same Microsoft Active Directory structure. This is required to enable the single sign-on functionality described below.
- The SAM JumpBox as shown is implemented on Microsoft Windows 2008 R2.

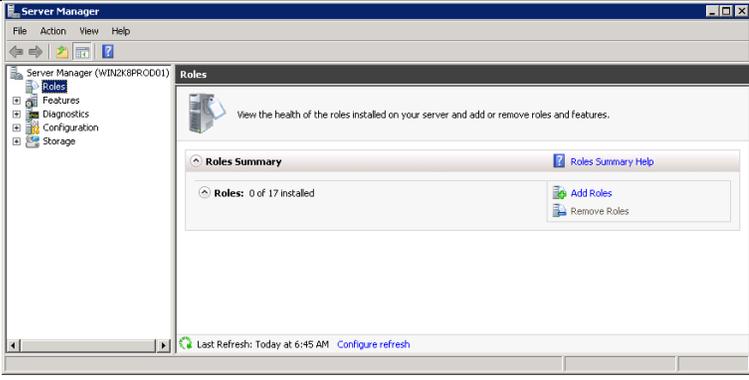
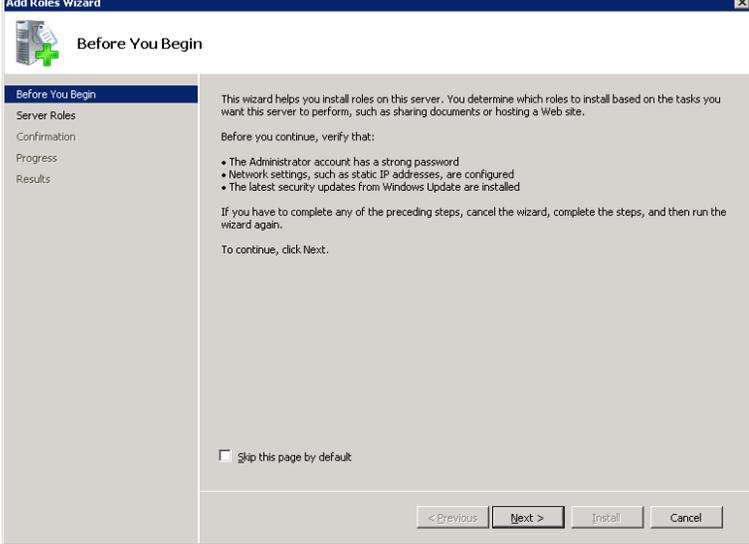
Configure MS Windows Remote Desktop Services

You will use MS Windows Remote Desktop Services for the implementation of JumpBox.

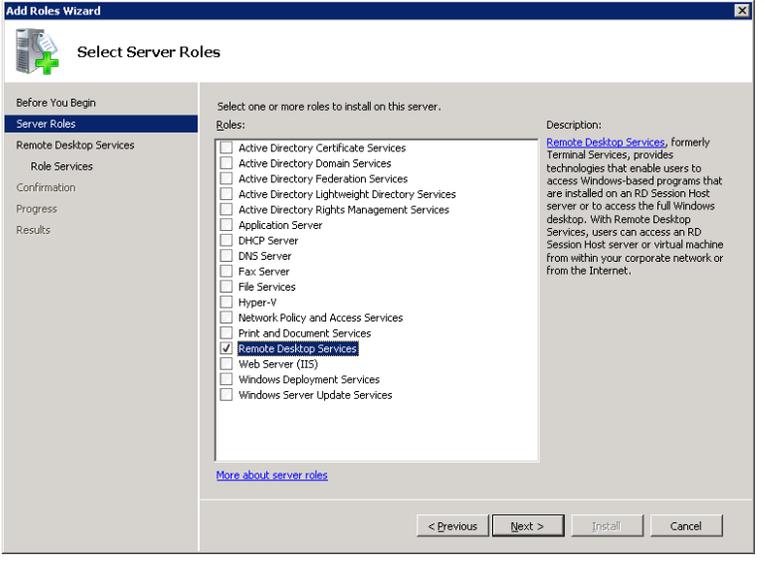
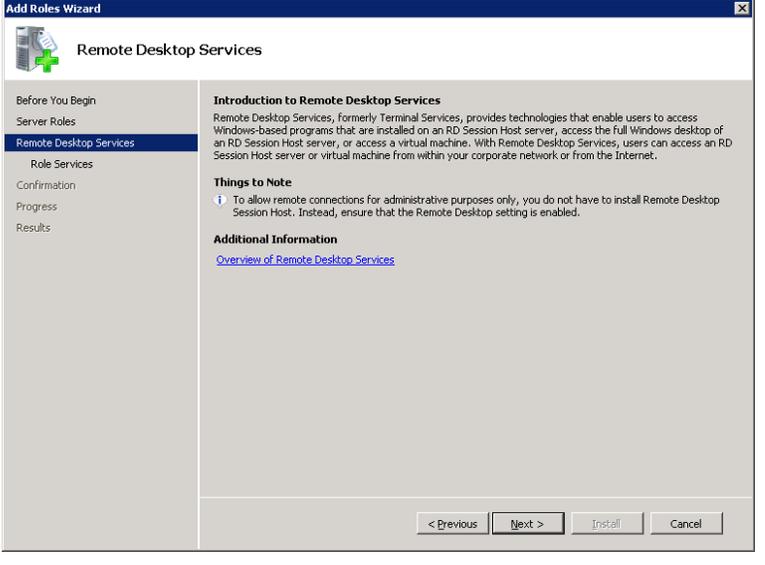
This chapter provides step by step instruction to install, configure and license the necessary components.

Please refer to the vendor documentation for any additional details or tuning and sizing information.

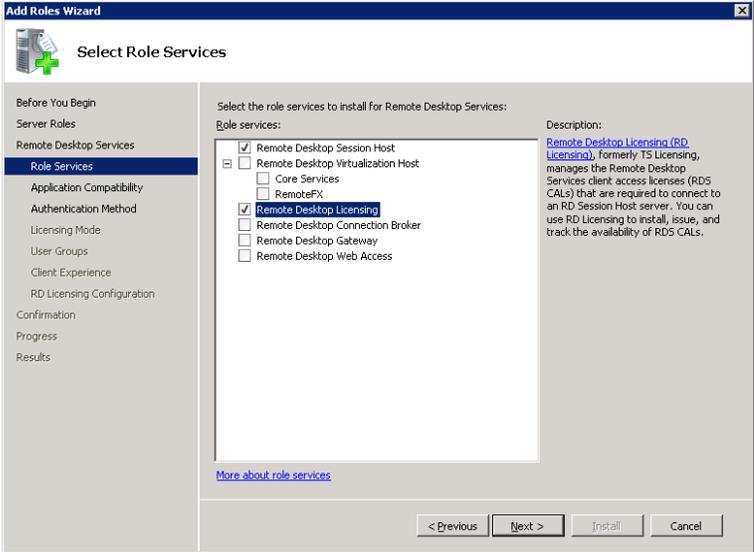
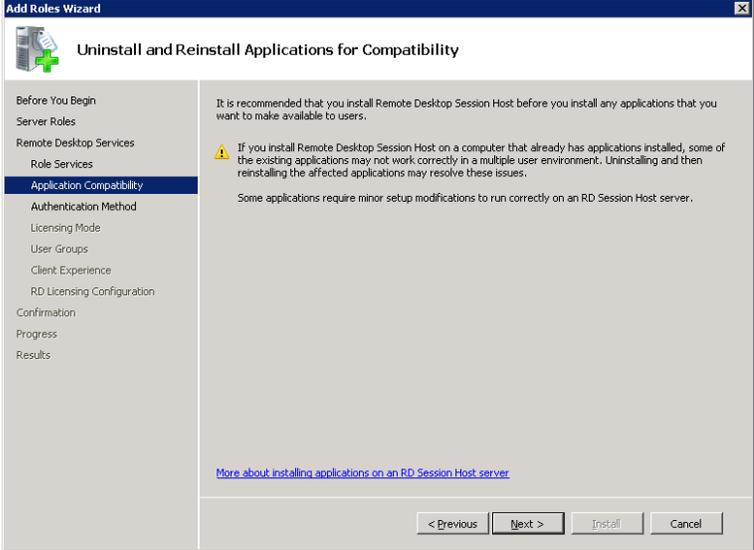
Log in to the server as a member of the Domain Admins group.

<p>Start the Windows Server Manager</p> <p>Navigate to Roles.</p> <p>Click Add Roles.</p>	 <p>The screenshot shows the Windows Server Manager console. The left-hand navigation pane is expanded to 'Roles'. The main pane displays the 'Roles' page, which includes a 'Roles Summary' section showing '0 of 17 installed' roles. There are 'Add Roles' and 'Remove Roles' buttons visible on the right side of the summary section.</p>
<p>Click Next.</p>	 <p>The screenshot shows the 'Add Roles Wizard' window at the 'Before You Begin' step. The wizard provides instructions on how to use it and lists prerequisites that must be verified before proceeding, such as having a strong password for the Administrator account and ensuring network settings and security updates are configured. At the bottom, there are 'Previous', 'Next', 'Install', and 'Cancel' buttons.</p>

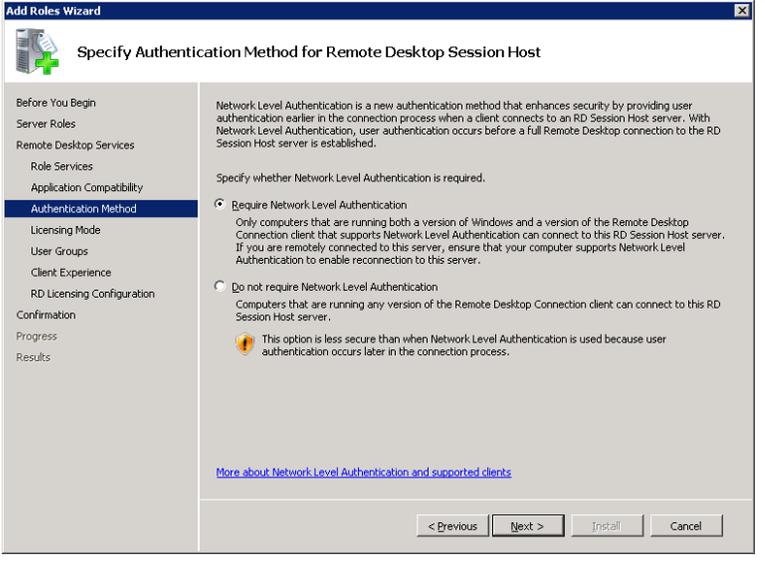
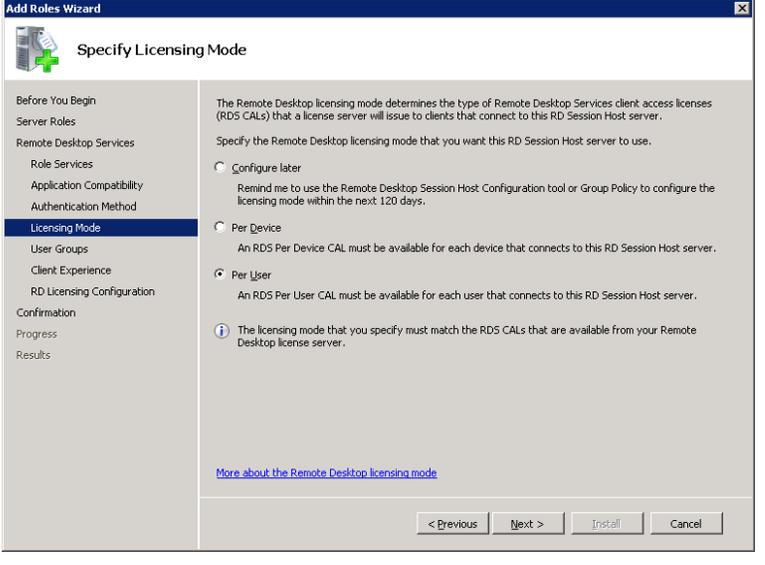
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Select Remote Desktop Services and click next.</p>	 <p>The screenshot shows the 'Add Roles Wizard' window with the title 'Select Server Roles'. On the left, a navigation pane lists 'Before You Begin', 'Server Roles', 'Remote Desktop Services', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The 'Server Roles' section is expanded, and 'Remote Desktop Services' is selected. The main area contains a list of roles with checkboxes. 'Remote Desktop Services' is checked. A description on the right explains that Remote Desktop Services, formerly Terminal Services, provides technologies for accessing Windows-based programs. At the bottom, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'.</p>
<p>Click Next.</p>	 <p>The screenshot shows the 'Add Roles Wizard' window with the title 'Remote Desktop Services'. The navigation pane on the left now highlights 'Remote Desktop Services'. The main area provides an 'Introduction to Remote Desktop Services', stating that it enables users to access Windows-based programs on an RD Session Host server or virtual machine. It also includes a 'Things to Note' section with a warning icon and text: 'To allow remote connections for administrative purposes only, you do not have to install Remote Desktop Session Host. Instead, ensure that the Remote Desktop setting is enabled.' Below this is an 'Additional Information' section with a link to 'Overview of Remote Desktop Services'. At the bottom, the same navigation buttons are present.</p>

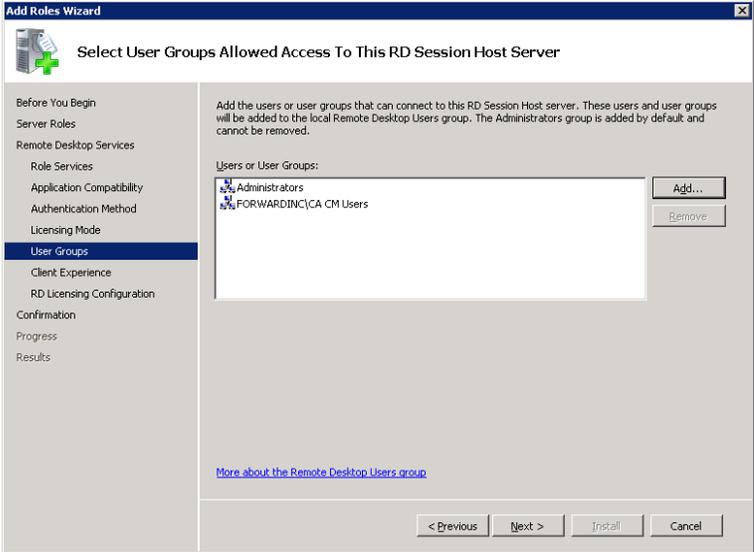
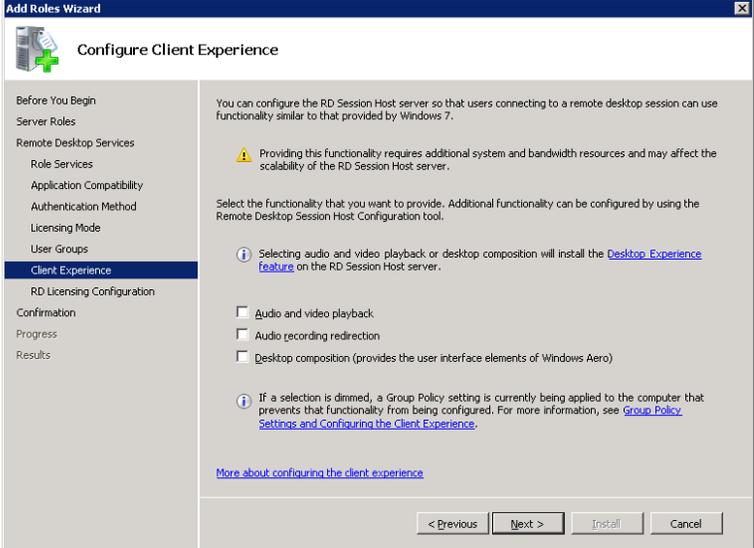
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Select Remote Desktop Session Host.</p> <p>If you do not already have Remote Desktop Licensing installed on another server you can install that on the same machine or other machine.</p>	
<p>Click Next.</p>	

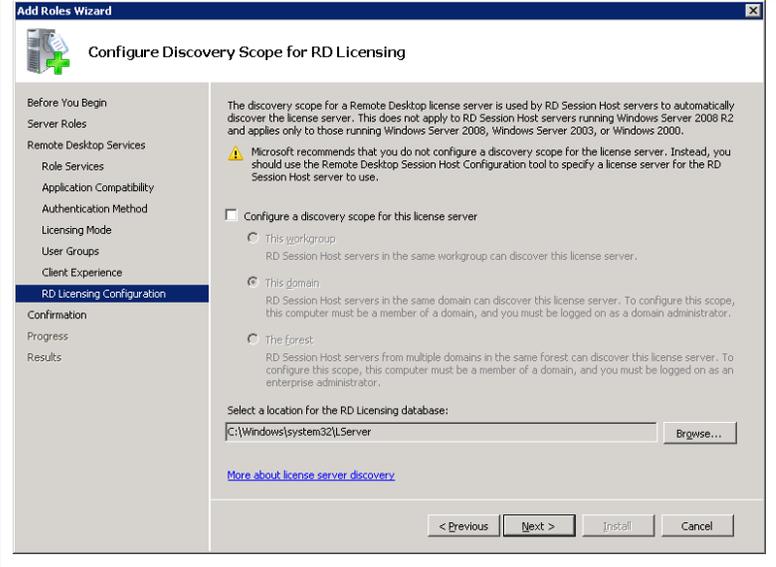
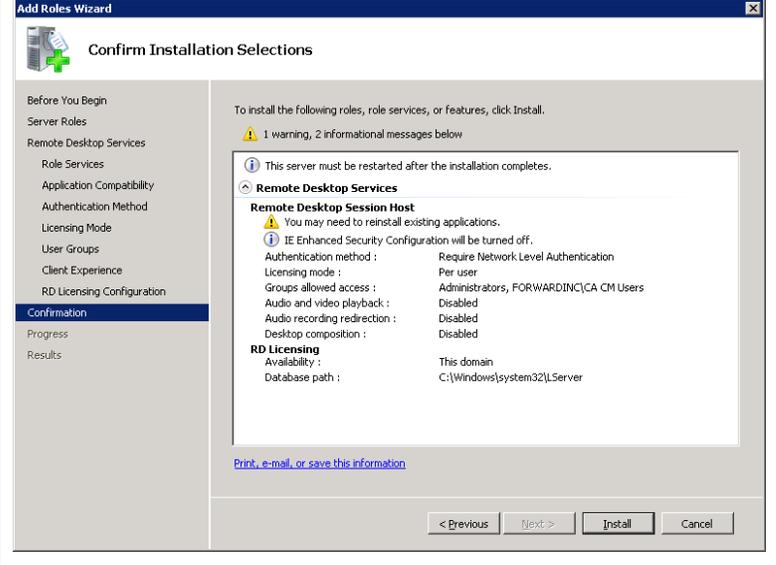
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Select if you want to use Network Layer Authentication and click Next.</p>	 <p>Add Roles Wizard</p> <p>Specify Authentication Method for Remote Desktop Session Host</p> <p>Before You Begin Server Roles Remote Desktop Services Role Services Application Compatibility Authentication Method Licensing Mode User Groups Client Experience RD Licensing Configuration Confirmation Progress Results</p> <p>Network Level Authentication is a new authentication method that enhances security by providing user authentication earlier in the connection process when a client connects to an RD Session Host server. With Network Level Authentication, user authentication occurs before a full Remote Desktop connection to the RD Session Host server is established.</p> <p>Specify whether Network Level Authentication is required.</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> Require Network Level Authentication Only computers that are running both a version of Windows and a version of the Remote Desktop Connection client that supports Network Level Authentication can connect to this RD Session Host server. If you are remotely connected to this server, ensure that your computer supports Network Level Authentication to enable reconnection to this server. <input type="radio"/> Do not require Network Level Authentication Computers that are running any version of the Remote Desktop Connection client can connect to this RD Session Host server. <p> This option is less secure than when Network Level Authentication is used because user authentication occurs later in the connection process.</p> <p>More about Network Level Authentication and supported clients</p> <p>< Previous Next > Install Cancel</p>
<p>Select your licensing method and click next.</p>	 <p>Add Roles Wizard</p> <p>Specify Licensing Mode</p> <p>Before You Begin Server Roles Remote Desktop Services Role Services Application Compatibility Licensing Mode User Groups Client Experience RD Licensing Configuration Confirmation Progress Results</p> <p>The Remote Desktop licensing mode determines the type of Remote Desktop Services client access licenses (RDS CALs) that a license server will issue to clients that connect to this RD Session Host server.</p> <p>Specify the Remote Desktop licensing mode that you want this RD Session Host server to use.</p> <ul style="list-style-type: none"> <input type="radio"/> Configure later Remind me to use the Remote Desktop Session Host Configuration tool or Group Policy to configure the licensing mode within the next 120 days. <input type="radio"/> Per Device An RDS Per Device CAL must be available for each device that connects to this RD Session Host server. <input checked="" type="radio"/> Per User An RDS Per User CAL must be available for each user that connects to this RD Session Host server. <p> The licensing mode that you specify must match the RDS CALs that are available from your Remote Desktop license server.</p> <p>More about the Remote Desktop licensing mode</p> <p>< Previous Next > Install Cancel</p>

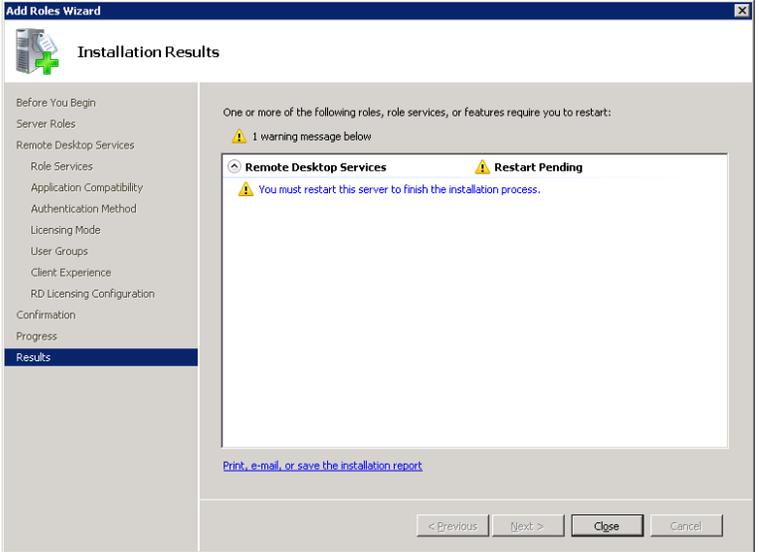
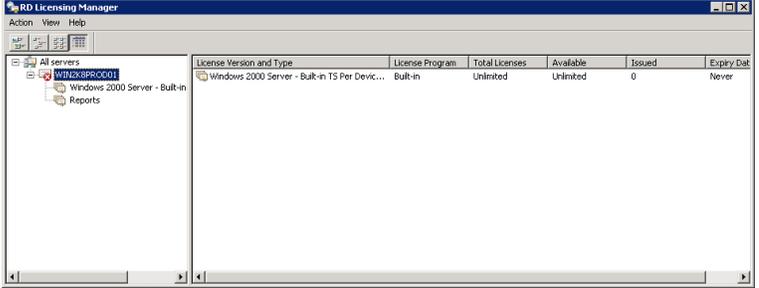
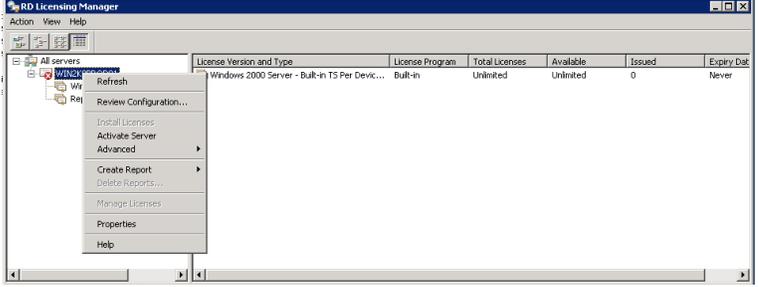
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

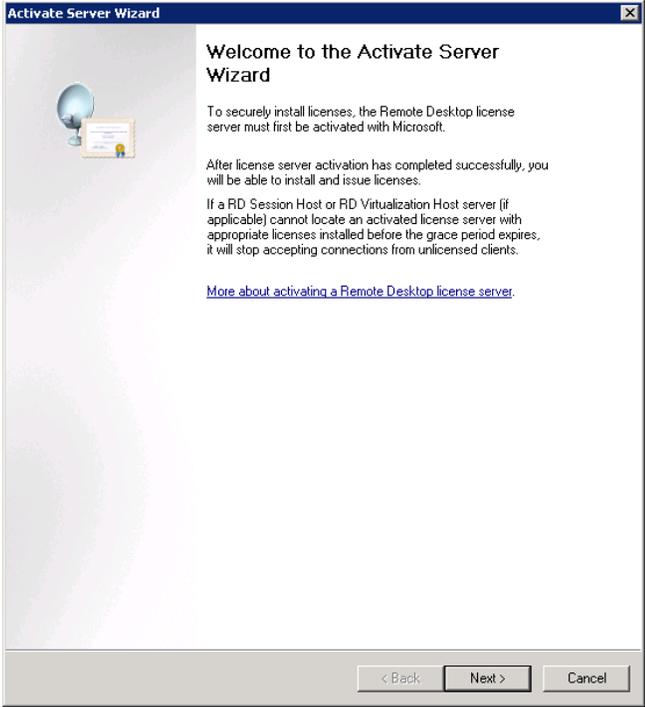
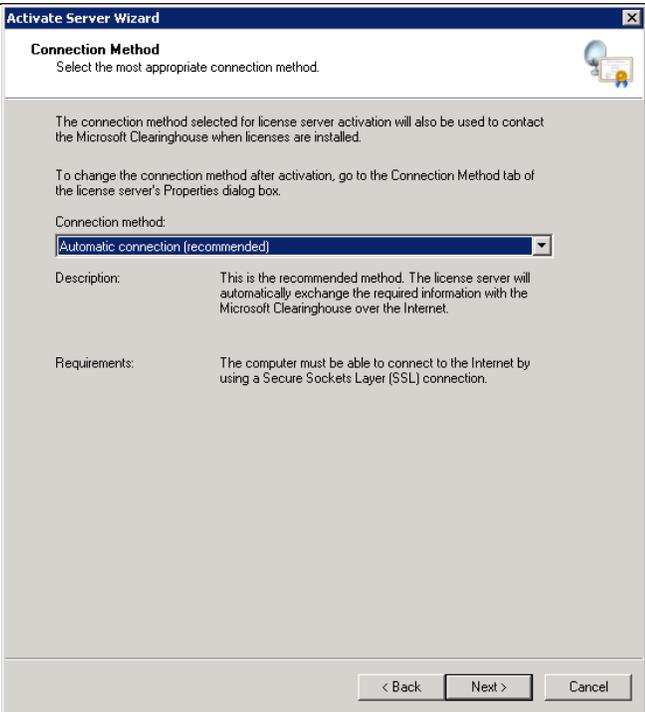
<p>Add the group that contains the CA ControlMinder Shared Account Management Users.</p> <p>Click Next.</p>	 <p>Add Roles Wizard</p> <p>Select User Groups Allowed Access To This RD Session Host Server</p> <p>Before You Begin Server Roles Remote Desktop Services Role Services Application Compatibility Authentication Method Licensing Mode User Groups Client Experience RD Licensing Configuration Confirmation Progress Results</p> <p>Add the users or user groups that can connect to this RD Session Host server. These users and user groups will be added to the local Remote Desktop Users group. The Administrators group is added by default and cannot be removed.</p> <p>Users or User Groups:</p> <ul style="list-style-type: none"> Administrators FORWARDING\CA CM Users <p>Buttons: Add..., Remove</p> <p>More about the Remote Desktop Users group</p> <p>Buttons: < Previous, Next >, Install, Cancel</p>
<p>The listed client experience features are not required by the CA ControlMinder SAM JumpBox. Click next to continue.</p>	 <p>Add Roles Wizard</p> <p>Configure Client Experience</p> <p>Before You Begin Server Roles Remote Desktop Services Role Services Application Compatibility Authentication Method Licensing Mode User Groups Client Experience RD Licensing Configuration Confirmation Progress Results</p> <p>You can configure the RD Session Host server so that users connecting to a remote desktop session can use functionality similar to that provided by Windows 7.</p> <p>Warning: Providing this functionality requires additional system and bandwidth resources and may affect the scalability of the RD Session Host server.</p> <p>Select the functionality that you want to provide. Additional functionality can be configured by using the Remote Desktop Session Host Configuration tool.</p> <p>Info: Selecting audio and video playback or desktop composition will install the Desktop Experience feature on the RD Session Host server.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Audio and video playback <input type="checkbox"/> Audio recording redirection <input type="checkbox"/> Desktop composition (provides the user interface elements of Windows Aero) <p>Info: If a selection is dimmed, a Group Policy setting is currently being applied to the computer that prevents that functionality from being configured. For more information, see Group Policy Settings and Configuring the Client Experience.</p> <p>More about configuring the client experience</p> <p>Buttons: < Previous, Next >, Install, Cancel</p>

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

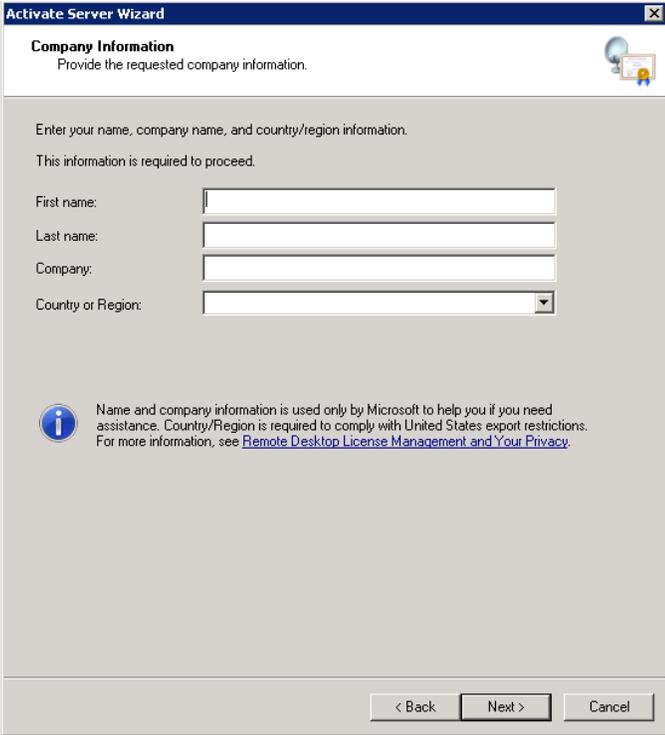
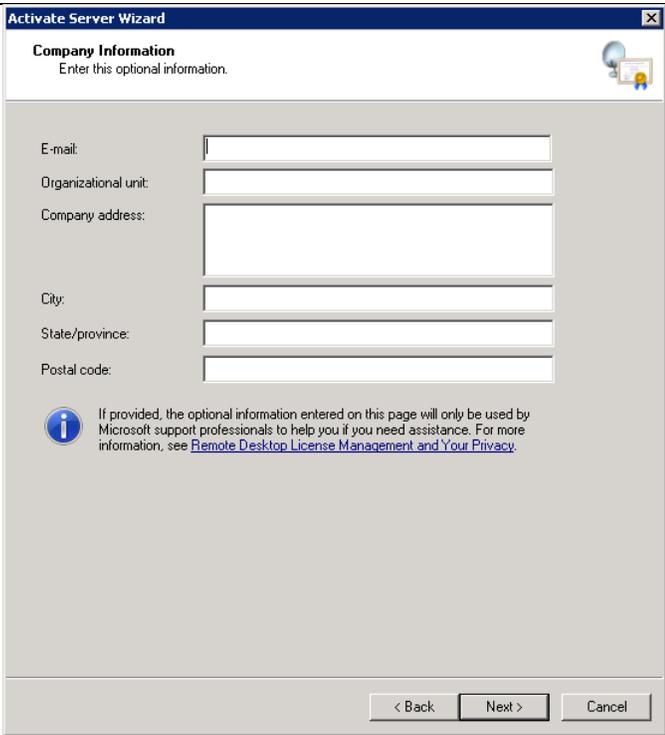
<p>Click Next.</p>	 <p>The screenshot shows the 'Add Roles Wizard' window with the title 'Configure Discovery Scope for RD Licensing'. The left-hand navigation pane includes 'Before You Begin', 'Server Roles', 'Remote Desktop Services', 'Role Services', 'Application Compatibility', 'Authentication Method', 'Licensing Mode', 'User Groups', 'Client Experience', 'RD Licensing Configuration' (which is selected), 'Confirmation', 'Progress', and 'Results'. The main content area contains the following text: 'The discovery scope for a Remote Desktop license server is used by RD Session Host servers to automatically discover the license server. This does not apply to RD Session Host servers running Windows Server 2008 R2 and applies only to those running Windows Server 2008, Windows Server 2003, or Windows 2000.' Below this is a warning icon and text: 'Microsoft recommends that you do not configure a discovery scope for the license server. Instead, you should use the Remote Desktop Session Host Configuration tool to specify a license server for the RD Session Host server to use.' There are three radio button options: 'This workgroup' (selected), 'This domain', and 'The forest'. A text box for 'Select a location for the RD Licensing database:' contains 'C:\Windows\system32\LServer' and a 'Browse...' button. At the bottom are '< Previous', 'Next >', 'Install', and 'Cancel' buttons.</p>
<p>Click Install.</p>	 <p>The screenshot shows the 'Add Roles Wizard' window with the title 'Confirm Installation Selections'. The left-hand navigation pane is identical to the previous screenshot, with 'RD Licensing Configuration' selected. The main content area contains the text: 'To install the following roles, role services, or Features, click Install.' Below this is a warning icon and text: '1 warning, 2 informational messages below'. A large white box contains the following information: 'This server must be restarted after the installation completes.' Under 'Remote Desktop Services', there is a warning icon and text: 'You may need to reinstall existing applications.' Under 'Remote Desktop Session Host', there is an information icon and text: 'IE Enhanced Security Configuration will be turned off.' A list of settings follows: 'Authentication method : Require Network Level Authentication', 'Licensing mode : Per user', 'Groups allowed access : Administrators, FORWARDING\CA CM Users', 'Audio and video playback : Disabled', 'Audio recording redirection : Disabled', and 'Desktop composition : Disabled'. Under 'RD Licensing', there is an information icon and text: 'Availability : This domain' and 'Database path : C:\Windows\system32\LServer'. At the bottom are '< Previous', 'Next >', 'Install', and 'Cancel' buttons.</p>

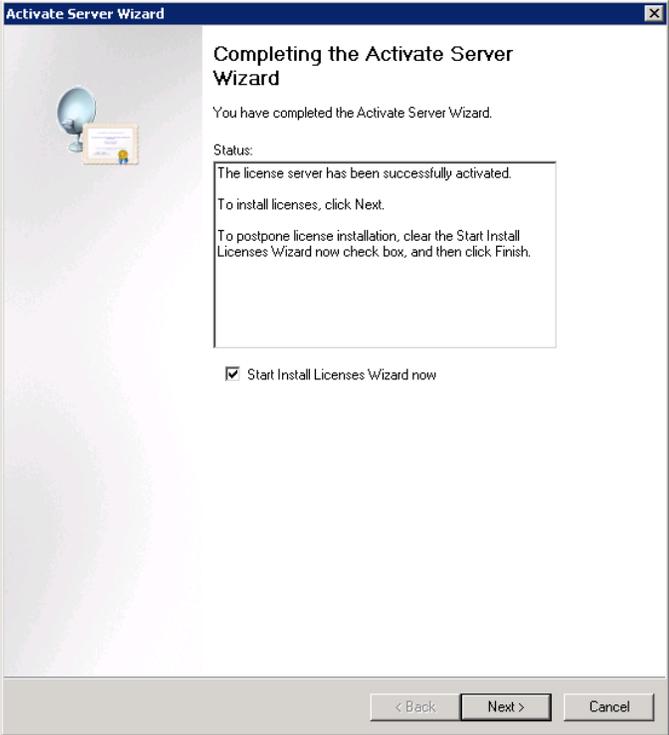
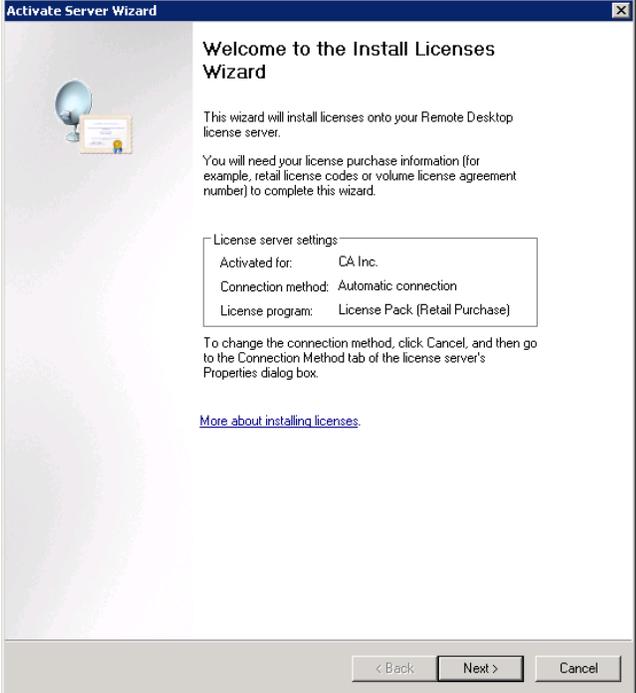
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Restart your server.</p>													
<p>Start Remote Desktop Licensing Manager Configuration from Start/Administrative Tools/Remote Desktop Services</p>	 <table border="1" data-bbox="678 926 1437 1157"> <thead> <tr> <th>License Version and Type</th> <th>License Program</th> <th>Total Licenses</th> <th>Available</th> <th>Issued</th> <th>Expiry Date</th> </tr> </thead> <tbody> <tr> <td>Windows 2000 Server - Built-in TS Per Devic...</td> <td>Built-in</td> <td>Unlimited</td> <td>Unlimited</td> <td>0</td> <td>Never</td> </tr> </tbody> </table>	License Version and Type	License Program	Total Licenses	Available	Issued	Expiry Date	Windows 2000 Server - Built-in TS Per Devic...	Built-in	Unlimited	Unlimited	0	Never
License Version and Type	License Program	Total Licenses	Available	Issued	Expiry Date								
Windows 2000 Server - Built-in TS Per Devic...	Built-in	Unlimited	Unlimited	0	Never								
<p>Right Click on the server and select Activate Server.</p>													

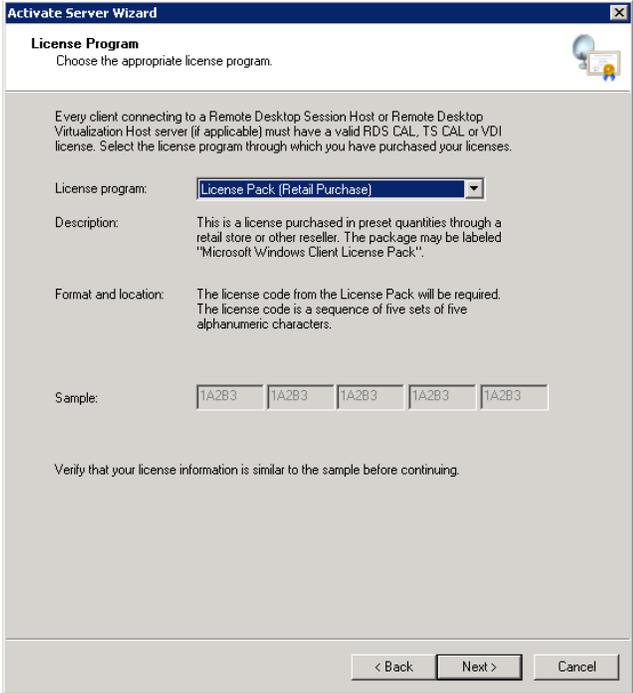
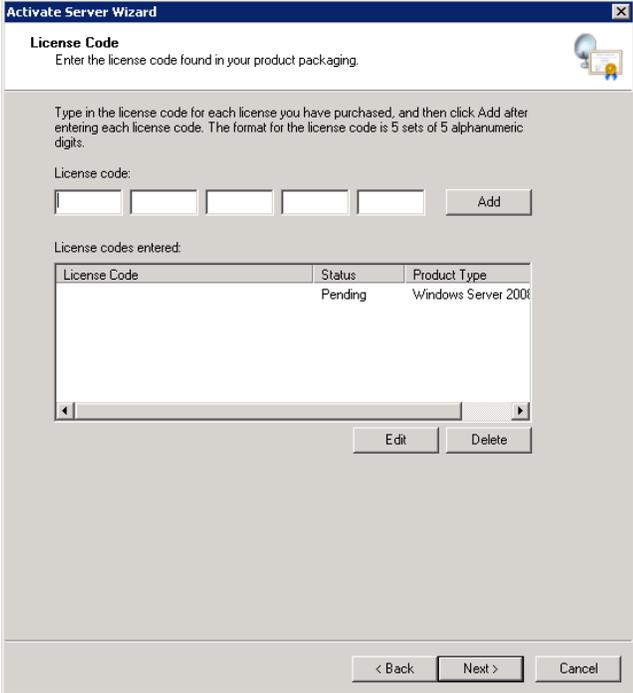
<p>Click Next.</p>	
<p>Select the connection method and click Next.</p>	

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

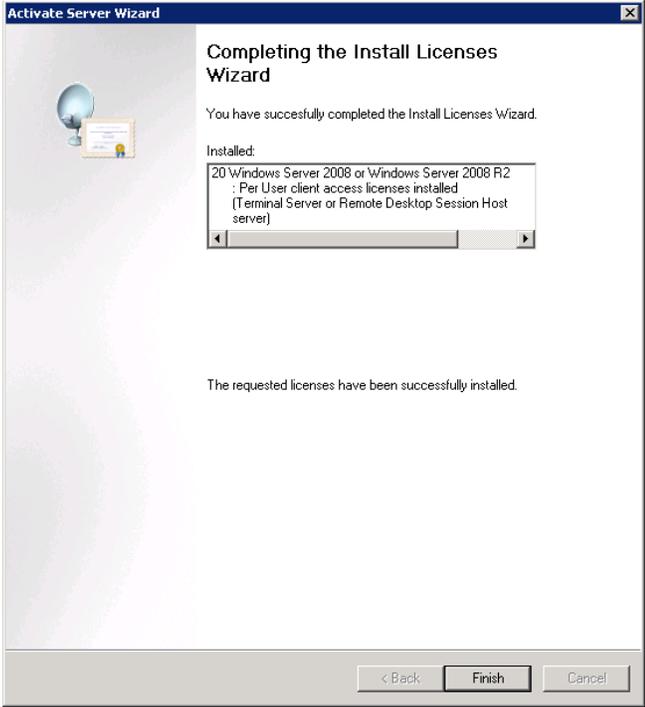
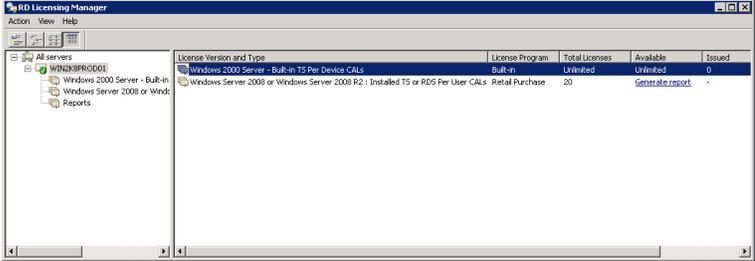
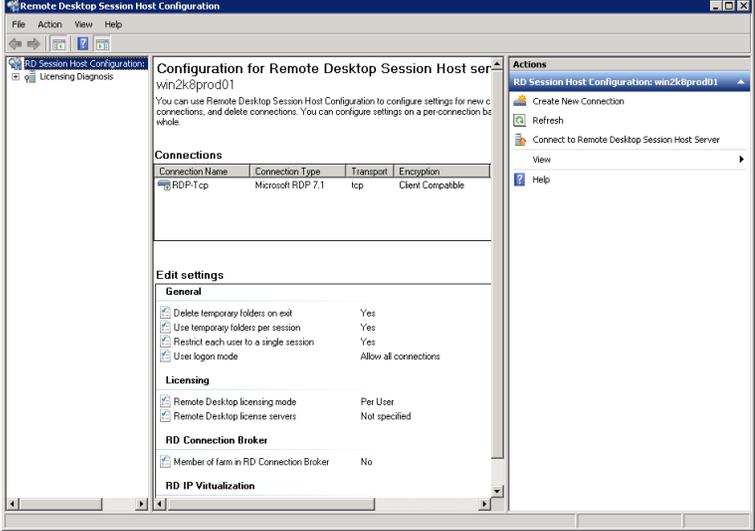
<p>Provide your company information.</p>	
<p>Provide your contact information and click Next.</p>	

<p>Click Next to start the Install Licenses Wizard.</p>	
<p>Click Next.</p>	

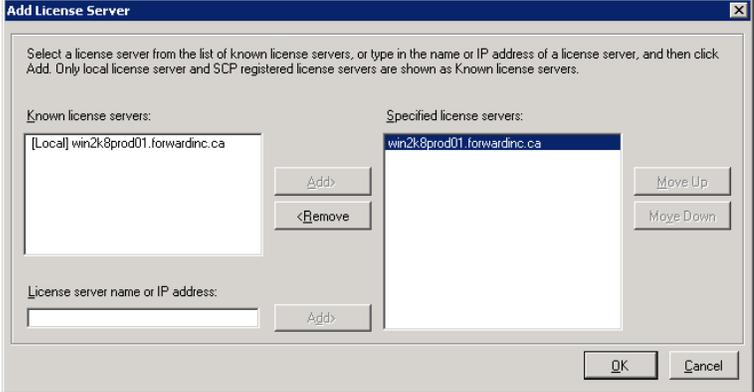
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Click Next.</p>	
<p>Add a license and click Next.</p>	

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Click Finish.</p>																
<p>Your RD Licensing Manger should be activated now and there should be a valid license displayed.</p>	 <table border="1" data-bbox="852 1073 1422 1115"> <thead> <tr> <th>License Version and Type</th> <th>License Program</th> <th>Total Licenses</th> <th>Available</th> <th>Issued</th> </tr> </thead> <tbody> <tr> <td>Windows 2000 Server - Built-in TS Per Device CALs</td> <td>Built-in</td> <td>Unlimited</td> <td>Unlimited</td> <td>0</td> </tr> <tr> <td>Windows Server 2008 or Windows Server 2008 R2 : Installed TS or RDS Per User CALs - Retail Purchase</td> <td>Retail Purchase</td> <td>20</td> <td>Unlimited</td> <td>0</td> </tr> </tbody> </table>	License Version and Type	License Program	Total Licenses	Available	Issued	Windows 2000 Server - Built-in TS Per Device CALs	Built-in	Unlimited	Unlimited	0	Windows Server 2008 or Windows Server 2008 R2 : Installed TS or RDS Per User CALs - Retail Purchase	Retail Purchase	20	Unlimited	0
License Version and Type	License Program	Total Licenses	Available	Issued												
Windows 2000 Server - Built-in TS Per Device CALs	Built-in	Unlimited	Unlimited	0												
Windows Server 2008 or Windows Server 2008 R2 : Installed TS or RDS Per User CALs - Retail Purchase	Retail Purchase	20	Unlimited	0												
<p>Start Remote Desktop Session Host Configuration from Start/Administrative Tools/Remote Desktop Services. Double click Remote Desktop license servers.</p>																

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

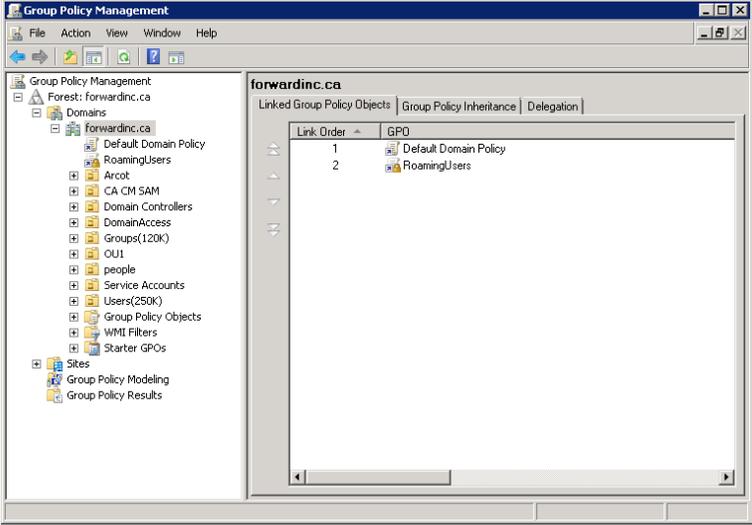
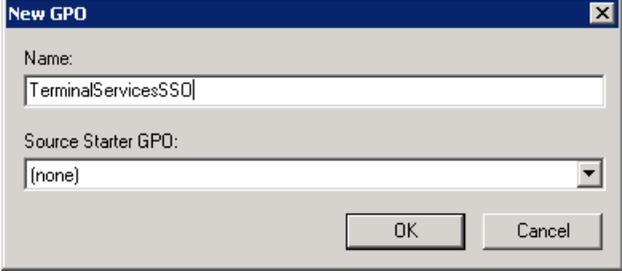
<p>Click Add.</p>	
<p>Add license server/servers available in your organization and click OK.</p> <p>Note that in MS Remote Desktop Session Host and Session server are on the same computer.</p>	

At this point, the Microsoft Remote Desktop Session host is now configured and licensed.

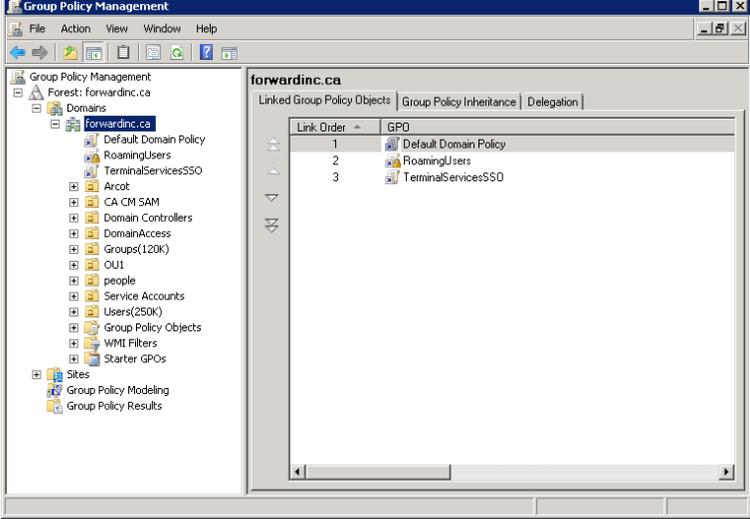
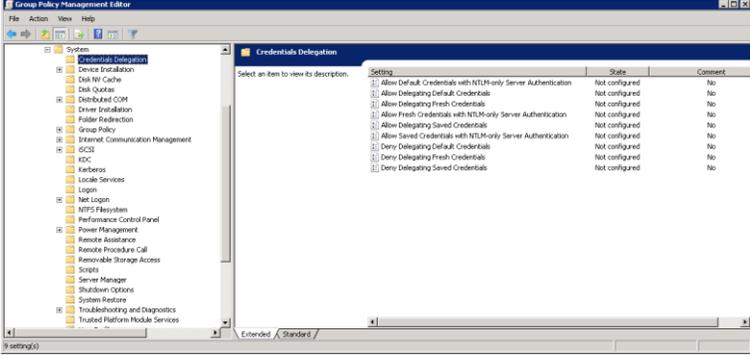
Enable Single Sign-On For Terminal Server Connections

If you use the same user name and password to log in to your computer and to the MS Remote Desktop Session then you can enable single sign-on that will allow you to log into the JB without an additional authentication challenge.

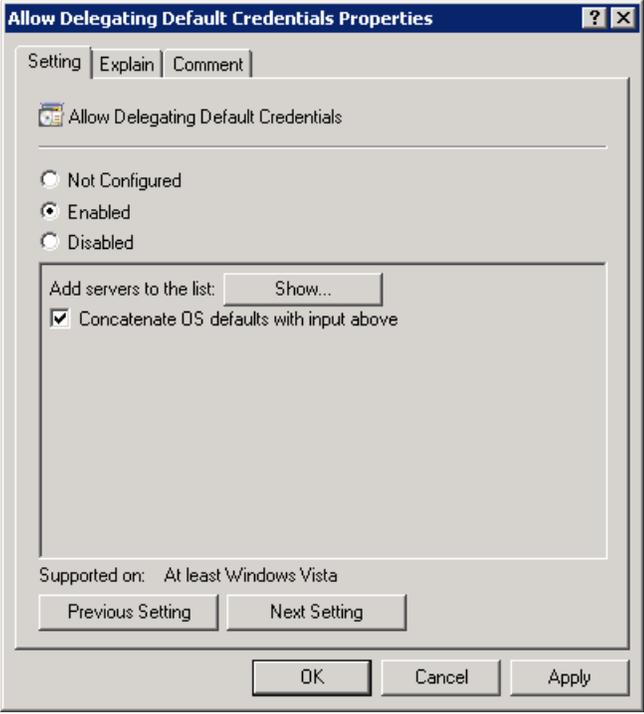
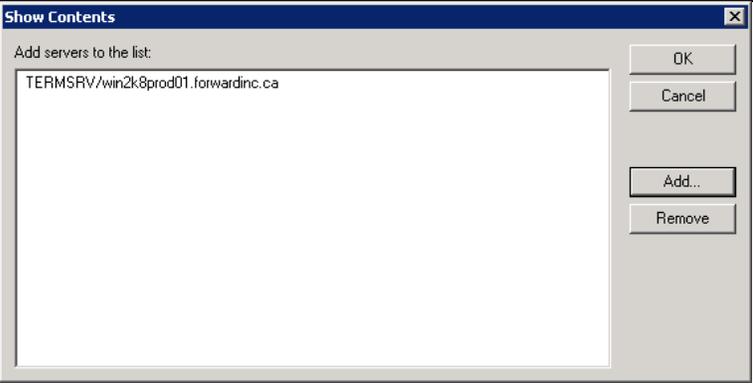
Single Sign-On is enabled through a Domain Group Policy.

<p>Log on to your machine where Group Policy Management Console is installed as an administrator.</p> <p>Start Group Policy Management Console - "gpmc.msc".</p>	
<p>Use can modify an existing group policy or create a new one. We will create a new Group Policy names TerminalServicesSSO and link it at the domain level.</p>	

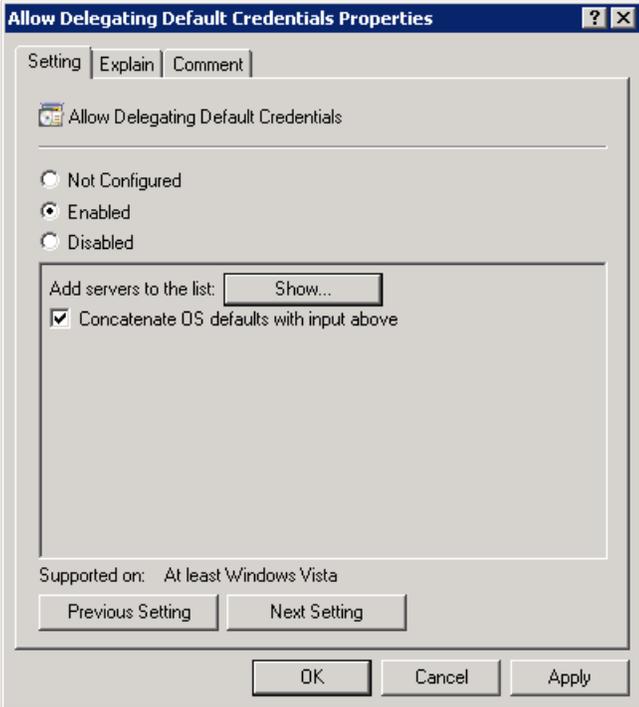
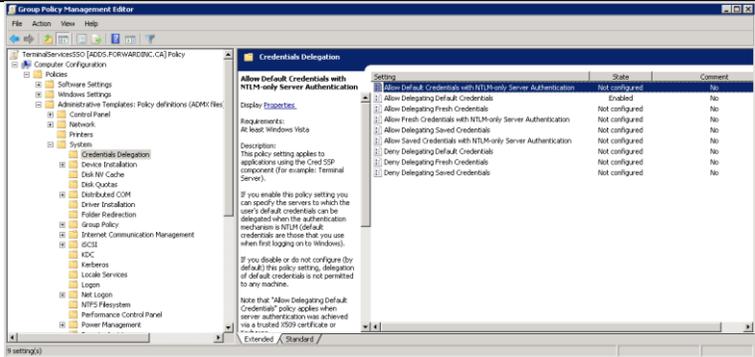
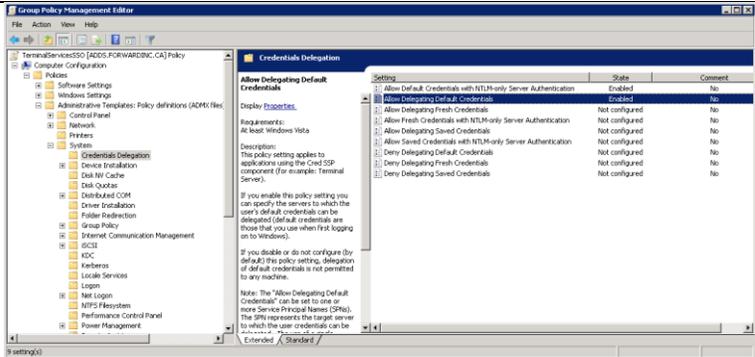
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Right click on the policy and select Edit.</p>																															
<p>Navigate to "Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation" and select and double click "Allow Delegating Default Credentials"</p>	 <table border="1" data-bbox="889 905 1404 1197"> <thead> <tr> <th>Setting</th> <th>Status</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>Allow Default Credentials with NTLM-only Server Authentication</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>Allow Delegating Default Credentials</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>Allow Delegating Fresh Credentials</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>Allow Fresh Credentials with NTLM-only Server Authentication</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>Allow Delegating Samed Credentials</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>Allow Saved Credentials with NTLM-only Server Authentication</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>Deny Delegating Default Credentials</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>Deny Delegating Fresh Credentials</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>Deny Delegating Samed Credentials</td> <td>Not configured</td> <td>No</td> </tr> </tbody> </table>	Setting	Status	Comment	Allow Default Credentials with NTLM-only Server Authentication	Not configured	No	Allow Delegating Default Credentials	Not configured	No	Allow Delegating Fresh Credentials	Not configured	No	Allow Fresh Credentials with NTLM-only Server Authentication	Not configured	No	Allow Delegating Samed Credentials	Not configured	No	Allow Saved Credentials with NTLM-only Server Authentication	Not configured	No	Deny Delegating Default Credentials	Not configured	No	Deny Delegating Fresh Credentials	Not configured	No	Deny Delegating Samed Credentials	Not configured	No
Setting	Status	Comment																													
Allow Default Credentials with NTLM-only Server Authentication	Not configured	No																													
Allow Delegating Default Credentials	Not configured	No																													
Allow Delegating Fresh Credentials	Not configured	No																													
Allow Fresh Credentials with NTLM-only Server Authentication	Not configured	No																													
Allow Delegating Samed Credentials	Not configured	No																													
Allow Saved Credentials with NTLM-only Server Authentication	Not configured	No																													
Deny Delegating Default Credentials	Not configured	No																													
Deny Delegating Fresh Credentials	Not configured	No																													
Deny Delegating Samed Credentials	Not configured	No																													

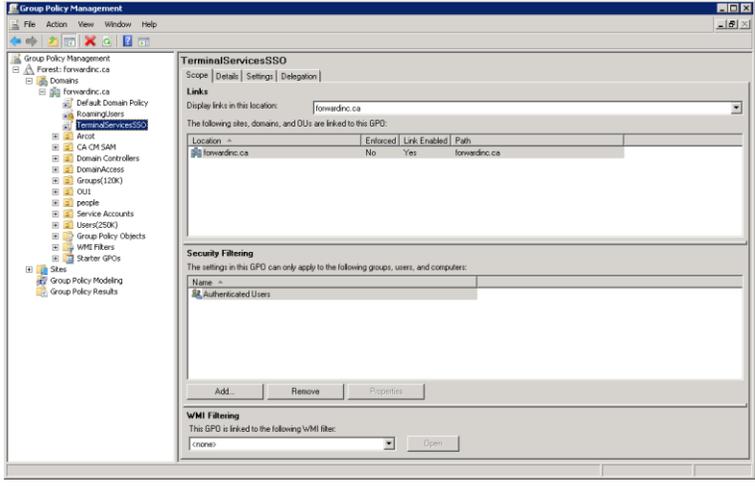
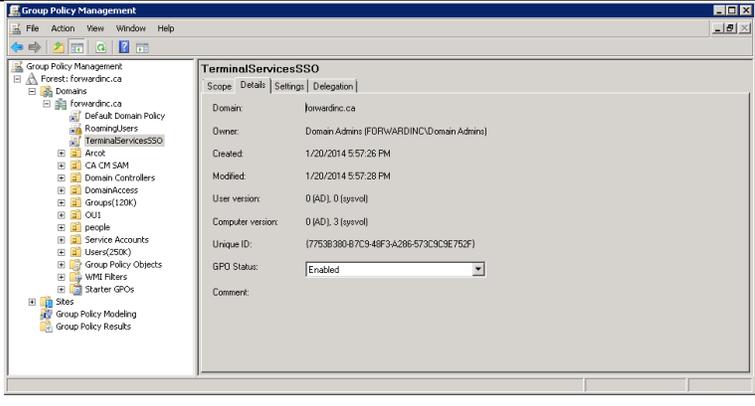
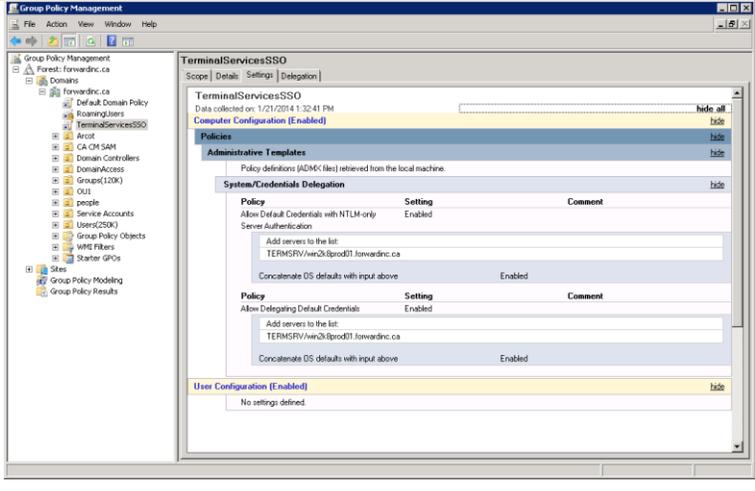
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Select "Enabled", Click Show next to add servers to the list.</p>	
<p>Add your JumpBox server to the list. User TERMSRV\servername format. Click OK.</p>	

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Click OK to accept the changes.</p>	
<p>If the server you are connecting to cannot be authenticated via Kerberos or SSL certificate, Single Sign-On will not work. You can circumvent this restriction by enabling "Allow Default Credentials with NTLM-only Server Authentication" policy, which is less secure. (NTLM-only Server Authentication is less secure compared to using Certificates or Kerberos.)</p>	
<p>Follow the same steps to enable "Allow Default Credentials with NTLM-only Server Authentication" as for "Allow Delegating Default Credentials". If you want to enable this option.</p>	

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Navigate to Group Policy Management and go to the policy you created/modified and validate the policy scope applies to users of ControlMinder SAM. The scope is “Authenticated Users” by default for a new policy.</p>	
<p>Navigate to Details tab validate that it is enabled.</p>	
<p>Navigate to Settings and click show all. Validate that the settings are correct.</p>	

The new Group Policy is applied during the next policy refresh interval or when the computer is rebooted.

Configure The Enterprise Management Server For Integrated Windows Authentication

By default, users log into CA ControlMinder Enterprise Management by providing their account credentials in the login page. If the ENTM user datastore is embedded then the credentials are maintained in the ENTM internal repository. If the user datastore is Microsoft Active Directory then the credentials are maintained in AD.

If you specified to use AD as the user store then you may configure the Enterprise Management Server to support Integrated Windows Authentication (IWA) which will enable login to the CA ControlMinder Enterprise Management Web UI using the user's domain account credentials from the user's current Windows session.

If you wish to configure the integrated MS AD authentication follow "Configuring the Enterprise Management Server for Integrated Windows Authentication" document ID TEC583462 knowledge base article available on support.ca.com.

Search for **TEC583462** on support.ca.com to find the document.

Create A Remote App For CM ENTM

RemoteApp enables you to make programs that are accessed remotely through Remote Desktop Services appear as if they are running on the end user's local computer. These programs are referred to as RemoteApp programs. Instead of being presented to the user in the desktop of the Remote Desktop Session Host (RD Session Host) server, the RemoteApp program is integrated with the client's desktop. The RemoteApp program runs in its own resizable window, can be dragged between multiple monitors, and has its own entry in the taskbar.

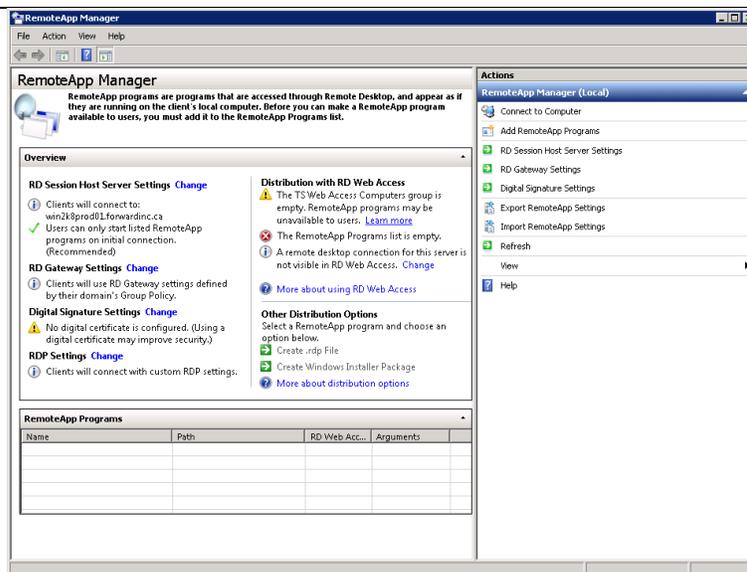
CA ControlMinder web interface can be configured as a RemoteApp on the JumpBox server so the end user can easily access the SAM functionality.

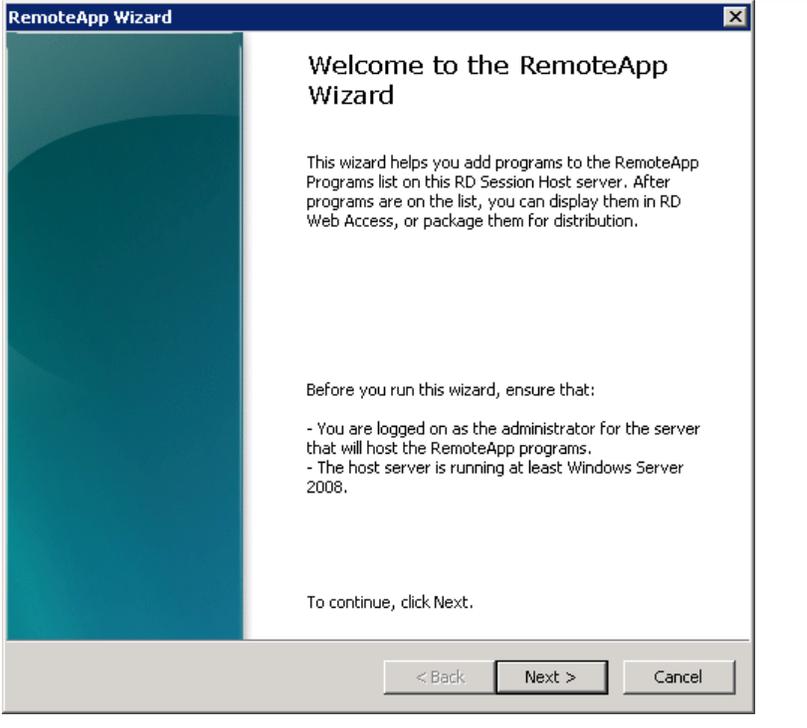
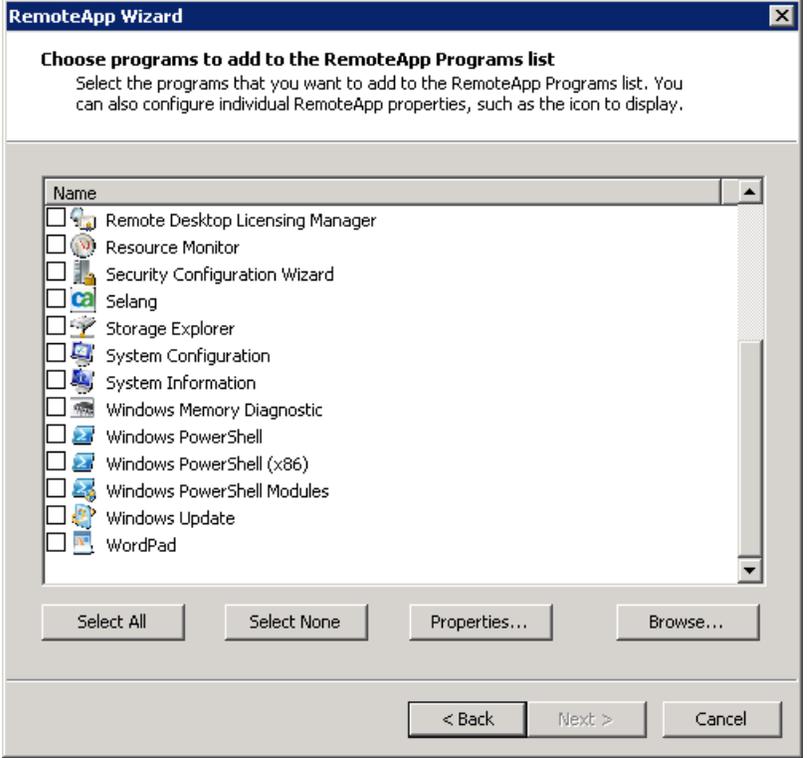
Follow the steps detailed below to create a RemoteApp.

Connect to the JumpBox server.

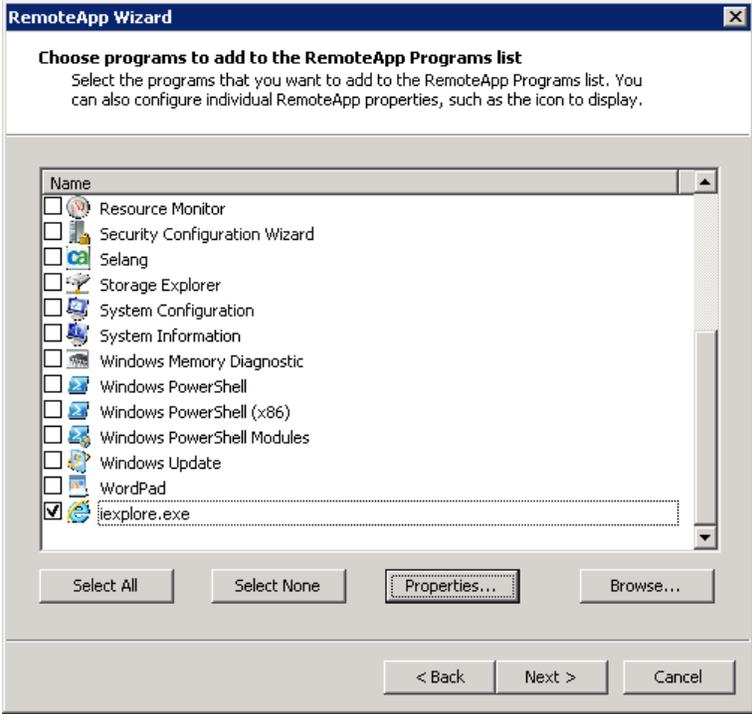
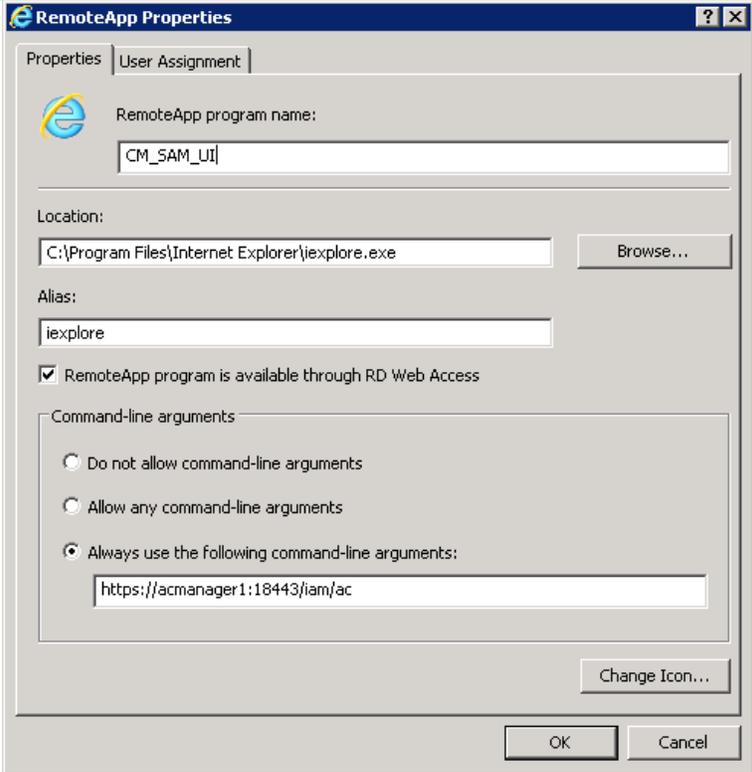
Applications are configured as RemoteApp using the TS RemoteApp Manager tool.

This can be accessed either from the Start -> All Programs -> Terminal Services -> TS Remote App Manager or by running remoteprograms.msc in a Run dialog or at a command prompt.

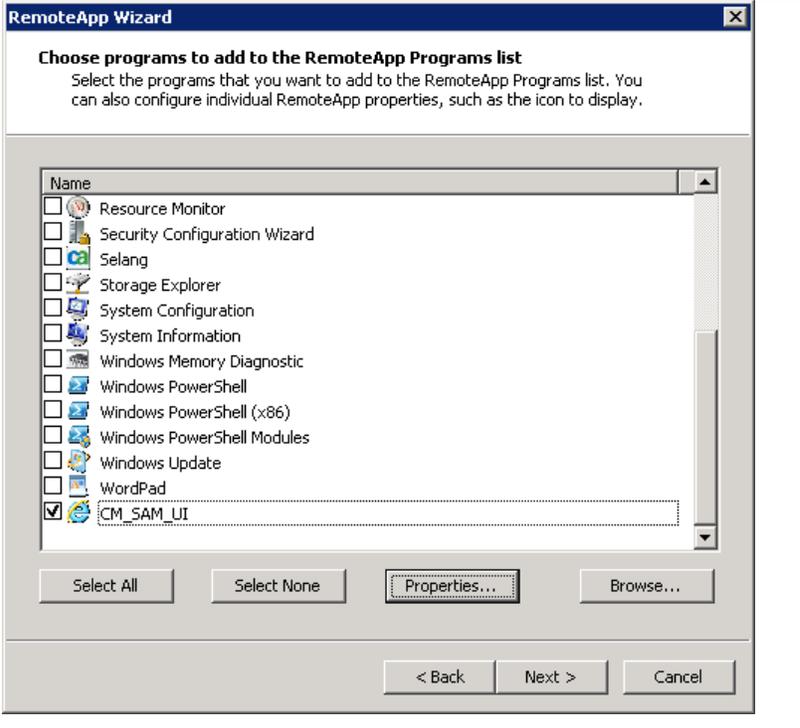
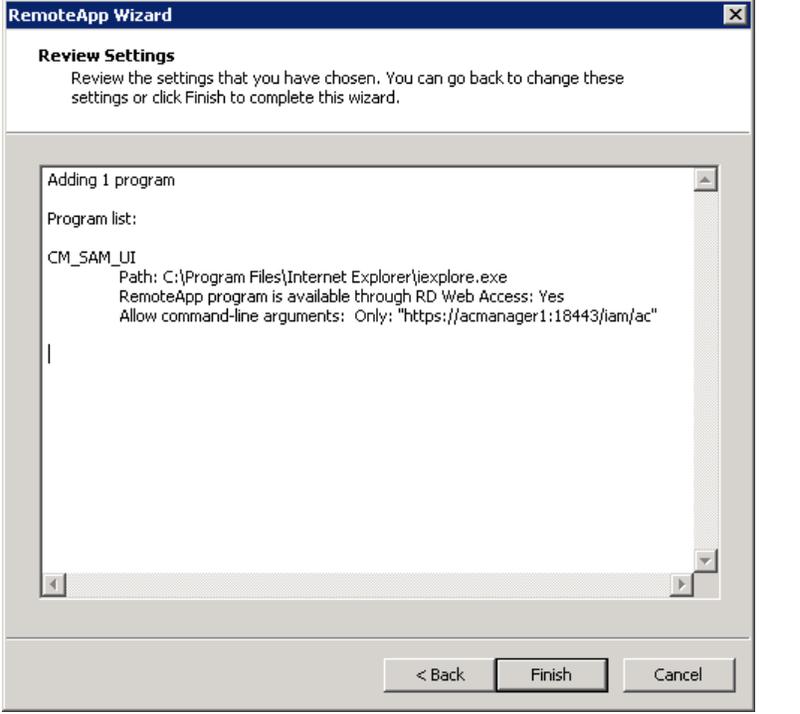


<p>Click "Add RemoteApp Program". This will open RemoteApp Wizard. Click Next to continue.</p>	 <p>The screenshot shows the 'RemoteApp Wizard' window with the title 'Welcome to the RemoteApp Wizard'. The text inside reads: 'This wizard helps you add programs to the RemoteApp Programs list on this RD Session Host server. After programs are on the list, you can display them in RD Web Access, or package them for distribution. Before you run this wizard, ensure that: - You are logged on as the administrator for the server that will host the RemoteApp programs. - The host server is running at least Windows Server 2008. To continue, click Next.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.</p>
<p>Browse for the internet browser you want to use. We will be using MS Internet Explorer for the purpose of this guide.</p>	 <p>The screenshot shows the 'RemoteApp Wizard' window with the title 'Choose programs to add to the RemoteApp Programs list'. The text inside reads: 'Select the programs that you want to add to the RemoteApp Programs list. You can also configure individual RemoteApp properties, such as the icon to display.' Below the text is a list box with a 'Name' header and a scroll bar. The list contains the following items, each with an unchecked checkbox: Remote Desktop Licensing Manager, Resource Monitor, Security Configuration Wizard, Selang, Storage Explorer, System Configuration, System Information, Windows Memory Diagnostic, Windows PowerShell, Windows PowerShell (x86), Windows PowerShell Modules, Windows Update, and WordPad. At the bottom of the list box are four buttons: 'Select All', 'Select None', 'Properties...', and 'Browse...'. At the bottom of the wizard window are three buttons: '< Back', 'Next >', and 'Cancel'.</p>

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Click Properties...</p>	
<p>Provide a program name. The program name that will appear to users.</p> <p>Specify the CM ENTM URL in the “Always use the following command-line arguments”.</p> <p>This means that this RemoteApp will start CM ENTM UI in MS Internet Explorer.</p> <p>Click OK.</p>	

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

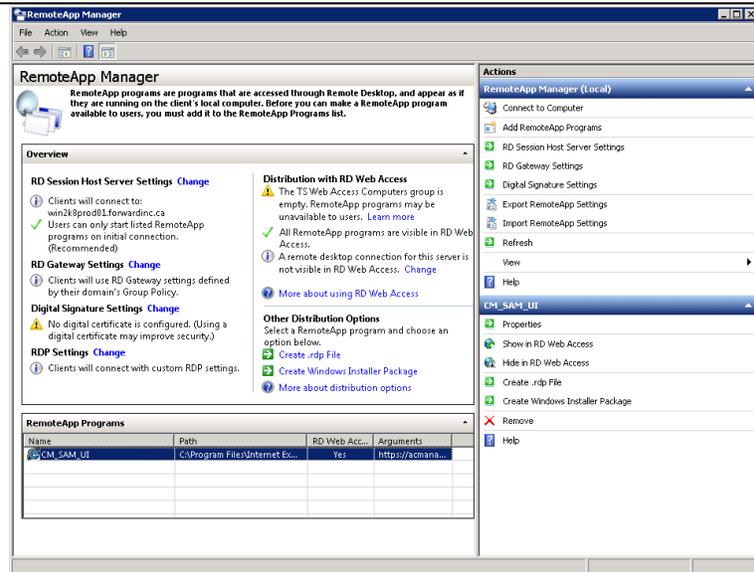
<p>Click Next.</p>	
<p>Review the settings and click Finish if they are correct.</p>	

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

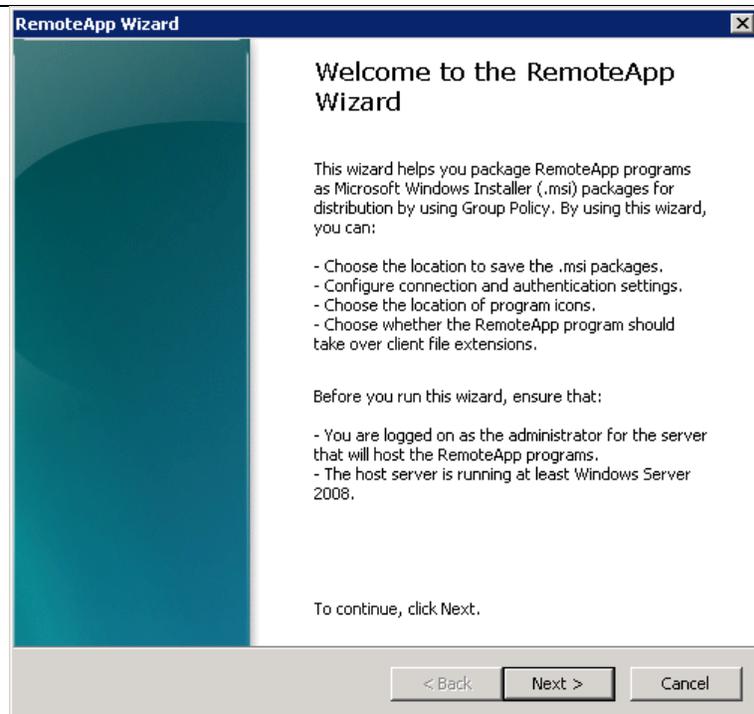
The new RemoteApp will appear in the list.

Right click on the application and select “Create Windows Installer Package.”

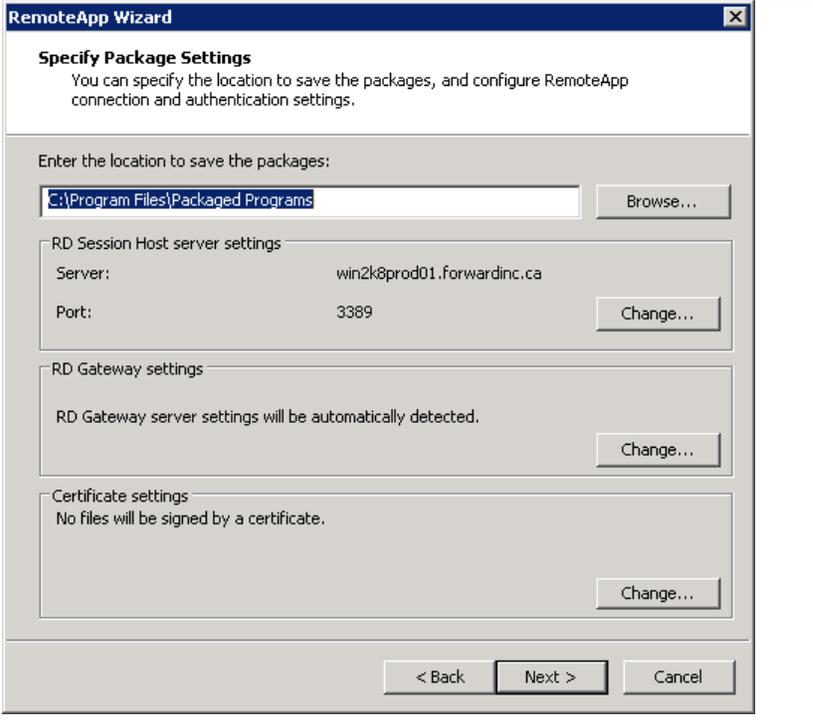
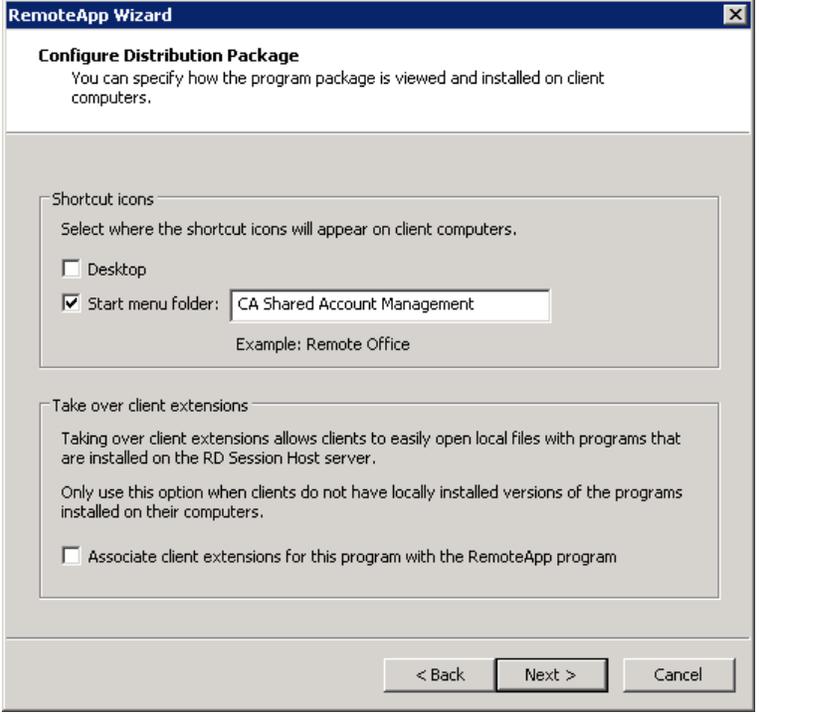
Note: You can also generate an .rdp file and distribute that to the end users.



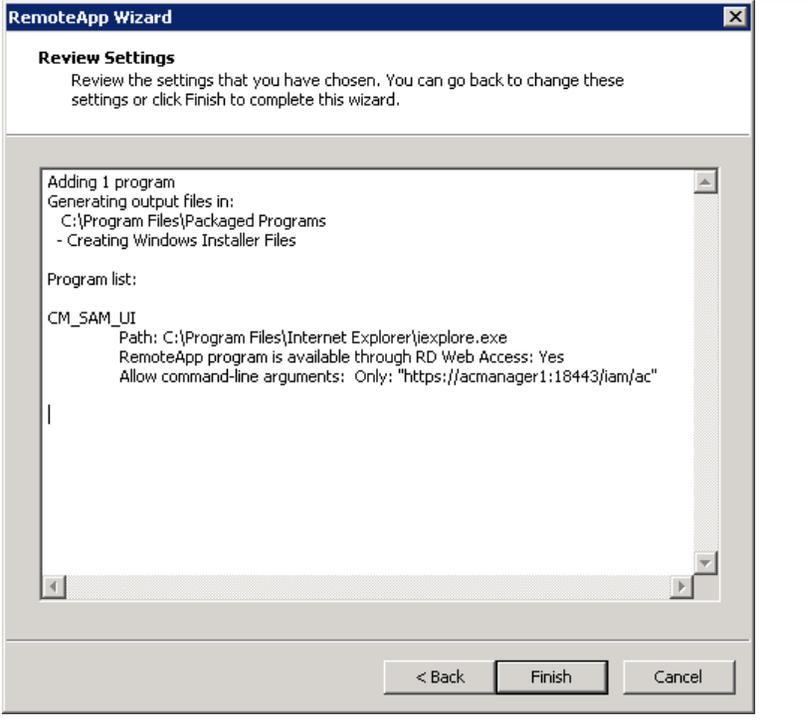
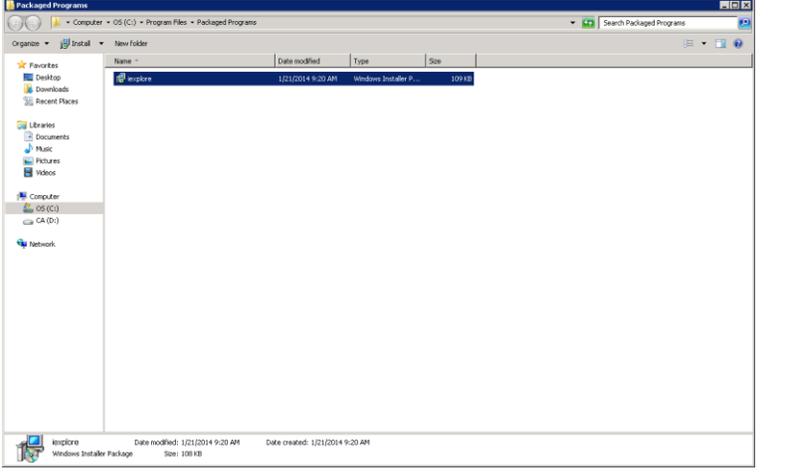
Click Next to start the wizard.



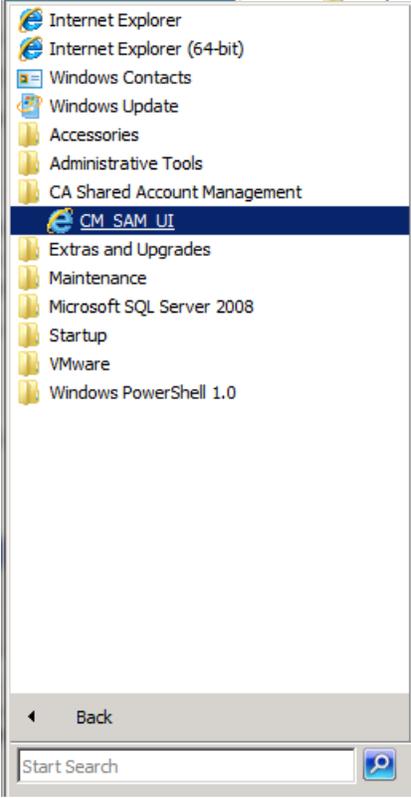
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Select the location to save the package to and click Next.</p>	 <p>RemoteApp Wizard</p> <p>Specify Package Settings You can specify the location to save the packages, and configure RemoteApp connection and authentication settings.</p> <p>Enter the location to save the packages: <input type="text" value="C:\Program Files\Packaged Programs"/> <input type="button" value="Browse..."/></p> <p>RD Session Host server settings Server: win2k8prod01.forwardinc.ca Port: 3389 <input type="button" value="Change..."/></p> <p>RD Gateway settings RD Gateway server settings will be automatically detected. <input type="button" value="Change..."/></p> <p>Certificate settings No files will be signed by a certificate. <input type="button" value="Change..."/></p> <p>< Back <input 108="" 378="" 491="" 835"="" type="button" value="Next > Cancel</p> </td> </tr> <tr> <td data-bbox="/> <p>Select if the program shortcut will be located on the Desktop or under the Start Menu.</p> <p>The configuration on the screenshot will create a shortcut under CA Shared Account Management.</p> <p>Click Next to continue.</p> </p>	 <p>RemoteApp Wizard</p> <p>Configure Distribution Package You can specify how the program package is viewed and installed on client computers.</p> <p>Shortcut icons Select where the shortcut icons will appear on client computers. <input type="checkbox"/> Desktop <input checked="" type="checkbox"/> Start menu folder: <input type="text" value="CA Shared Account Management"/> Example: Remote Office</p> <p>Take over client extensions Taking over client extensions allows clients to easily open local files with programs that are installed on the RD Session Host server. Only use this option when clients do not have locally installed versions of the programs installed on their computers. <input type="checkbox"/> Associate client extensions for this program with the RemoteApp program</p> <p>< Back <input 112="" 284="" 917="" 936"="" data-label="Page-Footer" type="button" value="Next > Cancel</p> </td> </tr> </table> </div> <div data-bbox="/> <p>CA Technologies, 2014</p> </p>
---	---	---

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

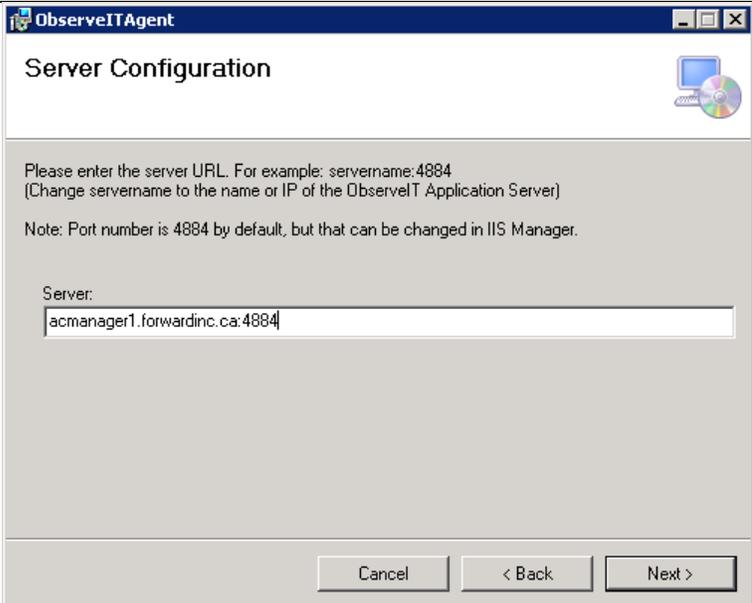
<p>Review the settings and click Finish.</p>	 <p>RemoteApp Wizard</p> <p>Review Settings Review the settings that you have chosen. You can go back to change these settings or click Finish to complete this wizard.</p> <p>Adding 1 program Generating output files in: C:\Program Files\Packaged Programs - Creating Windows Installer Files</p> <p>Program list: CM_SAM_UI Path: C:\Program Files\Internet Explorer\iexplore.exe RemoteApp program is available through RD Web Access: Yes Allow command-line arguments: Only: "https://acmanager1:18443/iam/ac"</p> <p>< Back Finish Cancel</p>								
<p>MS Installer Package will be created.</p>	 <p>Packaged Programs</p> <p>Computer > OS (C:) > Program Files > Packaged Programs</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Date modified</th> <th>Type</th> <th>Size</th> </tr> </thead> <tbody> <tr> <td>iexplore</td> <td>1/21/2014 9:20 AM</td> <td>Windows Installer P...</td> <td>109 KB</td> </tr> </tbody> </table> <p>File: iexplore Date modified: 1/21/2014 9:20 AM Date created: 1/21/2014 9:20 AM Size: 109 KB</p>	Name	Date modified	Type	Size	iexplore	1/21/2014 9:20 AM	Windows Installer P...	109 KB
Name	Date modified	Type	Size						
iexplore	1/21/2014 9:20 AM	Windows Installer P...	109 KB						

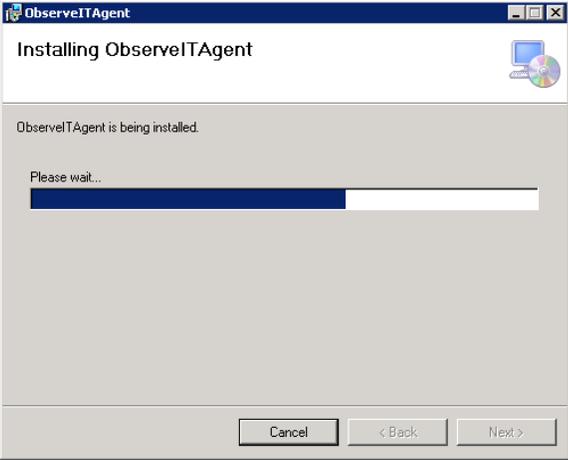
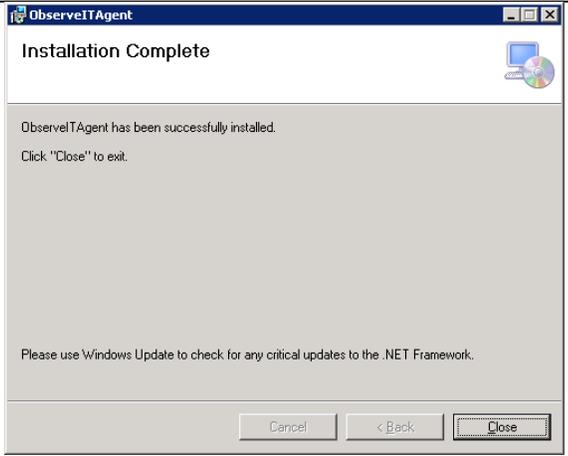
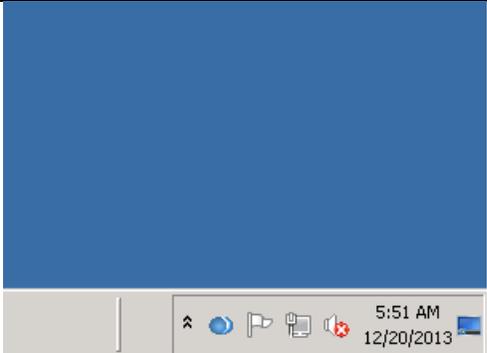
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Distribute and install this package on the end user workstation using the software distribution tool of your choice or manually.</p> <p>The RemoteApp will be available under Start Menu after installation.</p> <p>If you configured your MS Terminal Server for single sign on and ControlMinder for integrated MS Windows authentication then the RemoteApp will start CM user interface on the JumpBox and log you in automatically.</p>	 <p>The screenshot shows a Windows Start Menu with the following items listed: Internet Explorer, Internet Explorer (64-bit), Windows Contacts, Windows Update, Accessories, Administrative Tools, CA Shared Account Management, CM SAM UI (highlighted), Extras and Upgrades, Maintenance, Microsoft SQL Server 2008, Startup, VMware, and Windows PowerShell 1.0. At the bottom, there is a 'Back' button and a search box labeled 'Start Search'.</p>
---	--

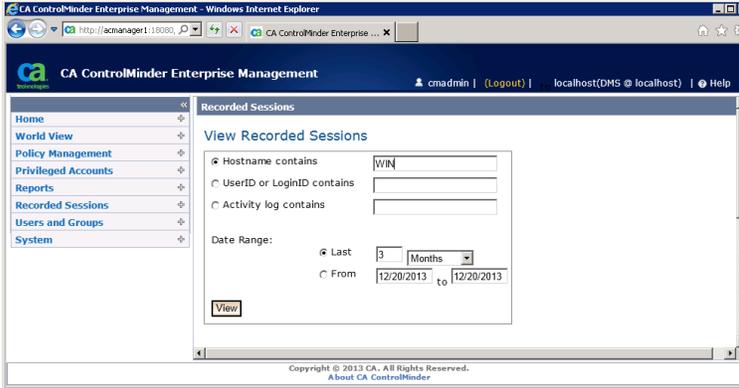
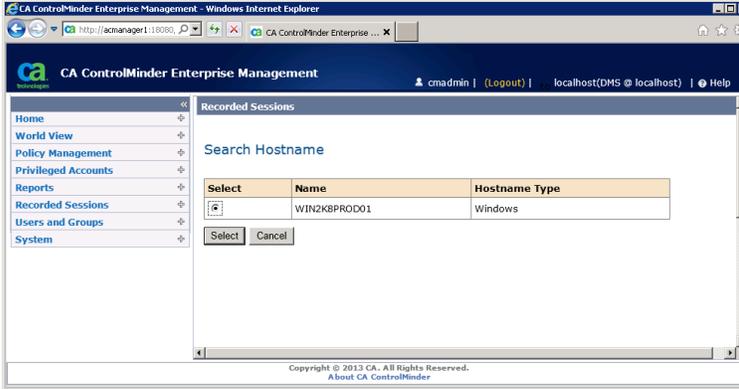
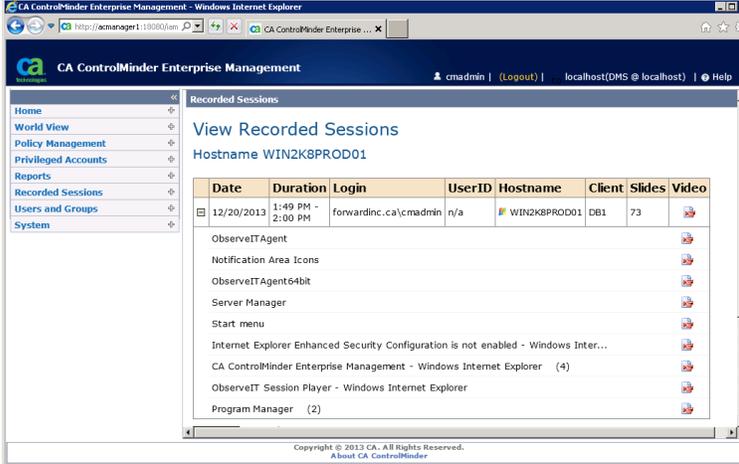
Install Session Recording Agent

You need to install CA Session Recording agent software on the JumpBox if you require recording of the privileged session.

<p>Run either the Setup.exe file or the ObserveIT.Agent.msi file, from the ObserveITAgent subdirectory that was created when you extracted the installation files.</p> <p>Use “Run As Administrator” option.</p> <p>The ObserveIT Agent Setup Wizard screen opens.</p>	
<p>Provide the url of the Session Recording server.</p>	

	
<p>Click Close to finish the installation.</p>	
<p>You will see a blue icon</p>  <p>on your taskbar that indicates that the session recording is running.</p> <p>All the sessions on this computer are being recorded from now on.</p> <p>This is the default configuration.</p>	

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

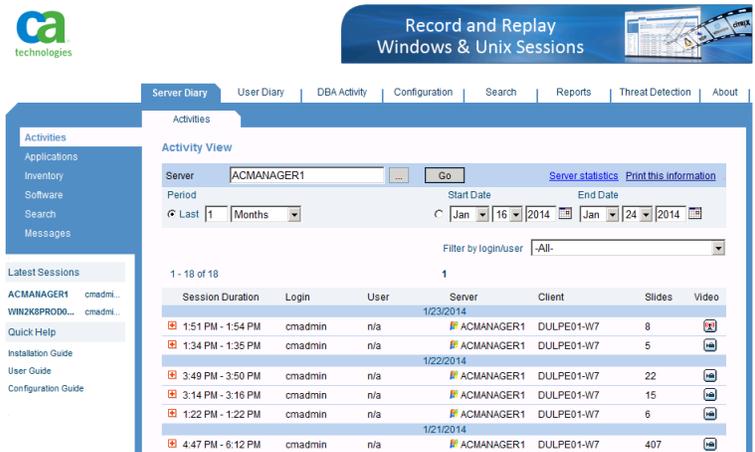
<p>Start CM ENTM and verify that all the sessions on the JumpBox are being recorded.</p> <p>Navigate to Recorded Sessions.</p> <p>Search for the hostname of your JumpBox.</p>																	
<p>Select your JumpBox.</p>	 <table border="1" data-bbox="857 884 1328 940"> <thead> <tr> <th>Select</th> <th>Name</th> <th>Hostname Type</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>WIN2K8PROD01</td> <td>Windows</td> </tr> </tbody> </table>	Select	Name	Hostname Type	<input type="checkbox"/>	WIN2K8PROD01	Windows										
Select	Name	Hostname Type															
<input type="checkbox"/>	WIN2K8PROD01	Windows															
<p>Verify that all the sessions initiated after the installation of the agent are being recorded.</p>	 <table border="1" data-bbox="857 1289 1370 1325"> <thead> <tr> <th>Date</th> <th>Duration</th> <th>Login</th> <th>UserID</th> <th>Hostname</th> <th>Client</th> <th>Slides</th> <th>Video</th> </tr> </thead> <tbody> <tr> <td>12/20/2013</td> <td>1:49 PM - 2:00 PM</td> <td>forwardinc.ca\cmadmin</td> <td>n/a</td> <td>WIN2K8PROD01</td> <td>DB1</td> <td>73</td> <td></td> </tr> </tbody> </table>	Date	Duration	Login	UserID	Hostname	Client	Slides	Video	12/20/2013	1:49 PM - 2:00 PM	forwardinc.ca\cmadmin	n/a	WIN2K8PROD01	DB1	73	
Date	Duration	Login	UserID	Hostname	Client	Slides	Video										
12/20/2013	1:49 PM - 2:00 PM	forwardinc.ca\cmadmin	n/a	WIN2K8PROD01	DB1	73											

Change The Recording Behavior

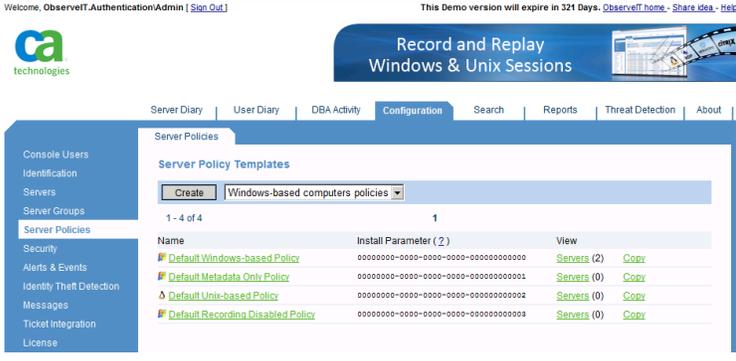
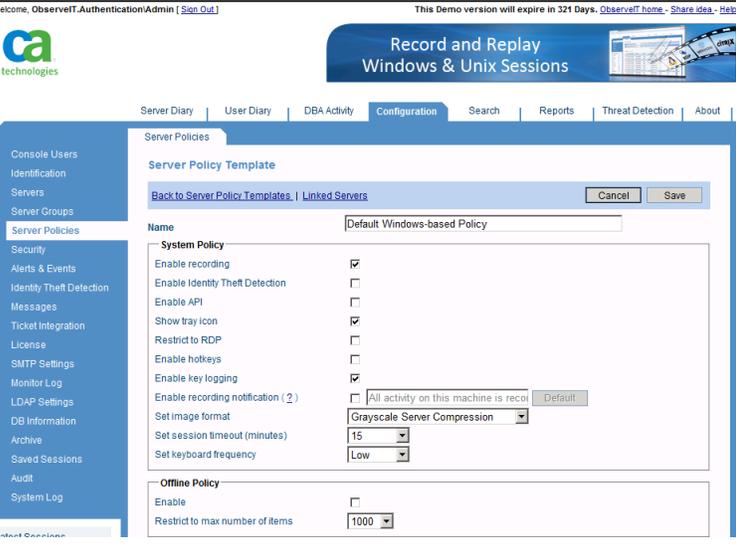
The default recording scope is that all the sessions on the JumpBox are being recorded. This means that if you start a session using the previously defined RemoteApp then both ControlMinder UI and the session started from by SAM using the login application will be recorded. It does not matter if the login applications are using VBS scripts that initiate the recording or not; the session is still being recorded. You can use standard VBS scripts and do not need to use the CA Session Recording -enhanced recording VBS scripts.

If you do not want to record everything that is happening on the JB then you can change the recording behavior to record only the sessions that are started from ControlMinder UI using login applications. In this case you will need to use the VBS scripts for the login applications that initiate the recording using the session recording API.

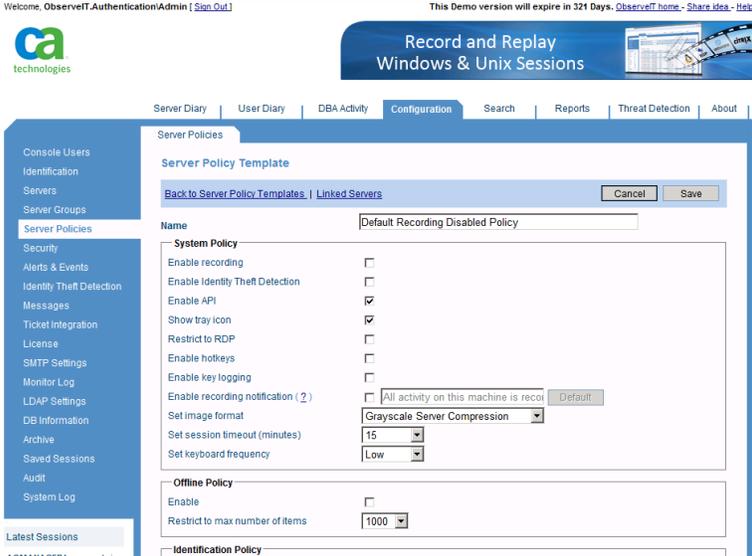
To change the recording behaviors follow these steps.

<p>Connect to the session recording console.</p>																																																																							
<p>Go to Configuration tab.</p>	 <table border="1"> <thead> <tr> <th>Session Duration</th> <th>Login</th> <th>User</th> <th>Server</th> <th>Client</th> <th>Slides</th> <th>Video</th> </tr> </thead> <tbody> <tr> <td colspan="7" style="text-align: center;">1/23/2014</td> </tr> <tr> <td>1:51 PM - 1:54 PM</td> <td>cmadmin</td> <td>n/a</td> <td>ACMANAGER1</td> <td>DULPE01-W7</td> <td>8</td> <td></td> </tr> <tr> <td>1:34 PM - 1:35 PM</td> <td>cmadmin</td> <td>n/a</td> <td>ACMANAGER1</td> <td>DULPE01-W7</td> <td>5</td> <td></td> </tr> <tr> <td colspan="7" style="text-align: center;">1/22/2014</td> </tr> <tr> <td>3:49 PM - 3:50 PM</td> <td>cmadmin</td> <td>n/a</td> <td>ACMANAGER1</td> <td>DULPE01-W7</td> <td>22</td> <td></td> </tr> <tr> <td>3:14 PM - 3:16 PM</td> <td>cmadmin</td> <td>n/a</td> <td>ACMANAGER1</td> <td>DULPE01-W7</td> <td>15</td> <td></td> </tr> <tr> <td>1:22 PM - 1:22 PM</td> <td>cmadmin</td> <td>n/a</td> <td>ACMANAGER1</td> <td>DULPE01-W7</td> <td>6</td> <td></td> </tr> <tr> <td colspan="7" style="text-align: center;">1/21/2014</td> </tr> <tr> <td>4:47 PM - 6:12 PM</td> <td>cmadmin</td> <td>n/a</td> <td>ACMANAGER1</td> <td>DULPE01-W7</td> <td>407</td> <td></td> </tr> </tbody> </table>	Session Duration	Login	User	Server	Client	Slides	Video	1/23/2014							1:51 PM - 1:54 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	8		1:34 PM - 1:35 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	5		1/22/2014							3:49 PM - 3:50 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	22		3:14 PM - 3:16 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	15		1:22 PM - 1:22 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	6		1/21/2014							4:47 PM - 6:12 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	407	
Session Duration	Login	User	Server	Client	Slides	Video																																																																	
1/23/2014																																																																							
1:51 PM - 1:54 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	8																																																																		
1:34 PM - 1:35 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	5																																																																		
1/22/2014																																																																							
3:49 PM - 3:50 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	22																																																																		
3:14 PM - 3:16 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	15																																																																		
1:22 PM - 1:22 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	6																																																																		
1/21/2014																																																																							
4:47 PM - 6:12 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	407																																																																		

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

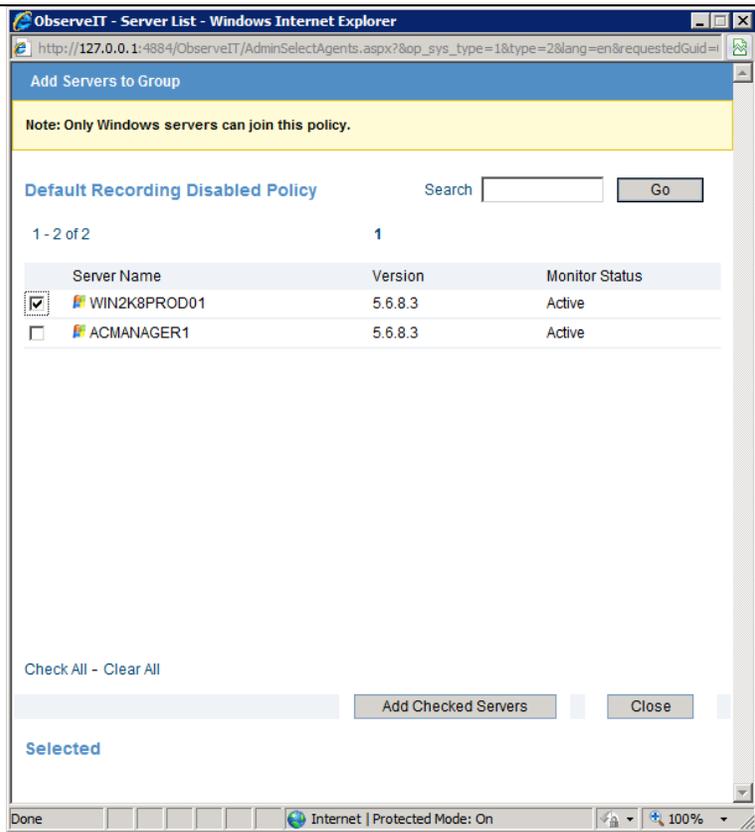
<p>Select Server Policies.</p>	
<p>The MS Windows agents are placed by default into “Default Windows-based Policy”</p>	
<p>This policy is configured to record all sessions.</p>	

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>You need to move JB Server to “Default Recording Disabled Policy” to record only the session initiated over API.</p> <p>Note that “Enable API” is checked for this policy.</p> <p>Click on “Linked Servers” to allocate the servers to this policy.</p>	 <p>Welcome, ObserverrT.AuthenticationAdmin [Sign Out] This Demo version will expire in 321 Days. ObserverrT home - Share Idea - Help</p> <p>Record and Replay Windows & Unix Sessions</p> <p>Server Diary User Diary DBA Activity Configuration Search Reports Threat Detection About</p> <p>Server Policies</p> <p>Server Policy Template</p> <p>Back to Server Policy Templates Linked Servers Cancel Save</p> <p>Name: Default Recording Disabled Policy</p> <p>System Policy</p> <ul style="list-style-type: none"> Enable recording: <input type="checkbox"/> Enable Identity Theft Detection: <input type="checkbox"/> Enable API: <input checked="" type="checkbox"/> Show tray icon: <input checked="" type="checkbox"/> Restrict to RDP: <input type="checkbox"/> Enable hotkeys: <input type="checkbox"/> Enable key logging: <input type="checkbox"/> Enable recording notification (2): <input type="checkbox"/> All activity on this machine is recorded Default Set image format: Grayscale Server Compression Set session timeout (minutes): 15 Set keyboard frequency: Low <p>Offline Policy</p> <ul style="list-style-type: none"> Enable: <input type="checkbox"/> Restrict to max number of items: 1000 <p>Identification Policy</p>				
<p>Click “Add Servers”</p>	 <p>Welcome, ObserverrT.AuthenticationAdmin [Sign Out] This Demo version will expire in 321 Days. ObserverrT home - Share Idea - Help</p> <p>Record and Replay Windows & Unix Sessions</p> <p>Server Diary User Diary DBA Activity Configuration Search Reports Threat Detection About</p> <p>Server Policies</p> <p>Default Recording Disabled Policy - Servers</p> <p>Back to Server Policy Templates Add Servers Add Servers from Group</p> <p>1 - 0 of 0 1</p> <table border="1"> <thead> <tr> <th>Server Name</th> <th>Version</th> <th>Status</th> <th>Date</th> </tr> </thead> <tbody> </tbody> </table>	Server Name	Version	Status	Date
Server Name	Version	Status	Date		

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

Select your JB Server and click “Add Checked Servers”.



Your JumpBox will now be recording only the sessions initiated through API. These are the sessions started by the recording VBS auto login scripts.



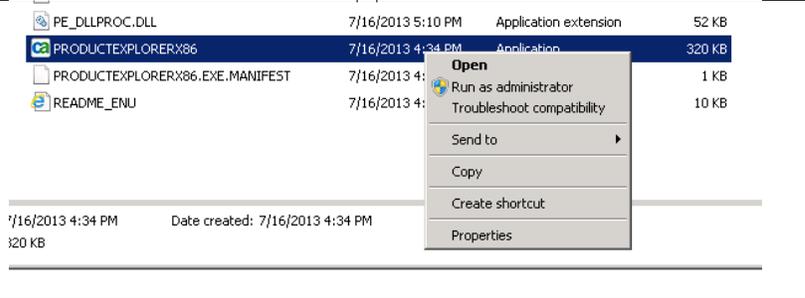
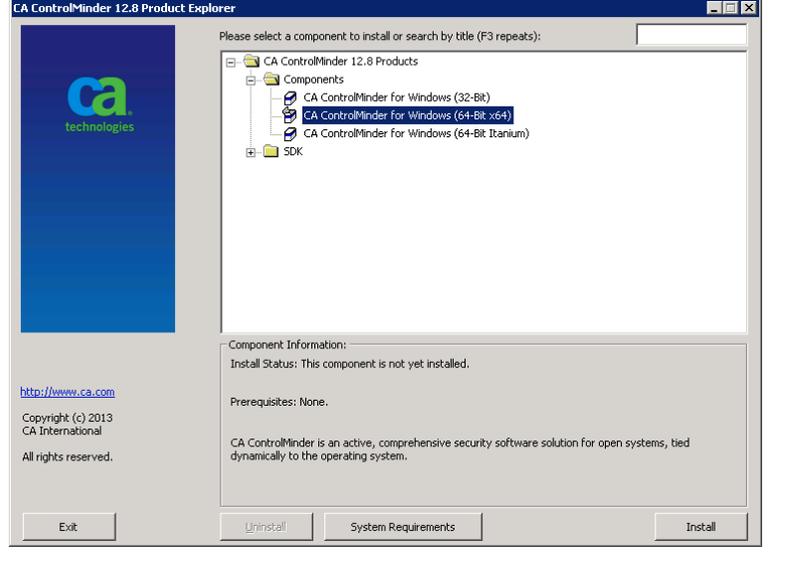
Install ControlMinder Endpoint Software On The JumpBox

You can use ControlMinder Endpoint software to protect the JumpBox.

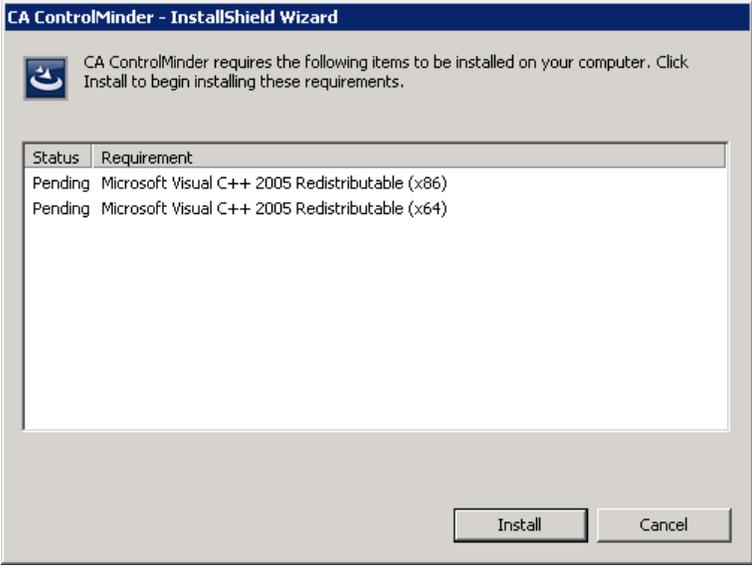
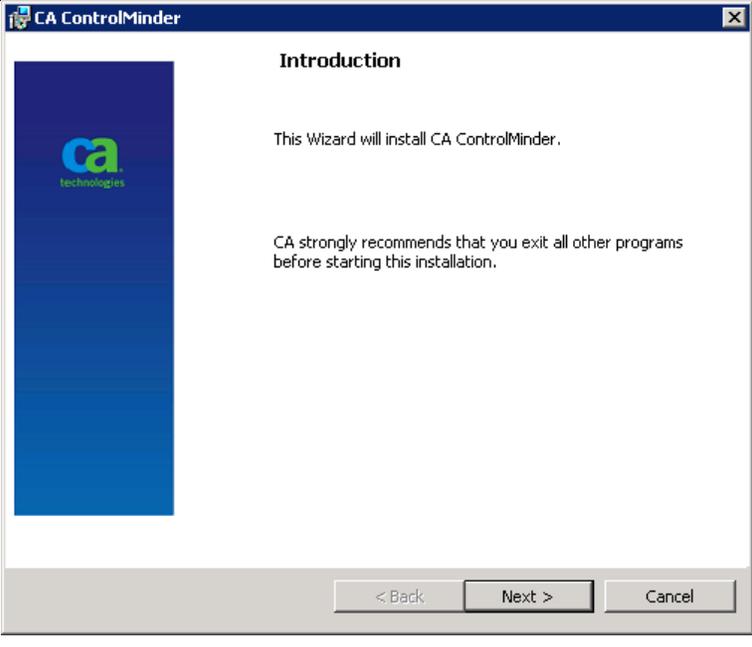
This will allow you to protect the processes of CA Session Recording agent from being terminated.

You must be a member of the local Administrators group to perform the installation of ControlMinder Endpoint components.

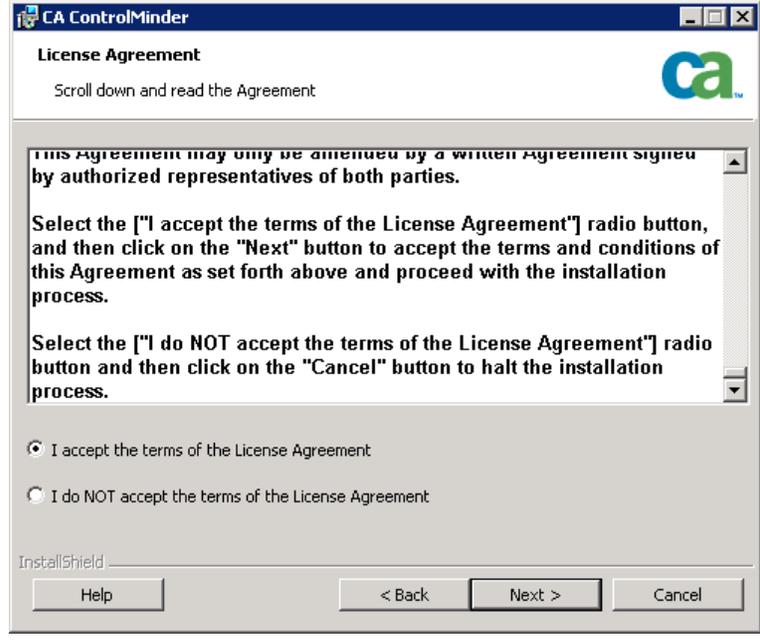
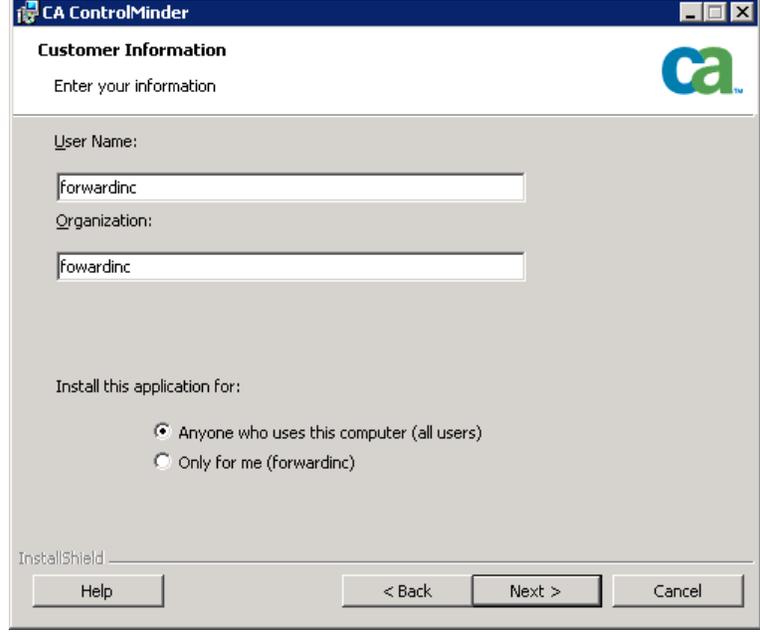
The following example leverages a graphical user interface (GUI) to install the endpoint software. Silent installation is available to facilitate unattended installation. Refer to the Implementation Guide for additional information.

<p>Locate the PRODUCTEXPLORERX86.EXE executable. Right-click the executable and choose <u>Run as administrator</u> to start the installation.</p>	
<p>This example assumes that the endpoint is a 64-bit Intel/AMD architecture. From the Components folder of the Product Explorer, select <u>CA ControlMinder for Windows (64-Bit x64)</u> Click the Install button.</p>	
<p>Select the language for the installation and click the OK button.</p>	

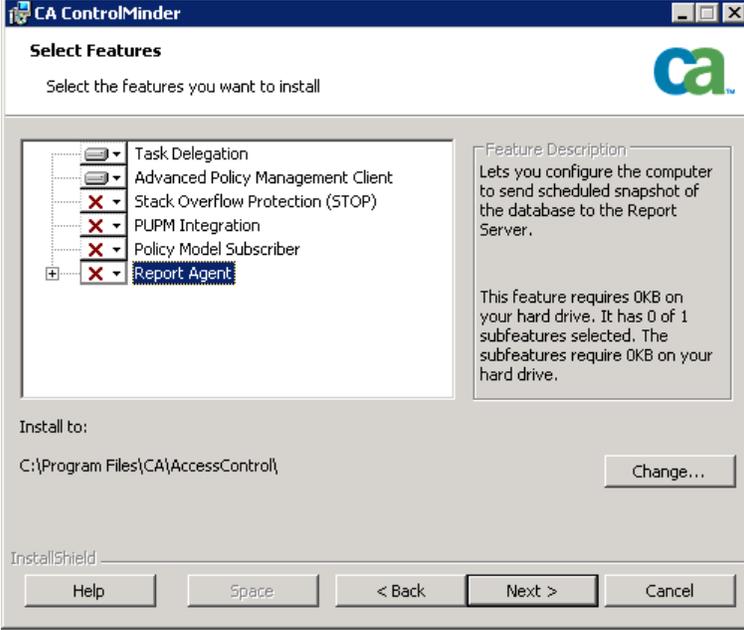
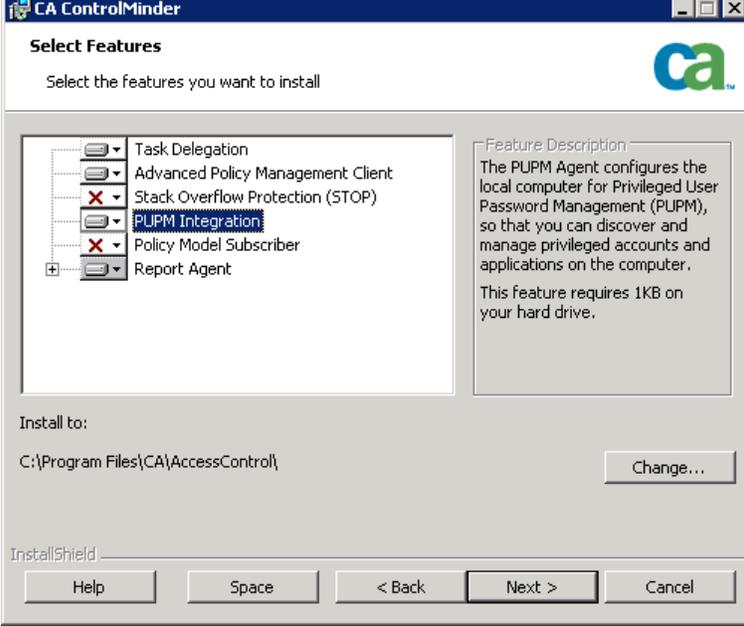
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>If prompted to install Microsoft Visual C++ Redistributable libraries, click the Install button.</p>	
<p>Click the Next button to proceed with the ControlMinder endpoint software installation.</p>	

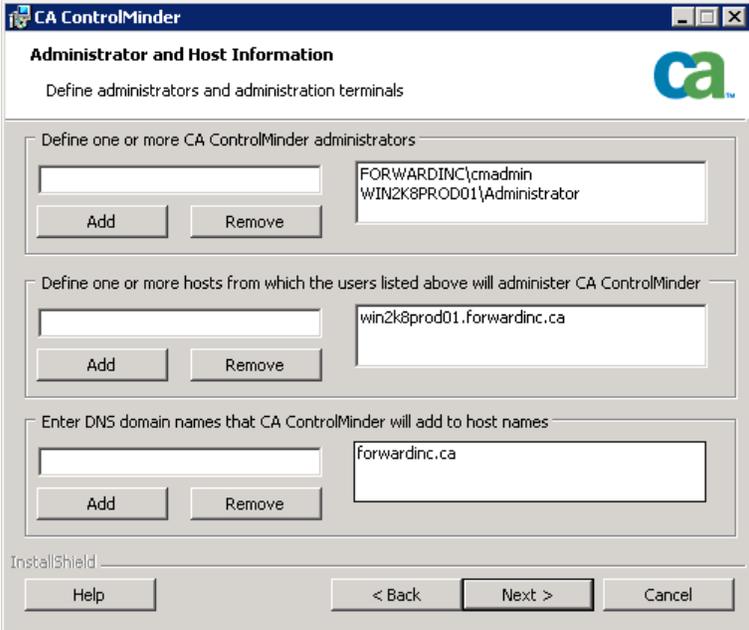
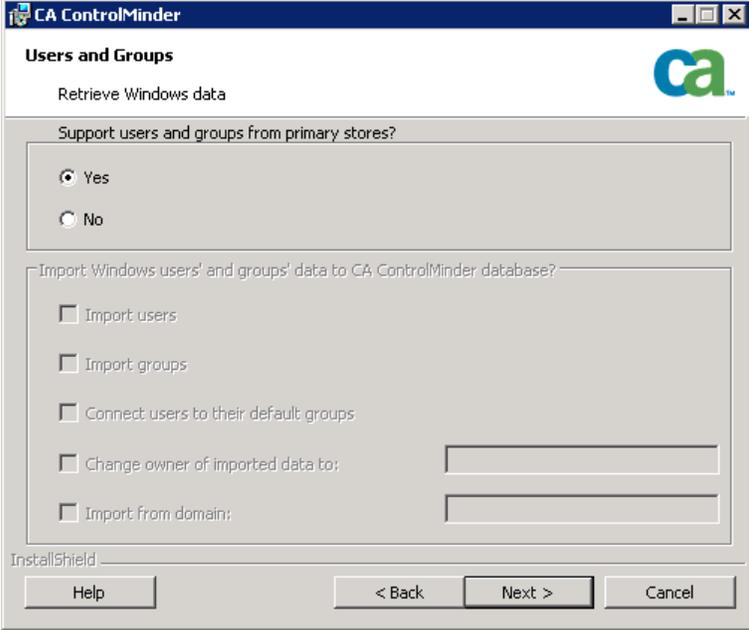
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Read the License Agreement as you use the scrollbar to advance through the document.</p> <p>Click the radial button noting <u>I accept the terms of the License Agreement</u>.</p> <p>Click the Next button.</p>	
<p>Provide customer information.</p> <p>Click the Next button.</p>	

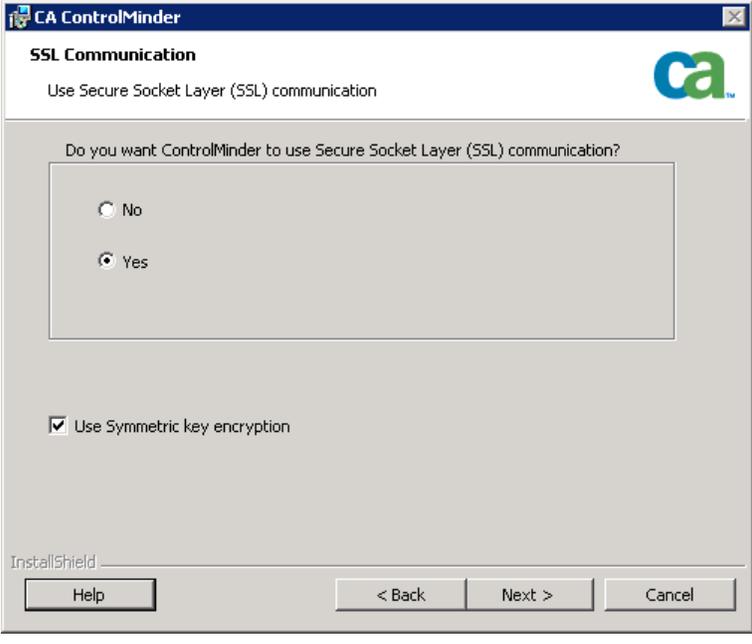
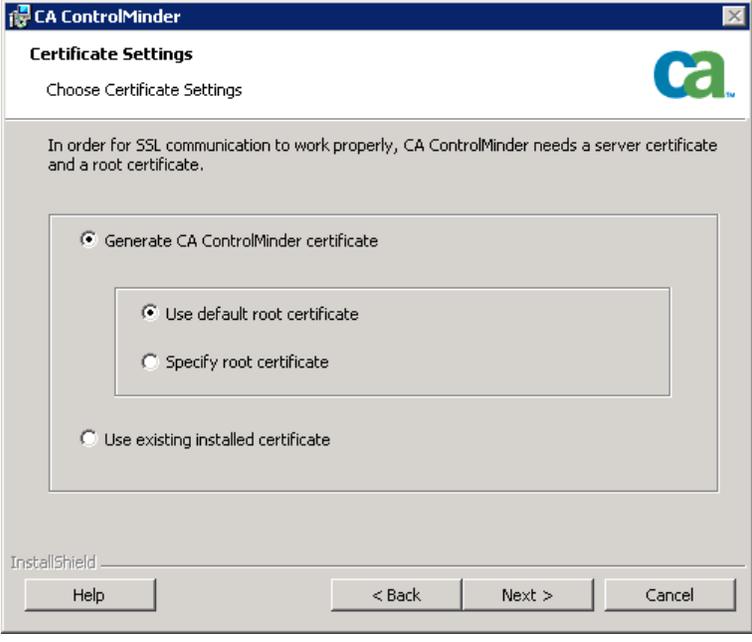
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

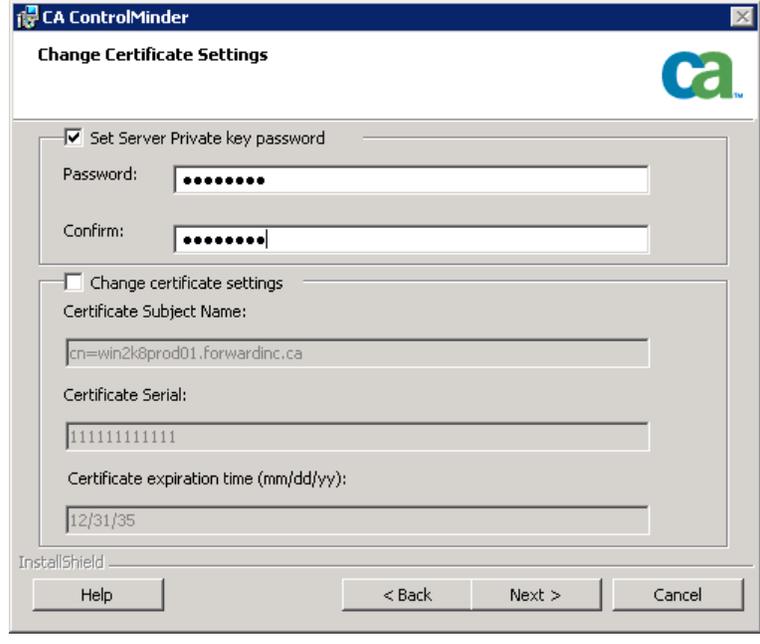
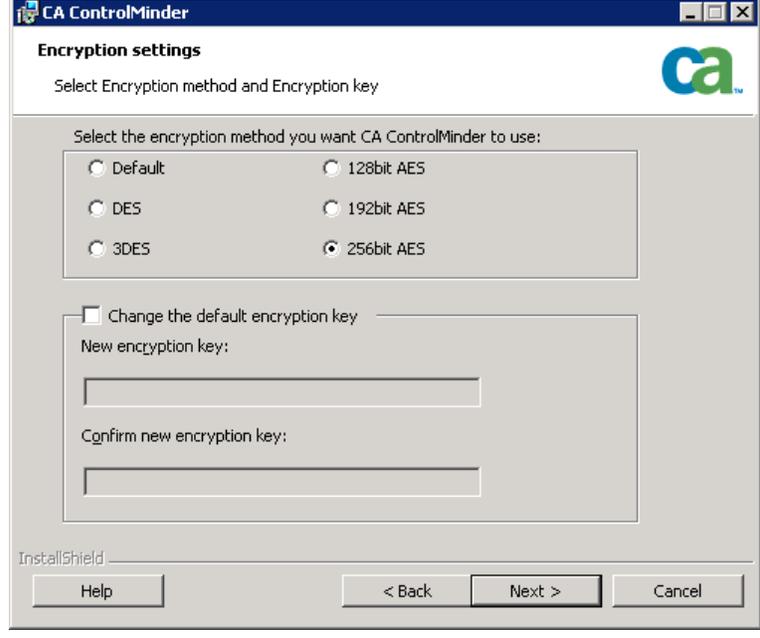
<p>Select the installation directory and the components to be installed.</p> <p>Add “PUPM Integration” and “Report Agent” out of those no selected by default.</p> <p>Click the Next button.</p>	 <p>CA ControlMinder</p> <p>Select Features</p> <p>Select the features you want to install</p> <ul style="list-style-type: none"> <input type="checkbox"/> Task Delegation <input type="checkbox"/> Advanced Policy Management Client <input checked="" type="checkbox"/> Stack Overflow Protection (STOP) <input checked="" type="checkbox"/> PUPM Integration <input checked="" type="checkbox"/> Policy Model Subscriber <input checked="" type="checkbox"/> Report Agent <p>Feature Description</p> <p>Lets you configure the computer to send scheduled snapshot of the database to the Report Server.</p> <p>This feature requires 0KB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive.</p> <p>Install to: C:\Program Files\CA\AccessControl\ Change...</p> <p>InstallShield</p> <p>Help Space < Back Next > Cancel</p>
<p>If you do not plan to use ControlMinder reporting functionality and audit event collection, do not install the <u>Report Agent</u> component.</p> <p>Click the Next button.</p>	 <p>CA ControlMinder</p> <p>Select Features</p> <p>Select the features you want to install</p> <ul style="list-style-type: none"> <input type="checkbox"/> Task Delegation <input type="checkbox"/> Advanced Policy Management Client <input checked="" type="checkbox"/> Stack Overflow Protection (STOP) <input checked="" type="checkbox"/> PUPM Integration <input checked="" type="checkbox"/> Policy Model Subscriber <input type="checkbox"/> Report Agent <p>Feature Description</p> <p>The PUPM Agent configures the local computer for Privileged User Password Management (PUPM), so that you can discover and manage privileged accounts and applications on the computer.</p> <p>This feature requires 1KB on your hard drive.</p> <p>Install to: C:\Program Files\CA\AccessControl\ Change...</p> <p>InstallShield</p> <p>Help Space < Back Next > Cancel</p>

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

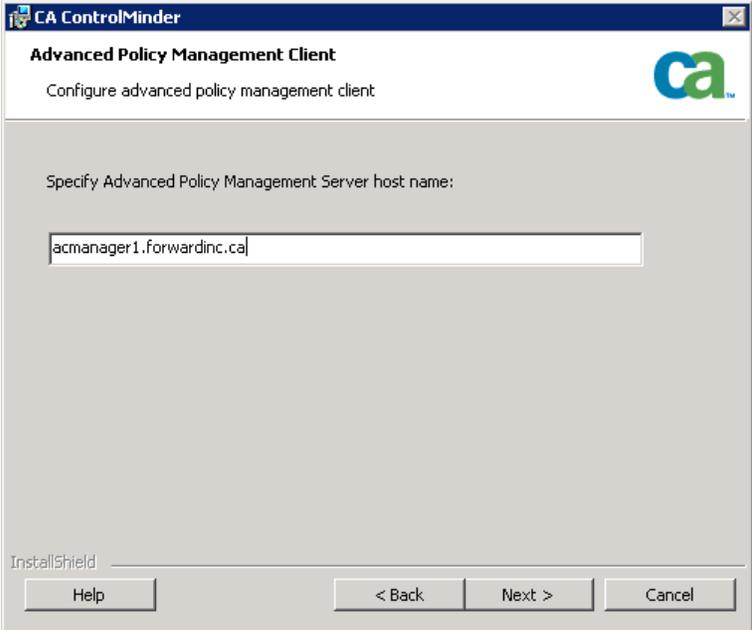
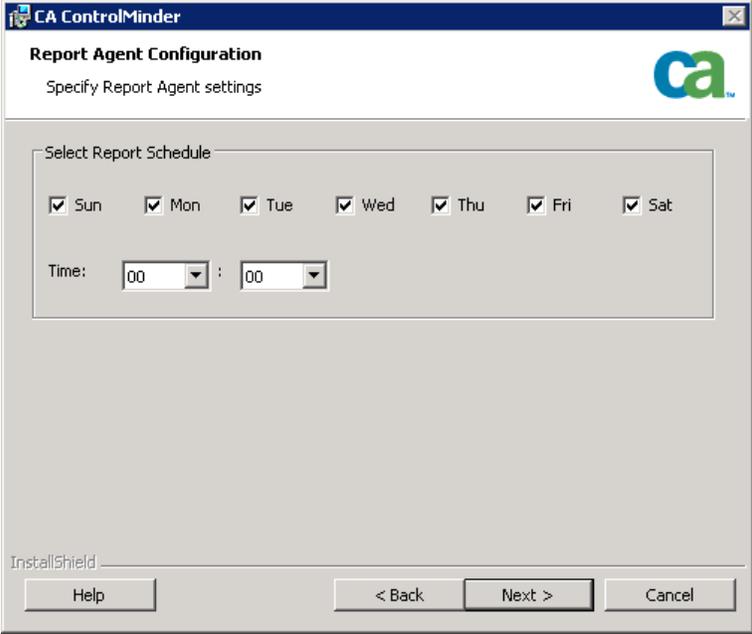
<p>Provide the names of the ControlMinder administrators.</p> <p>Identify the servers from which the ControlMinder administrators are allowed to manage the endpoint. Typically, this is the endpoint itself and possibly the Distribution Server and/or the ENTM Server. For the latter Security Group and/or firewall rules may be required.</p> <p>The user installing ControlMinder is added by default as a ControlMinder administrator.</p> <p>DO NOT REMOVE THIS USER!!</p> <p>If this user is removed then the installation will fail!</p> <p>This user can be removed after the installation has completed.</p> <p>In the example screenshot, cmadmin was added by default as the installer, and Administrator was manually added. Provide DNS domain names to add to the hostname when identifying the endpoint.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'Administrator and Host Information' dialog box. It has three main sections: 'Define one or more CA ControlMinder administrators' with a list containing 'FORWARDINC\cmadmin' and 'WIN2K8PROD01\Administrator'; 'Define one or more hosts from which the users listed above will administer CA ControlMinder' with a list containing 'win2k8prod01.forwardinc.ca'; and 'Enter DNS domain names that CA ControlMinder will add to host names' with a list containing 'forwardinc.ca'. At the bottom, there are 'Help', '< Back', 'Next >', and 'Cancel' buttons.</p>
<p>Unless there is a specific need to do otherwise, accept the default of selecting the radial button for Yes to <u>Support users and groups from primary stores</u>. This allows ControlMinder to recognize users from the native environment.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'Users and Groups' dialog box. It has two main sections: 'Support users and groups from primary stores?' with the 'Yes' radio button selected; and 'Import Windows users' and groups' data to CA ControlMinder database?' with several unchecked checkboxes: 'Import users', 'Import groups', 'Connect users to their default groups', 'Change owner of imported data to:', and 'Import from domain:'. At the bottom, there are 'Help', '< Back', 'Next >', and 'Cancel' buttons.</p>

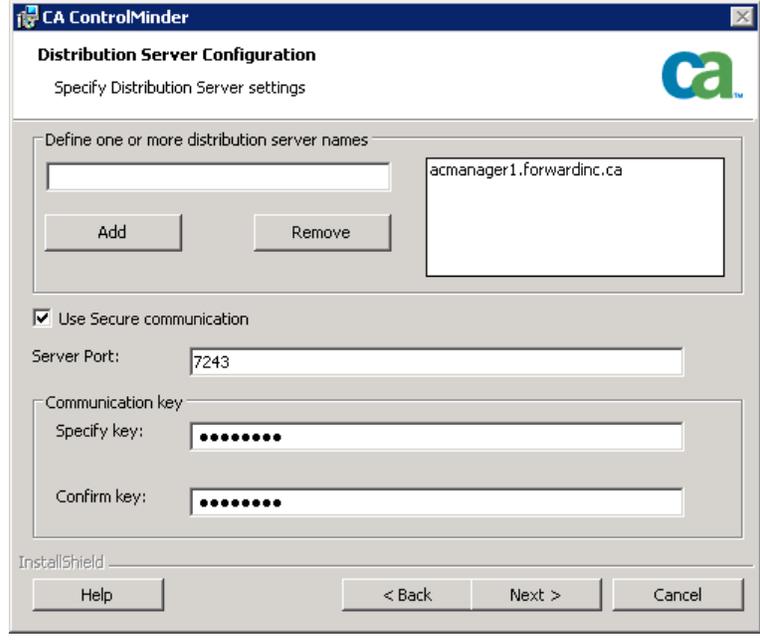
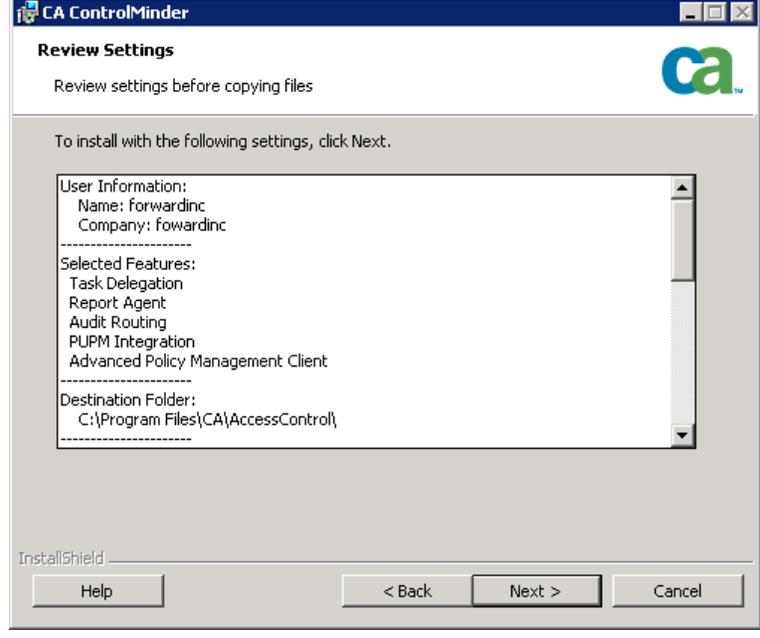
CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Click the radial button for Yes to use Secure Socket Layer (SSL) communication.</p> <p>Leave the <u>Use Symmetric key encryption</u> checkbox checked.</p> <p>Note that SSL is enabled by default on CM ENTM server.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'SSL Communication' dialog box in the CA ControlMinder application. The title bar reads 'CA ControlMinder'. Below the title bar, it says 'SSL Communication' and 'Use Secure Socket Layer (SSL) communication'. The main content area asks 'Do you want ControlMinder to use Secure Socket Layer (SSL) communication?' with two radio buttons: 'No' and 'Yes'. The 'Yes' radio button is selected. Below this, there is a checkbox labeled 'Use Symmetric key encryption' which is checked. At the bottom, there are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button. The 'InstallShield' logo is visible in the bottom left corner.</p>
<p>Specify the certificate to use for SSL communication.</p> <p>The example in the screenshot uses a default root certificate to create a self-signed certificate.</p> <p>A consideration is whether or not to use a certificate generated by the Certificate Authority employed by your organization.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'Certificate Settings' dialog box in the CA ControlMinder application. The title bar reads 'CA ControlMinder'. Below the title bar, it says 'Certificate Settings' and 'Choose Certificate Settings'. The main content area contains the text: 'In order for SSL communication to work properly, CA ControlMinder needs a server certificate and a root certificate.' Below this text, there are four radio button options: 'Generate CA ControlMinder certificate' (selected), 'Use default root certificate', 'Specify root certificate', and 'Use existing installed certificate'. At the bottom, there are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button. The 'InstallShield' logo is visible in the bottom left corner.</p>

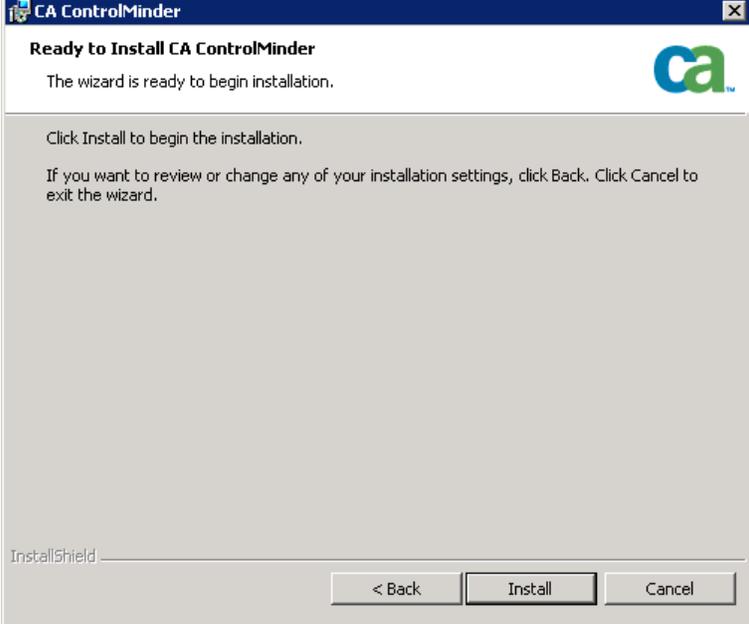
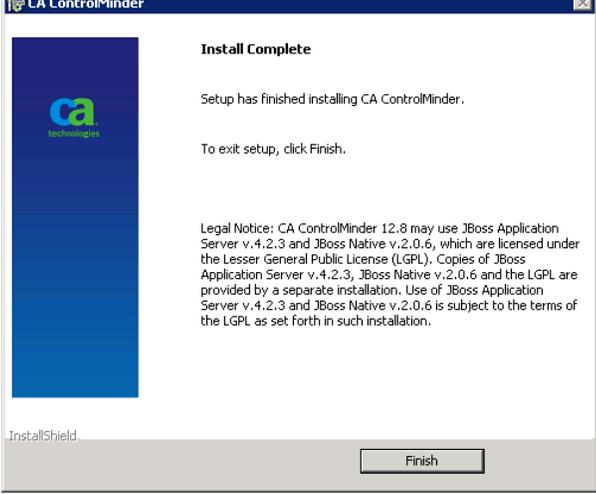
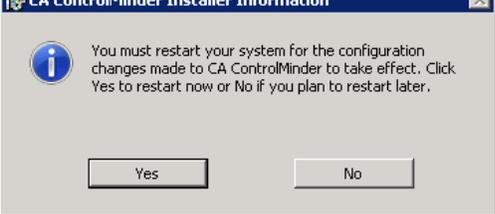
<p>Provide the password of the certificate's private key.</p> <p>Click the Next button.</p>	
<p>Select the encryption method to be used for symmetric encryption. 256bit AES is the default and preferred method. Other methods are available for backward capability.</p> <p>The example uses the default encryption key. Typically, the organization specifies a unique encryption key. When symmetric encryption is used, the same key must be used between all endpoints and servers.</p>	

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Provide the hostname of the Distribution Server.</p> <p>All communication between the endpoint and the ENTM Server flows through the Distribution Server.</p> <p>The endpoint must be able to resolve the hostname of the Distribution Server.</p> <p>Click the Next button.</p>	
<p>Specify when the Report Agent sends snapshots of the endpoint's ControlMinder database to the ENTM Server (via the Distribution Server).</p> <p>The snapshot data are used for reporting purposes.</p> <p>Click the Next button.</p>	

<p>Specify the Distribution Server that the endpoint will use for Message Queue (Tibco) communication.</p> <p>Use the same hostname as specified for Advanced Policy Management.</p> <p>Provide the communication password that was specified during the installation of Enterprise Management.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'Distribution Server Configuration' dialog box. It has a title bar 'CA ControlMinder' and a subtitle 'Distribution Server Configuration'. Below the subtitle is the instruction 'Specify Distribution Server settings'. The main area contains a section 'Define one or more distribution server names' with an empty text box on the left and a list box on the right containing 'acmanager1.forwardinc.ca'. There are 'Add' and 'Remove' buttons between the text box and the list box. Below this is a checked checkbox 'Use Secure communication'. Underneath is a 'Server Port:' label followed by a text box containing '7243'. There are two 'Communication key' sections: 'Specify key:' and 'Confirm key:', each followed by a text box filled with dots. At the bottom, there are 'Help', '< Back', 'Next >', and 'Cancel' buttons.</p>
<p>Review the installation parameters and click the Next button.</p>	 <p>The screenshot shows the 'Review Settings' dialog box. It has a title bar 'CA ControlMinder' and a subtitle 'Review Settings'. Below the subtitle is the instruction 'Review settings before copying files'. The main area contains the text 'To install with the following settings, click Next.' followed by a scrollable list box. The list box contains the following information: 'User Information: Name: forwardinc, Company: fowardinc'; 'Selected Features: Task Delegation, Report Agent, Audit Routing, PUPM Integration, Advanced Policy Management Client'; and 'Destination Folder: C:\Program Files\CA\AccessControl\'. At the bottom, there are 'Help', '< Back', 'Next >', and 'Cancel' buttons.</p>

CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Click the Install button.</p>	
<p>After the installation has completed, click the Finish button.</p>	
<p>The installation may require a reboot to load ControlMinder kernel drivers.</p> <p>Click the Yes button to reboot now or click the No button to manually reboot at a later time.</p>	

Protect The Session Recording Agent

You may use ControlMinder endpoint software to protect the session recording agent from being terminated.

The policy below creates a resource in the PROCESS class. This will protect all the processes with the name starting “rcd” and started from the session recording agent directory from being killed.

The policy allows only the SYSTEM user (the operating system itself) to kill the processes.

The other users can only stop the processes with winlogon.exe process.

Note that in the sample commands shown below, the software is installed on drive C: under Program Files. If another installation location is selected then modify the commands accordingly.

```
editres PROCESS ("C:\Program Files\ObserveIT\ObserveITAgent\Bin\rcd*.exe")
defaccess(none) audit(all) owner(nobody);

authorize PROCESS ("C:\Program Files\ObserveIT\ObserveITAgent\Bin\rcd*.exe") xuid('NT
AUTHORITY\SYSTEM') access(all);

authorize PROCESS ("C:\Program Files\ObserveIT\ObserveITAgent\Bin\rcd*.exe") uid(*)
access(all) via (pgm(C:\Windows\system32\winlogon.exe));
```

This policy can be applied locally on the JB using ControlMinder selang command line interface.

The policy can also be distributed using ControlMinder user interface through Advanced Policy Management.