



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

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.

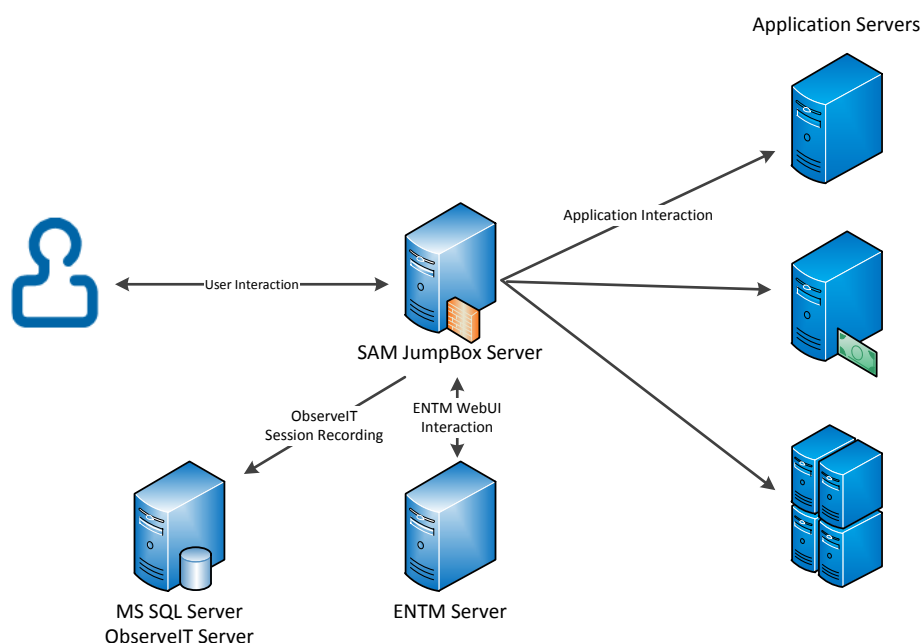
**Table 1 – Automatic Logon Access List**

Connection Type	Required Components
<b>Windows</b>	Microsoft RDP
<b>UNIX</b>	PuTTY (SSH, TELNET)
<b>MS SQL Server</b>	Microsoft SQL Management Studio
<b>ORACLE Web</b>	Microsoft Internet Explorer
<b>FTP</b>	FTP application (ftp.exe)
<b>Juniper NetScreen</b>	Microsoft Internet Explorer
<b>Nokia IPSO</b>	Microsoft Internet Explorer
<b>Reflection</b>	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.

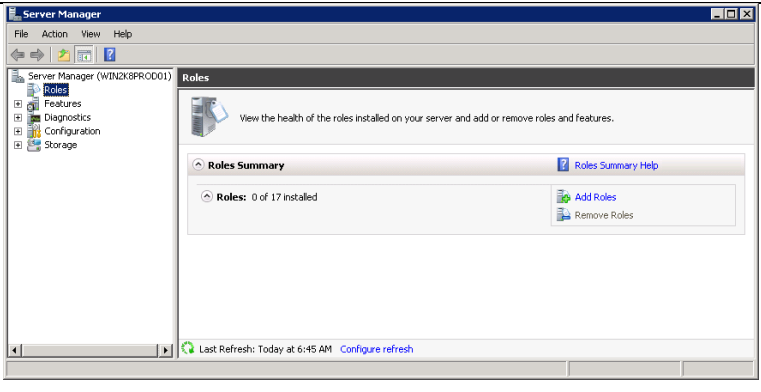
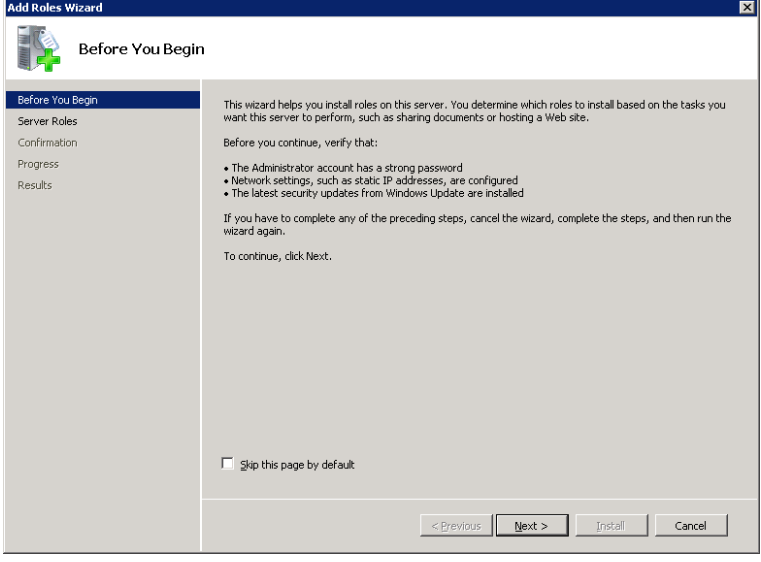
## Configure MS Windows Remote Desktop Services

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

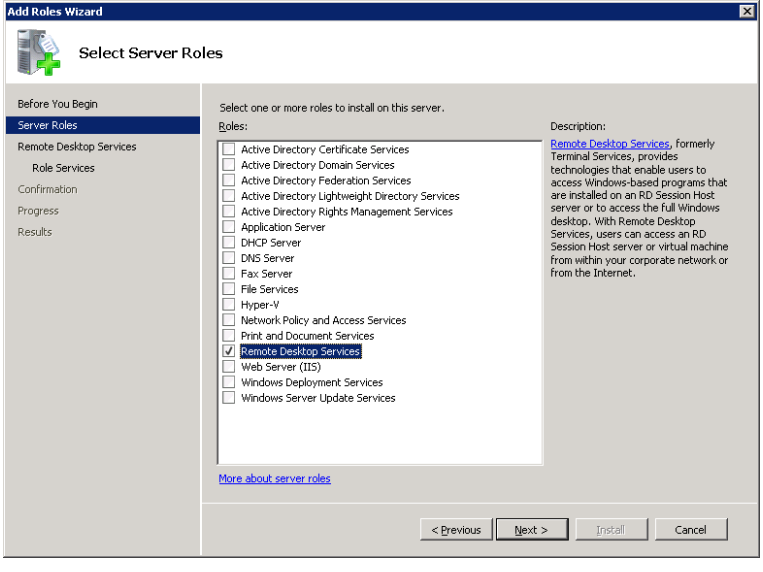
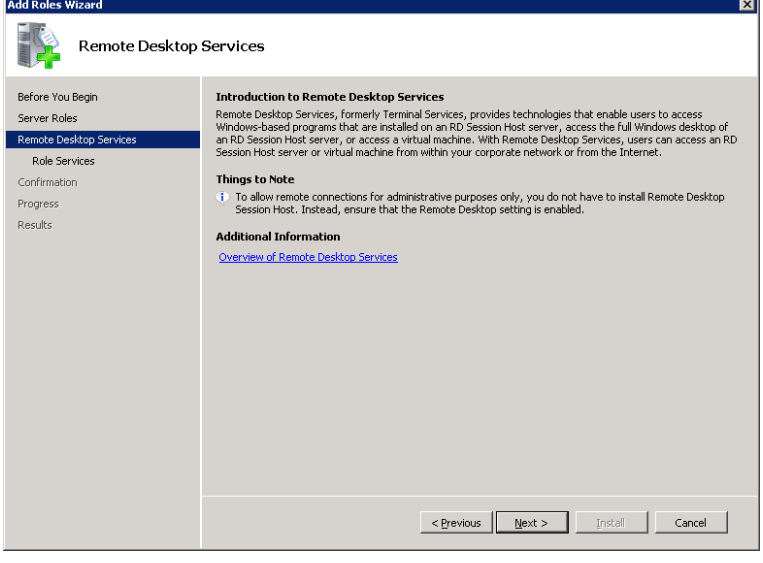
This chapter provides step by step instruction to install, configure and license the necessary components.

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

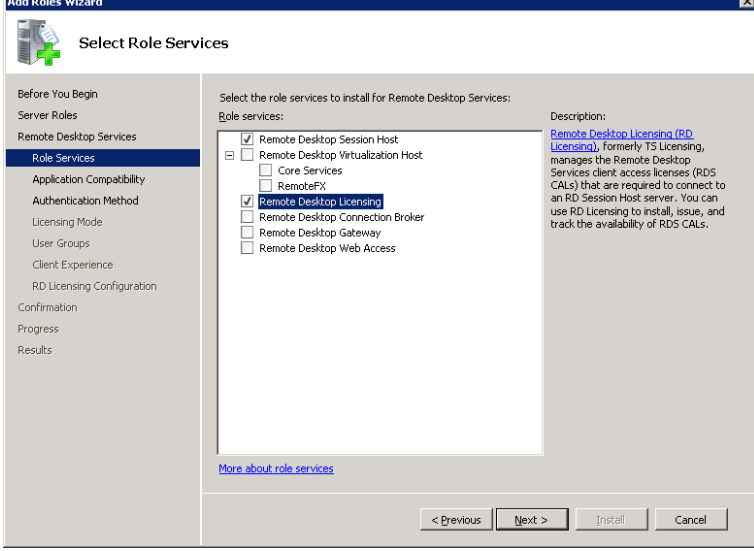
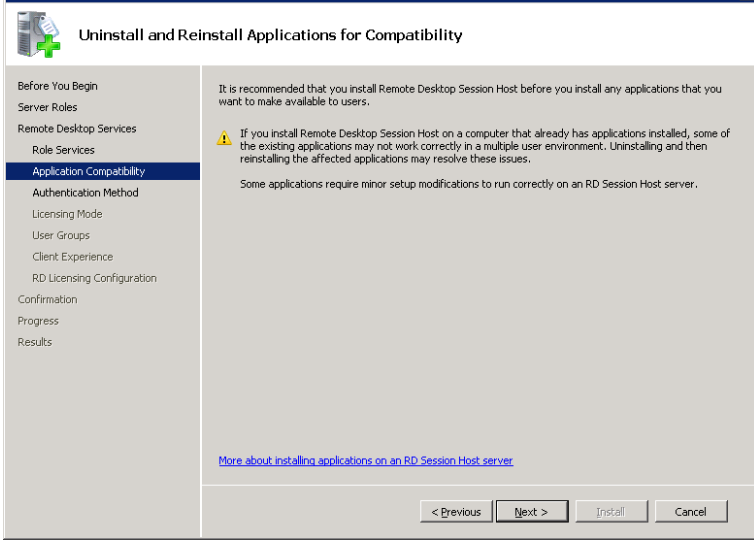
Log in to the server as a member of the Domain Admins group.

<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 pane displays the 'Roles' link under the 'Server Manager (WIN2K8PROD01)' tree. The right pane shows the 'Roles' page with a 'Roles Summary' section indicating '0 of 17 installed' roles. There are 'Add Roles' and 'Remove Roles' buttons available.</p>
<p>Click Next.</p>	 <p>The screenshot shows the 'Add Roles Wizard' window, specifically the 'Before You Begin' page. It provides instructions on what to verify before installing roles, such as having a strong password for the Administrator account, configuring network settings, and installing the latest security updates. At the bottom, there are buttons for '&lt; Previous', 'Next &gt;', 'Install', and 'Cancel'.</p>

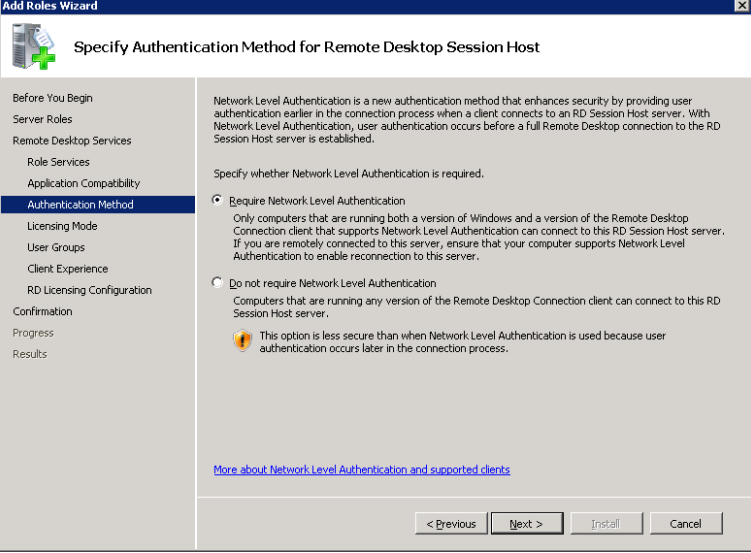

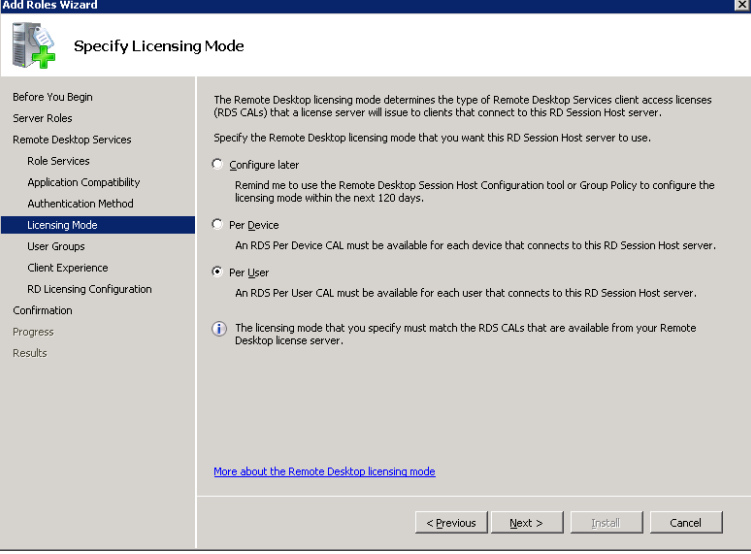

## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Select Remote Desktop Services and click next.</p>	
<p>Click Next.</p>	

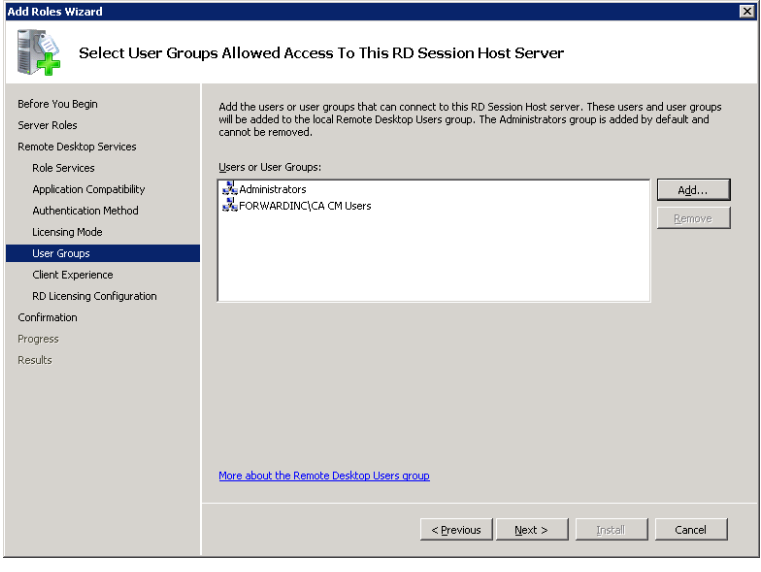
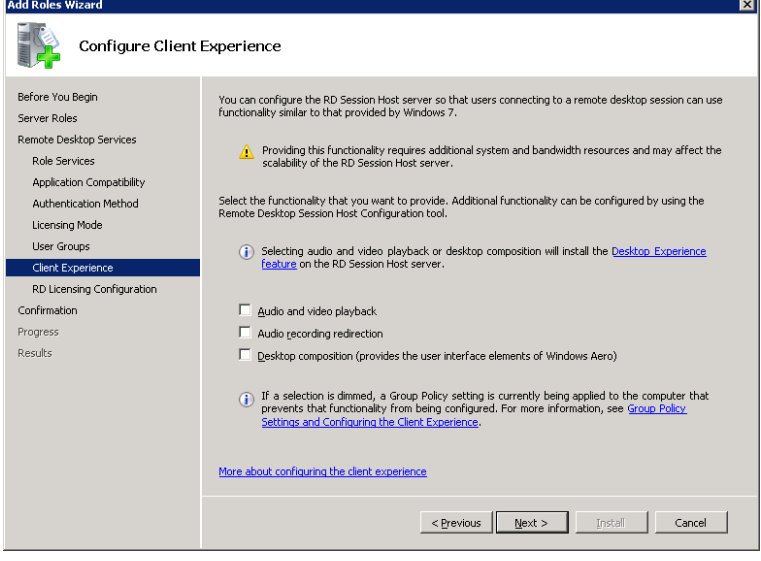
## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<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><b>Add Roles Wizard</b></p> <p><b>Select Role Services</b></p> <p>Before You Begin Server Roles Remote Desktop Services <b>Role Services</b> Application Compatibility Authentication Method Licensing Mode User Groups Client Experience RD Licensing Configuration Confirmation Progress Results</p> <p>Select the role services to install for Remote Desktop Services:</p> <p>Role services:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Remote Desktop Session Host</li> <li><input type="checkbox"/> Remote Desktop Virtualization Host</li> <li><input type="checkbox"/> Core Services</li> <li><input type="checkbox"/> RemoteFX</li> <li><input checked="" type="checkbox"/> Remote Desktop Licensing</li> <li><input type="checkbox"/> Remote Desktop Connection Broker</li> <li><input type="checkbox"/> Remote Desktop Gateway</li> <li><input type="checkbox"/> Remote Desktop Web Access</li> </ul> <p>Description: <a href="#">Remote Desktop Licensing (RD Licensing)</a>, formerly TS Licensing, manages the Remote Desktop Services client access licenses (RDS CALs) that are required to connect to an RD Session Host server. You can use RD Licensing to install, issue, and track the availability of RDS CALs.</p> <p><a href="#">More about role services</a></p> <p>&lt; Previous   Next &gt;   Install   Cancel</p>
<p>Click Next.</p>	 <p><b>Add Roles Wizard</b></p> <p><b>Uninstall and Reinstall Applications for Compatibility</b></p> <p>Before You Begin Server Roles Remote Desktop Services Role Services <b>Application Compatibility</b> Authentication Method Licensing Mode User Groups Client Experience RD Licensing Configuration Confirmation Progress Results</p> <p>It is recommended that you install Remote Desktop Session Host before you install any applications that you want to make available to users.</p> <p><b>Warning:</b> If you install Remote Desktop Session Host on a computer that already has applications installed, some of the existing applications may not work correctly in a multiple user environment. Uninstalling and then reinstalling the affected applications may resolve these issues.</p> <p>Some applications require minor setup modifications to run correctly on an RD Session Host server.</p> <p><a href="#">More about installing applications on an RD Session Host server</a></p> <p>&lt; Previous   Next &gt;   Install   Cancel</p>

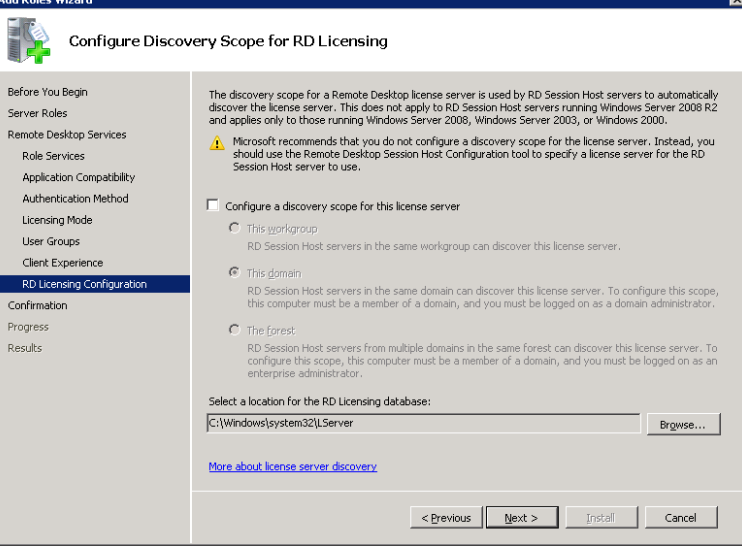
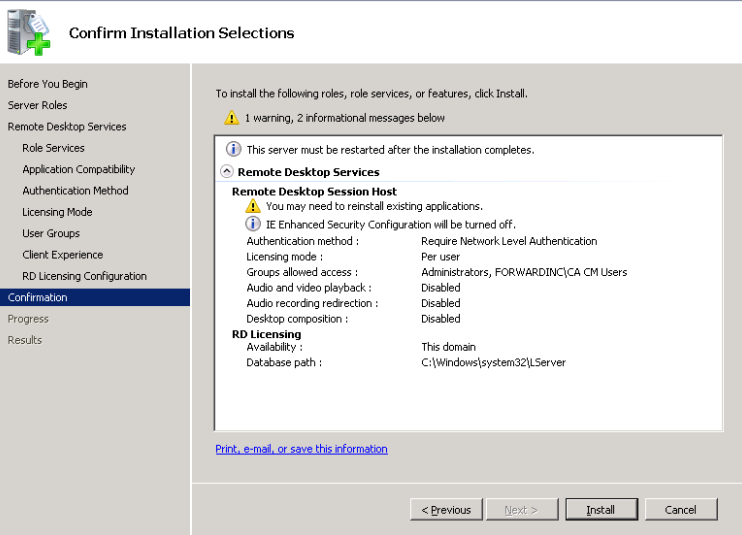
## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Select if you want to use Network Layer Authentication and click Next.</p>	 <p><b>Add Roles Wizard</b></p> <p><b>Specify Authentication Method for Remote Desktop Session Host</b></p> <p>Before You Begin Server Roles Remote Desktop Services Role Services Application Compatibility <b>Authentication Method</b> 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> <p><input checked="" type="radio"/> <b>Require Network Level Authentication</b> 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.</p> <p><input type="radio"/> <b>Do not require Network Level Authentication</b> Computers that are running any version of the Remote Desktop Connection client can connect to this RD Session Host server.</p> <p> This option is less secure than when Network Level Authentication is used because user authentication occurs later in the connection process.</p> <p><a href="#">More about Network Level Authentication and supported clients</a></p> <p>&lt; Previous   Next &gt;   Install   Cancel</p>
<p>Select your licensing method and click next.</p>	 <p><b>Add Roles Wizard</b></p> <p><b>Specify Licensing Mode</b></p> <p>Before You Begin Server Roles Remote Desktop Services Role Services Application Compatibility Authentication Method <b>Licensing Mode</b> 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> <p><input type="radio"/> <b>Configure later</b> Remind me to use the Remote Desktop Session Host Configuration tool or Group Policy to configure the licensing mode within the next 120 days.</p> <p><input type="radio"/> <b>Per Device</b> An RDS Per Device CAL must be available for each device that connects to this RD Session Host server.</p> <p><input checked="" type="radio"/> <b>Per User</b> An RDS Per User CAL must be available for each user that connects to this RD Session Host server.</p> <p> The licensing mode that you specify must match the RDS CALs that are available from your Remote Desktop license server.</p> <p><a href="#">More about the Remote Desktop licensing mode</a></p> <p>&lt; Previous   Next &gt;   Install   Cancel</p>

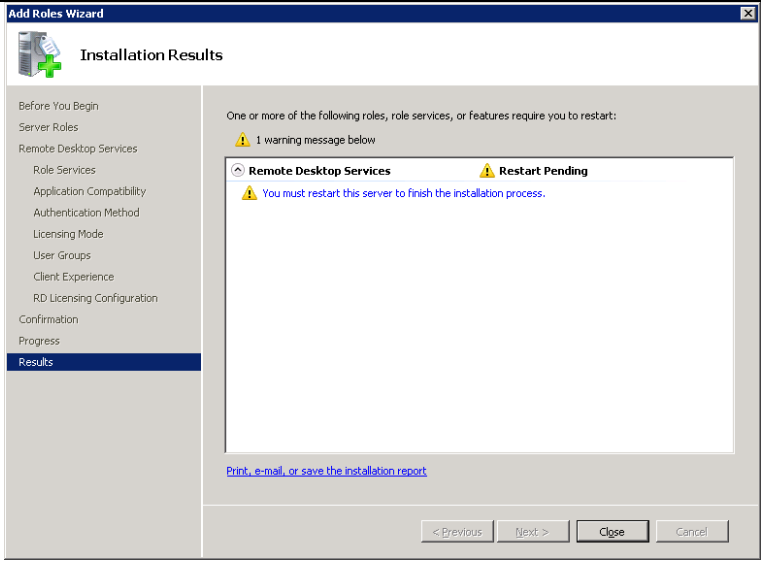
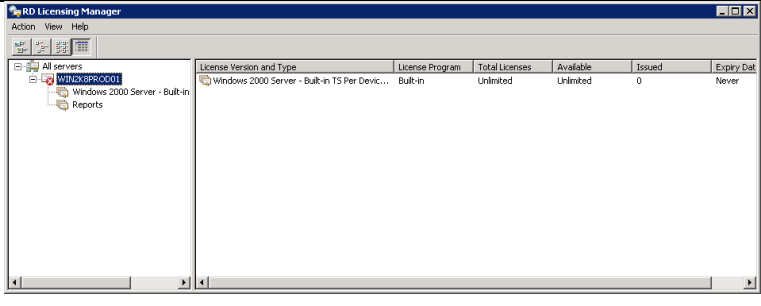
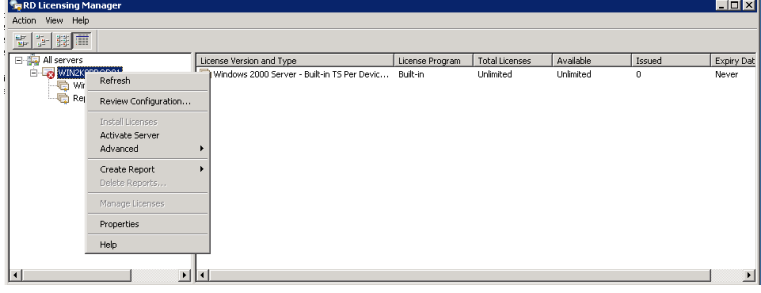
## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Add the group that contains the CA ControlMinder Shared Account Management Users.</p> <p>Click Next.</p>	
<p>The listed client experience features are not required by the CA ControlMinder SAM JumpBox. Click next to continue.</p>	

## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

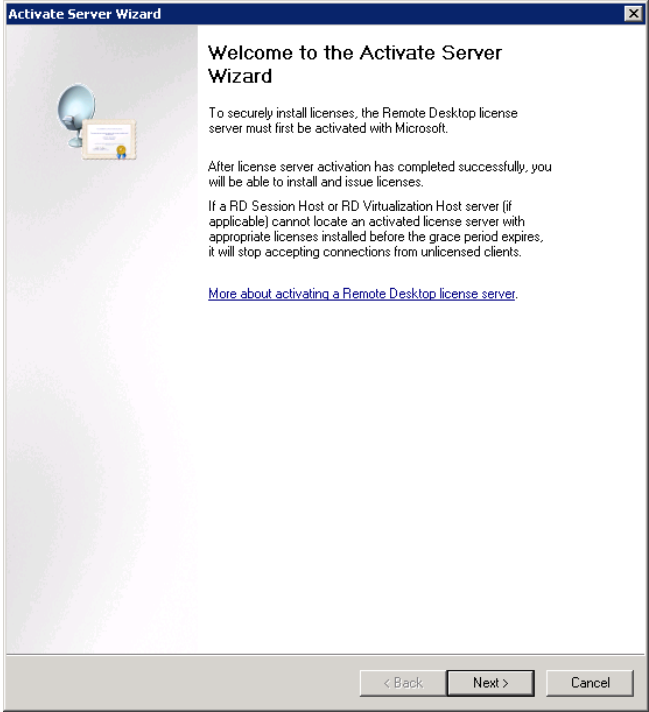
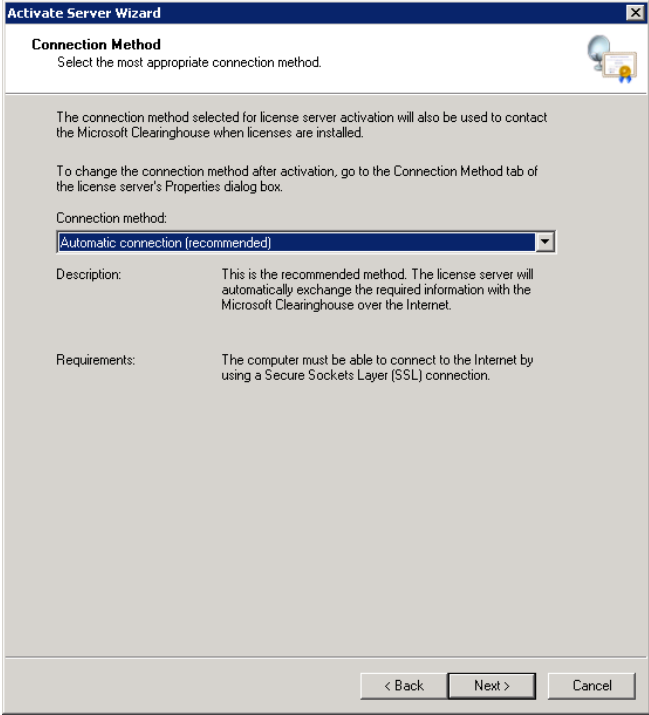
<p>Click Next.</p>	 <p><b>Add Roles Wizard</b></p> <p><b>Configure Discovery Scope for RD Licensing</b></p> <p>Before You Begin Server Roles Remote Desktop Services Role Services Application Compatibility Authentication Method Licensing Mode User Groups Client Experience <b>RD Licensing Configuration</b> Confirmation Progress Results</p> <p>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.</p> <p>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.</p> <p><input type="checkbox"/> Configure a discovery scope for this license server</p> <p><input type="radio"/> This workgroup RD Session Host servers in the same workgroup can discover this license server.</p> <p><input type="radio"/> This domain RD Session Host servers in the same domain can discover this license server. To configure this scope, this computer must be a member of a domain, and you must be logged on as a domain administrator.</p> <p><input type="radio"/> The forest RD Session Host servers from multiple domains in the same forest can discover this license server. To configure this scope, this computer must be a member of a domain, and you must be logged on as an enterprise administrator.</p> <p>Select a location for the RD Licensing database: C:\Windows\system32\LServer <span>Browse...</span></p> <p><a href="#">More about license server discovery</a></p> <p>&lt; Previous Next &gt; Install Cancel</p>																
<p>Click Install.</p>	 <p><b>Add Roles Wizard</b></p> <p><b>Confirm Installation Selections</b></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 <b>Confirmation</b> Progress Results</p> <p>To install the following roles, role services, or features, click Install.</p> <p>1 warning, 2 informational messages below</p> <p>This server must be restarted after the installation completes.</p> <p><b>Remote Desktop Services</b></p> <p><b>Remote Desktop Session Host</b></p> <p>You may need to reinstall existing applications.</p> <p>IE Enhanced Security Configuration will be turned off.</p> <table border="0"> <tr> <td>Authentication method :</td> <td>Require Network Level Authentication</td> </tr> <tr> <td>Licensing mode :</td> <td>Per user</td> </tr> <tr> <td>Groups allowed access :</td> <td>Administrators, FORWARDING\CA CM Users</td> </tr> <tr> <td>Audio and video playback :</td> <td>Disabled</td> </tr> <tr> <td>Audio recording redirection :</td> <td>Disabled</td> </tr> <tr> <td>Desktop composition :</td> <td>Disabled</td> </tr> </table> <p><b>RD Licensing</b></p> <table border="0"> <tr> <td>Availability :</td> <td>This domain</td> </tr> <tr> <td>Database path :</td> <td>C:\Windows\system32\LServer</td> </tr> </table> <p><a href="#">Print, e-mail, or save this information</a></p> <p>&lt; Previous Next &gt; Install Cancel</p>	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	Desktop composition :	Disabled	Availability :	This domain	Database path :	C:\Windows\system32\LServer
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																
Desktop composition :	Disabled																
Availability :	This domain																
Database path :	C:\Windows\system32\LServer																

## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

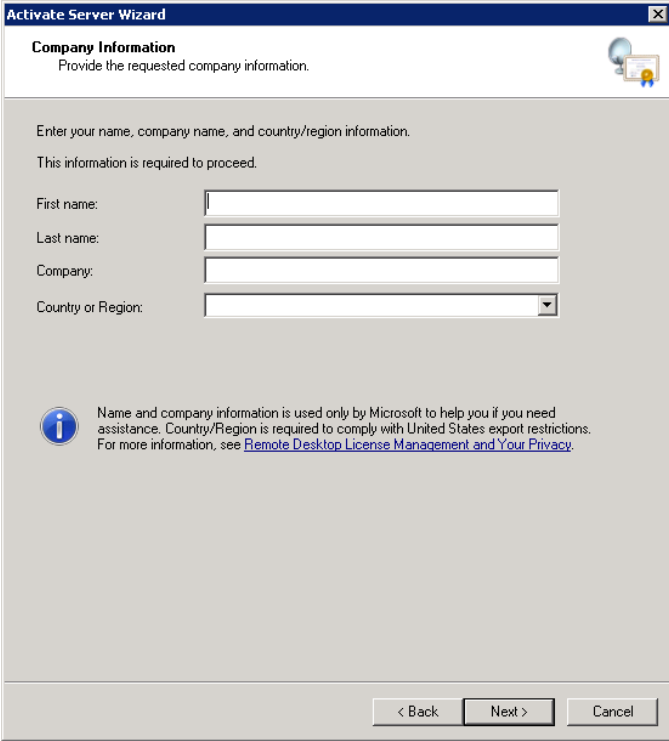

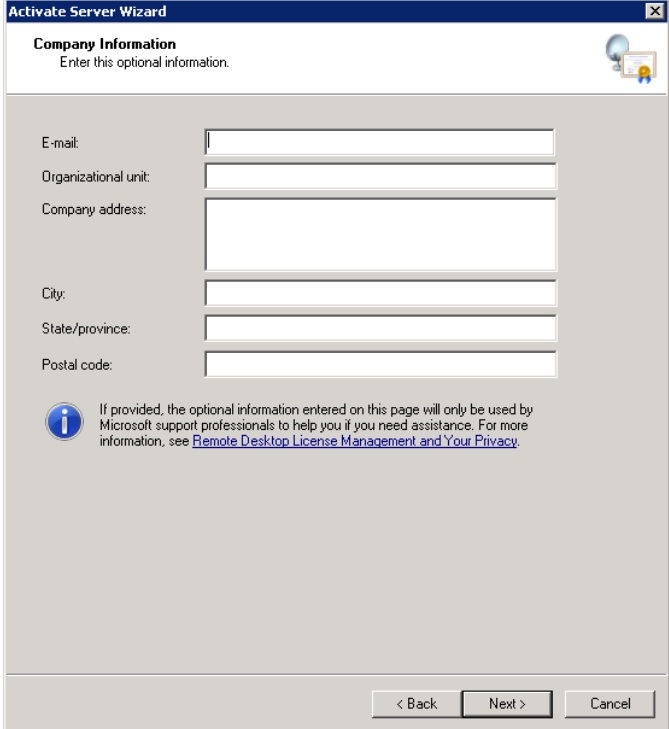

<p>Restart your server.</p>													
<p>Start Remote Desktop Licensing Manager Configuration from Start/Administrative Tools/Remote Desktop Services</p>	 <table><thead><tr><th>License Version and Type</th><th>License Program</th><th>Total Licenses</th><th>Available</th><th>Issued</th><th>Expiry Date</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>													

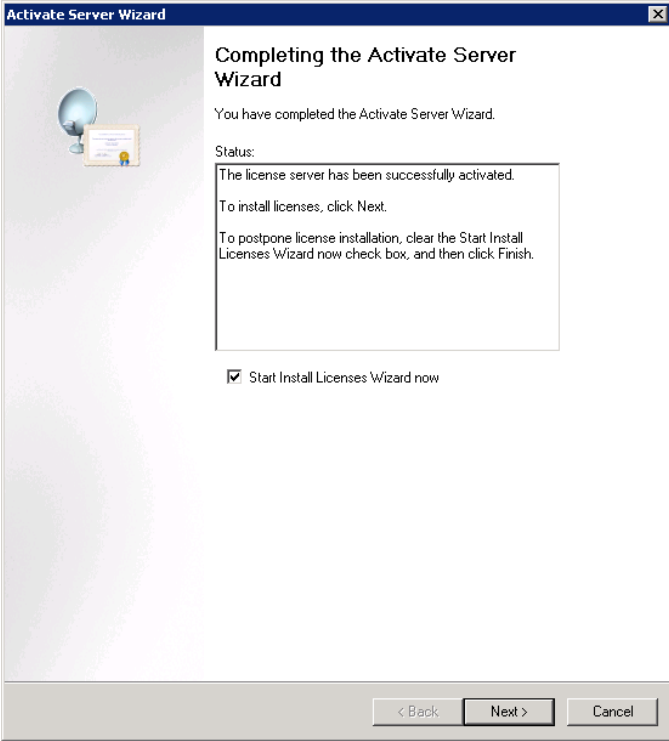
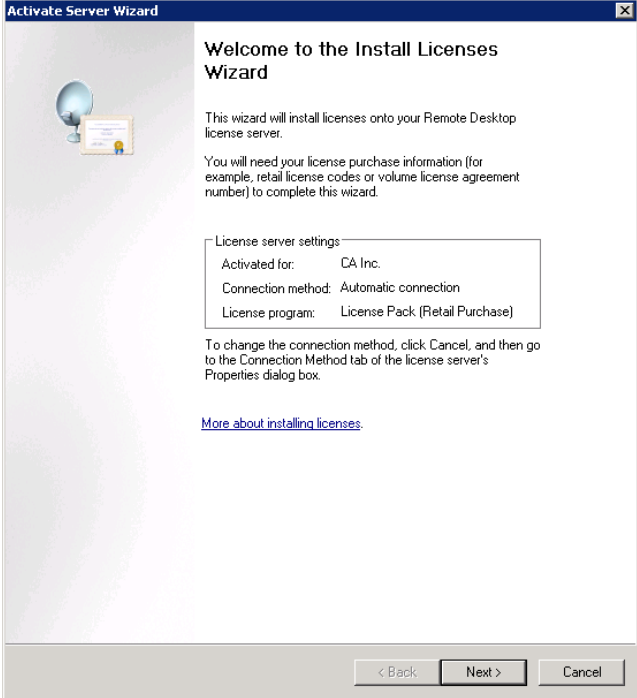


## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

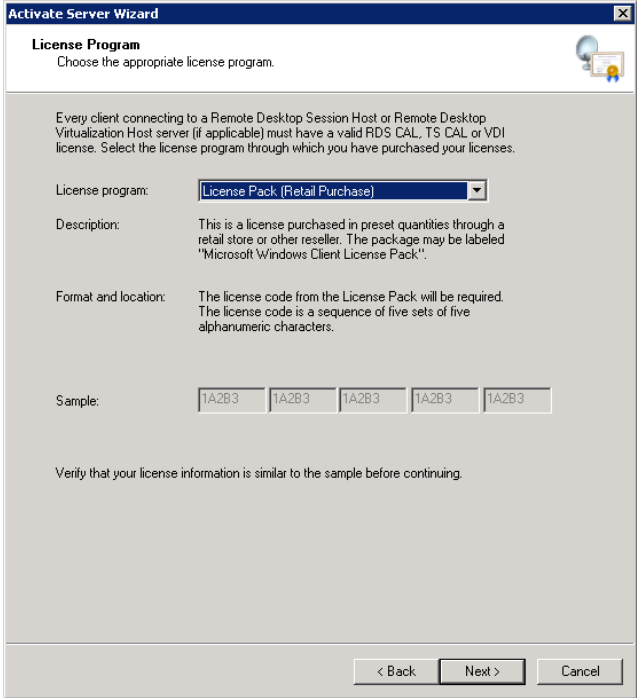
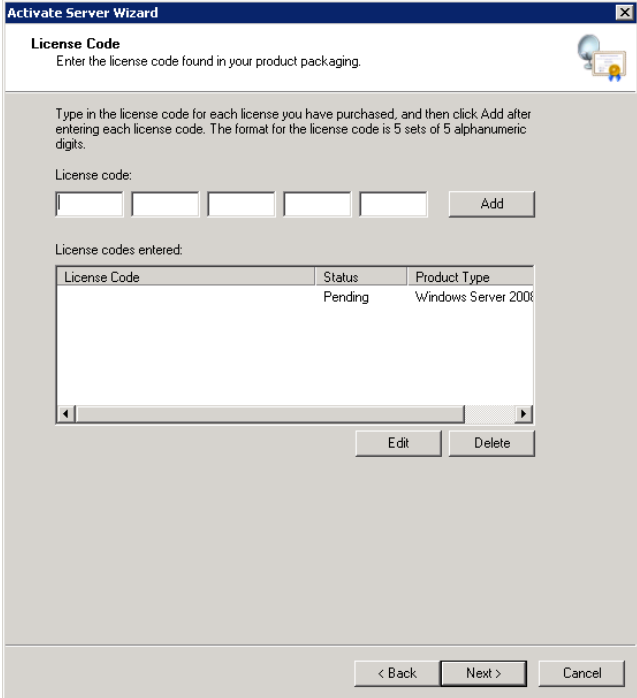
<p>Click Next.</p>	 <p><b>Activate Server Wizard</b></p> <p><b>Welcome to the Activate Server Wizard</b></p> <p>To securely install licenses, the Remote Desktop license server must first be activated with Microsoft.</p> <p>After license server activation has completed successfully, you will be able to install and issue licenses.</p> <p>If a RD Session Host or RD Virtualization Host server (if applicable) cannot locate an activated license server with appropriate licenses installed before the grace period expires, it will stop accepting connections from unlicensed clients.</p> <p><a href="#">More about activating a Remote Desktop license server.</a></p> <p>&lt; Back   Next &gt;   Cancel</p>
<p>Select the connection method and click Next.</p>	 <p><b>Activate Server Wizard</b></p> <p><b>Connection Method</b> Select the most appropriate connection method.</p> <p>The connection method selected for license server activation will also be used to contact the Microsoft Clearinghouse when licenses are installed.</p> <p>To change the connection method after activation, go to the Connection Method tab of the license server's Properties dialog box.</p> <p>Connection method: Automatic connection (recommended)</p> <p>Description: This is the recommended method. The license server will automatically exchange the required information with the Microsoft Clearinghouse over the Internet.</p> <p>Requirements: The computer must be able to connect to the Internet by using a Secure Sockets Layer (SSL) connection.</p> <p>&lt; Back   Next &gt;   Cancel</p>

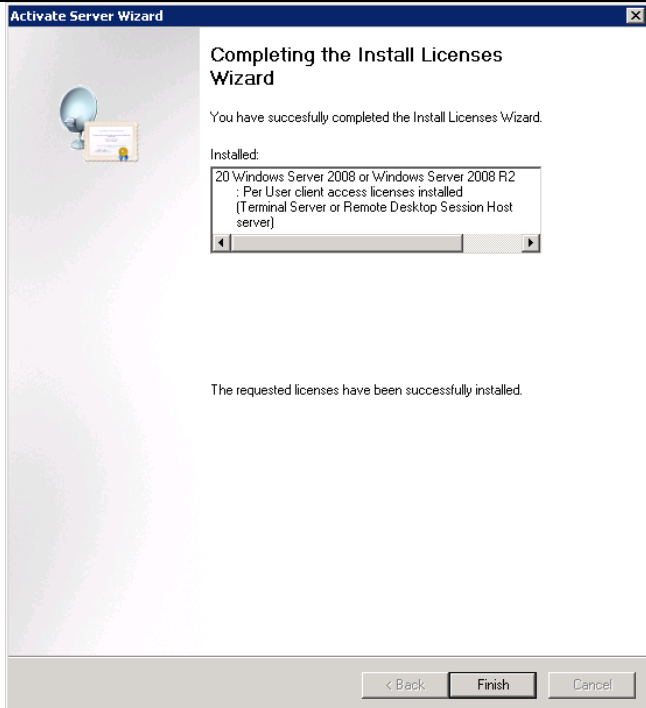
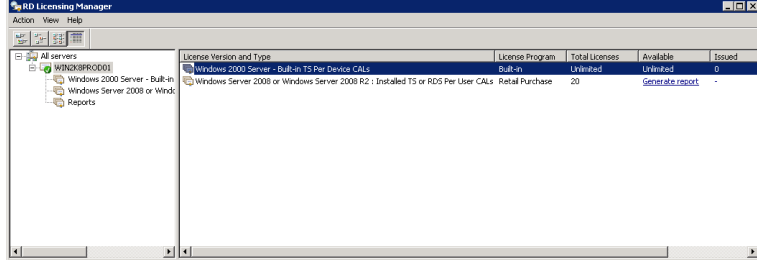
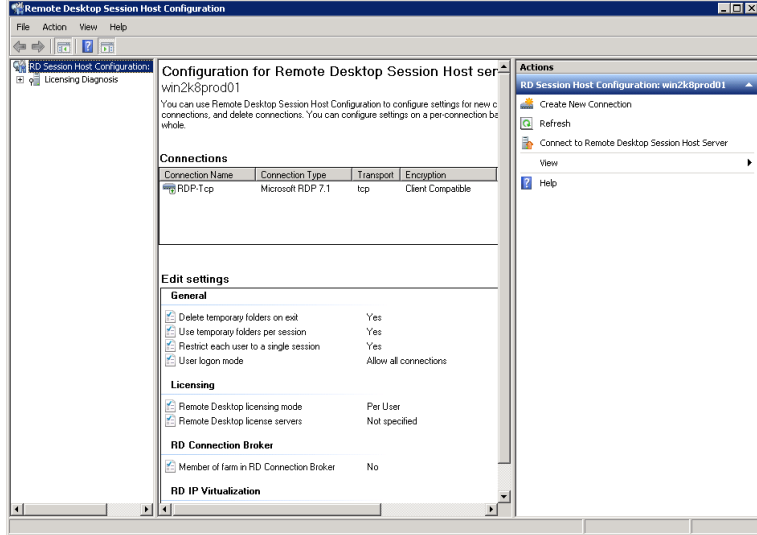
# CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Provide your company information.</p>	 <p><b>Activate Server Wizard</b></p> <p><b>Company Information</b> Provide the requested company information.</p> <p>Enter your name, company name, and country/region information. This information is required to proceed.</p> <p>First name: <input type="text"/></p> <p>Last name: <input type="text"/></p> <p>Company: <input type="text"/></p> <p>Country or Region: <input type="text"/></p> <p> Name and company information is used only by Microsoft to help you if you need assistance. Country/Region is required to comply with United States export restrictions. For more information, see <a href="#">Remote Desktop License Management and Your Privacy</a>.</p> <p>&lt; Back   Next &gt;   Cancel</p>
<p>Provide your contact information and click Next.</p>	 <p><b>Activate Server Wizard</b></p> <p><b>Company Information</b> Enter this optional information.</p> <p>E-mail: <input type="text"/></p> <p>Organizational unit: <input type="text"/></p> <p>Company address: <input type="text"/></p> <p>City: <input type="text"/></p> <p>State/province: <input type="text"/></p> <p>Postal code: <input type="text"/></p> <p> If provided, the optional information entered on this page will only be used by Microsoft support professionals to help you if you need assistance. For more information, see <a href="#">Remote Desktop License Management and Your Privacy</a>.</p> <p>&lt; Back   Next &gt;   Cancel</p>

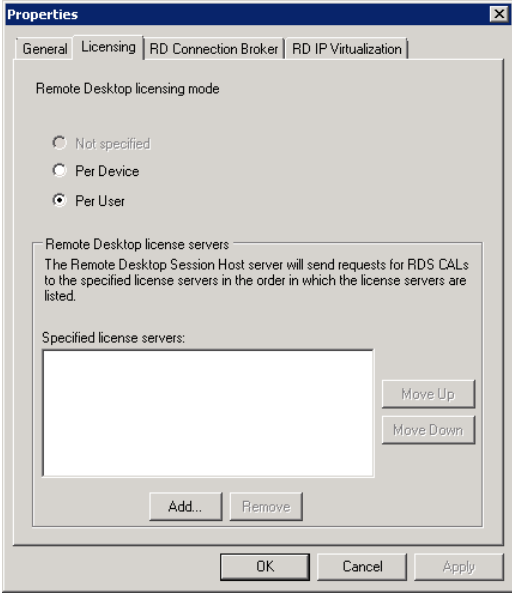
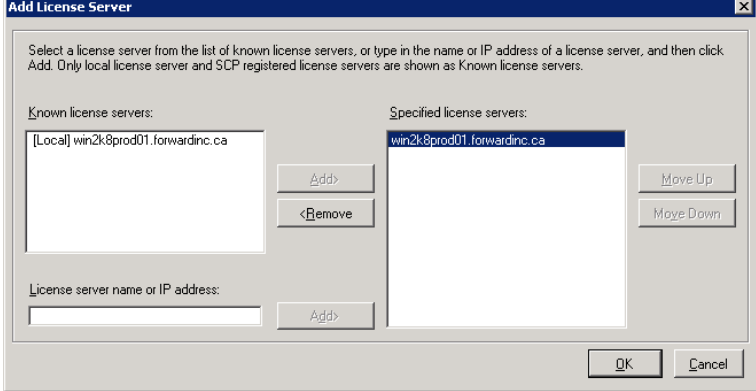
<p>Click Next to start the Install Licenses Wizard.</p>	
<p>Click Next.</p>	

## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

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

<p>Click Finish.</p>																
<p>Your RD Licensing Manager should be activated now and there should be a valid license displayed.</p>	 <table><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</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	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	20	Unlimited	0												
<p>Start Remote Desktop Session Host Configuration from Start/Administrative Tools/Remote Desktop Services.</p> <p>Double click Remote Desktop license servers.</p>																

## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

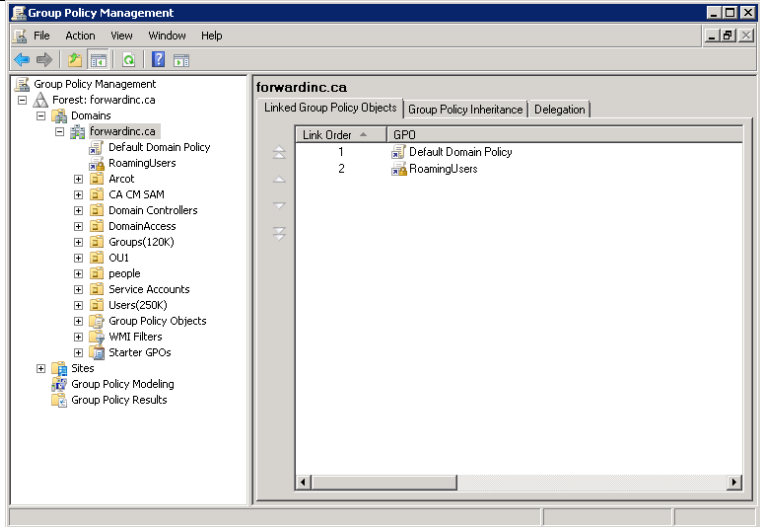
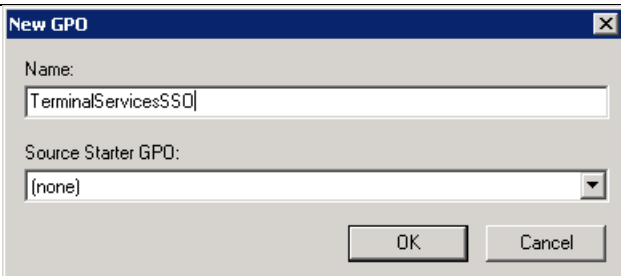
<p>Click Add.</p>	
<p>Add license server/servers available in your organization and click OK.</p> <p>Note that in MS Remote Desktop Session Host and Session server are on the same computer.</p>	

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

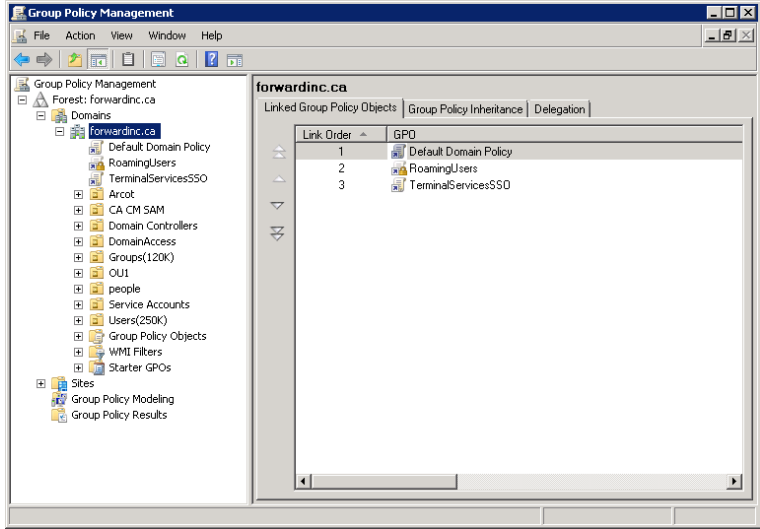
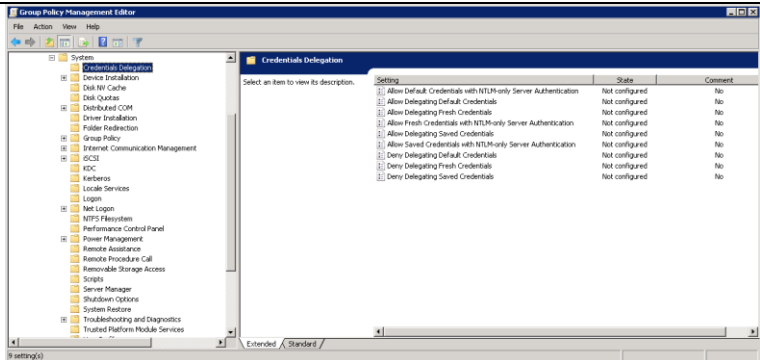
## Enable Single Sign-On For Terminal Server Connections

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.

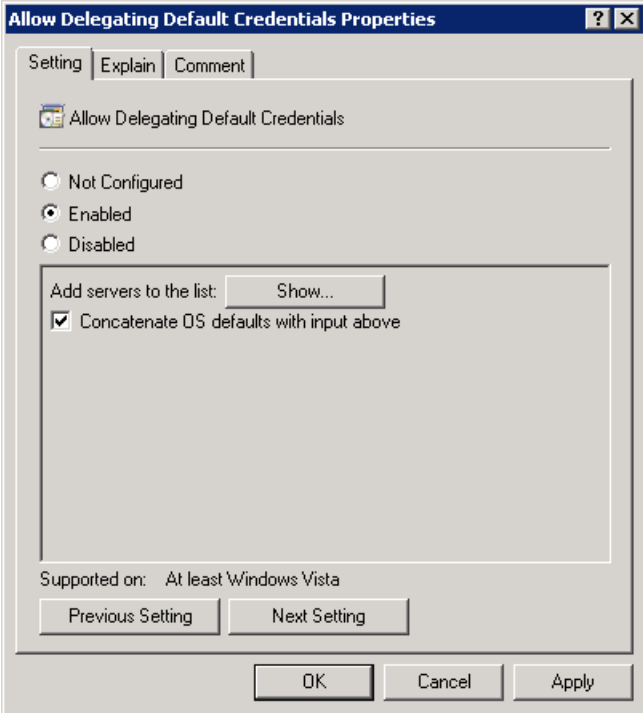
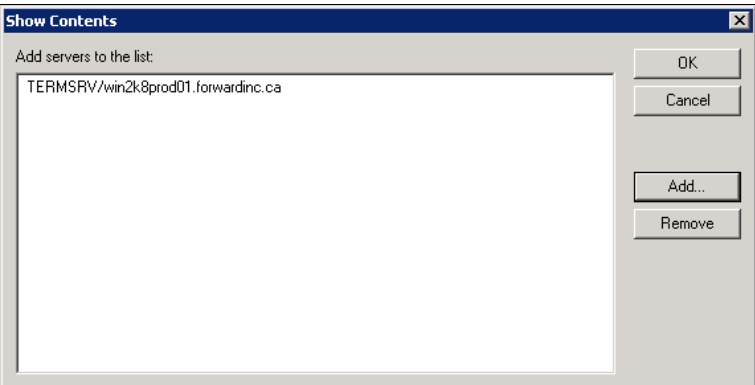
Single Sign-On is enabled through a Domain Group Policy.

<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>	

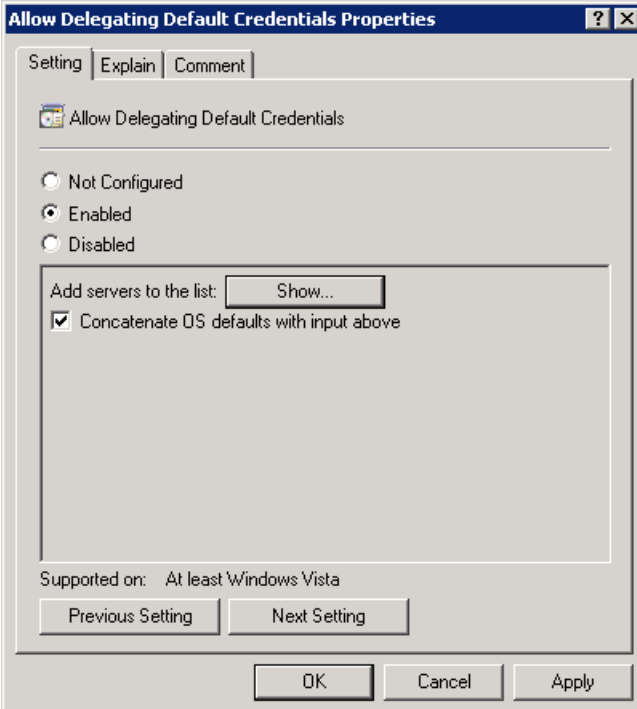
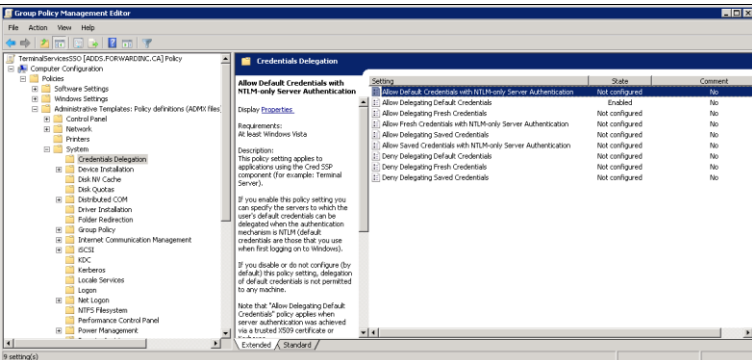
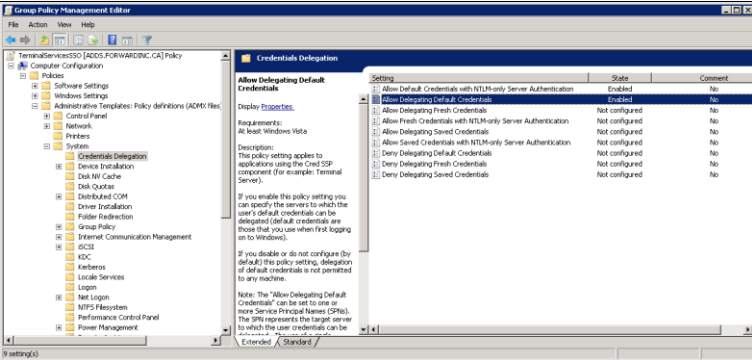
## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<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 1406 1024"> <thead> <tr> <th>Setting</th> <th>Status</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>1. Allow Default Credentials with NTLM-only Server Authentication</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>2. Allow Delegating Default Credentials</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>3. Allow Delegating Fresh Credentials</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>4. Allow Fresh Credentials with NTLM-only Server Authentication</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>5. Allow Delegating Served Credentials</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>6. Allow Served Credentials with NTLM-only Server Authentication</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>7. Deny Delegating Default Credentials</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>8. Deny Delegating Fresh Credentials</td> <td>Not configured</td> <td>No</td> </tr> <tr> <td>9. Deny Delegating Served Credentials</td> <td>Not configured</td> <td>No</td> </tr> </tbody> </table>	Setting	Status	Comment	1. Allow Default Credentials with NTLM-only Server Authentication	Not configured	No	2. Allow Delegating Default Credentials	Not configured	No	3. Allow Delegating Fresh Credentials	Not configured	No	4. Allow Fresh Credentials with NTLM-only Server Authentication	Not configured	No	5. Allow Delegating Served Credentials	Not configured	No	6. Allow Served Credentials with NTLM-only Server Authentication	Not configured	No	7. Deny Delegating Default Credentials	Not configured	No	8. Deny Delegating Fresh Credentials	Not configured	No	9. Deny Delegating Served Credentials	Not configured	No
Setting	Status	Comment																													
1. Allow Default Credentials with NTLM-only Server Authentication	Not configured	No																													
2. Allow Delegating Default Credentials	Not configured	No																													
3. Allow Delegating Fresh Credentials	Not configured	No																													
4. Allow Fresh Credentials with NTLM-only Server Authentication	Not configured	No																													
5. Allow Delegating Served Credentials	Not configured	No																													
6. Allow Served Credentials with NTLM-only Server Authentication	Not configured	No																													
7. Deny Delegating Default Credentials	Not configured	No																													
8. Deny Delegating Fresh Credentials	Not configured	No																													
9. Deny Delegating Served Credentials	Not configured	No																													

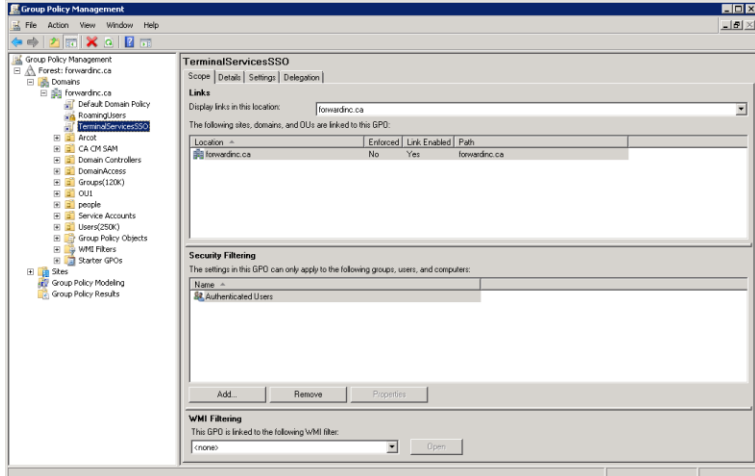
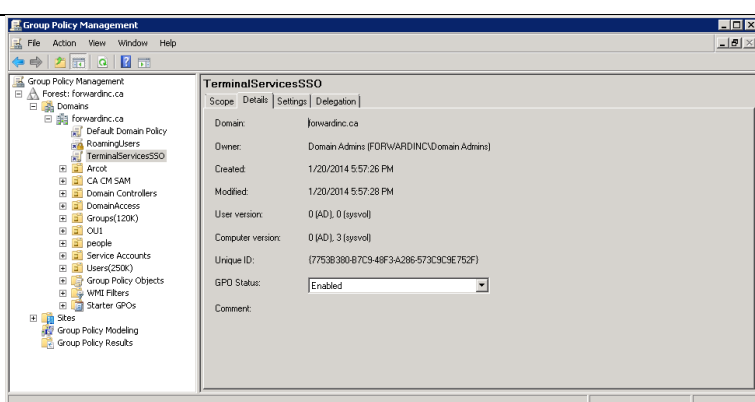
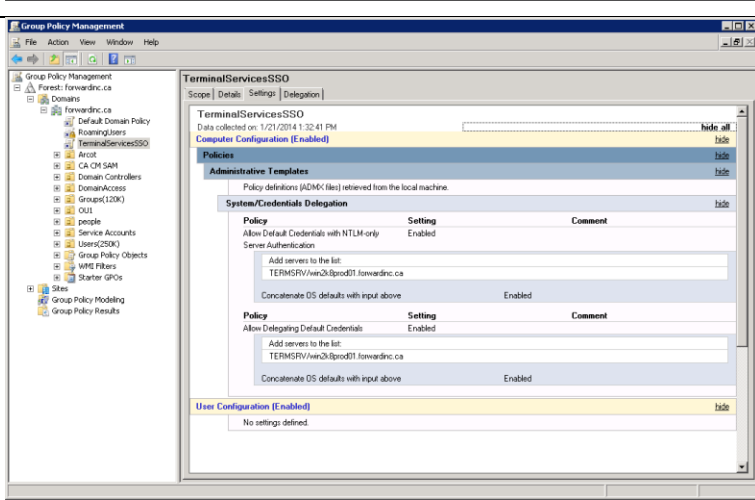


<p>Select “Enabled”,</p> <p>Click Show next to add servers to the list.</p>	
<p>Add your JumpBox server to the list.</p> <p>User TERMSRV\servername format.</p> <p>Click OK.</p>	

## 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](http://support.ca.com).

Search for **TEC583462** on [support.ca.com](http://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.

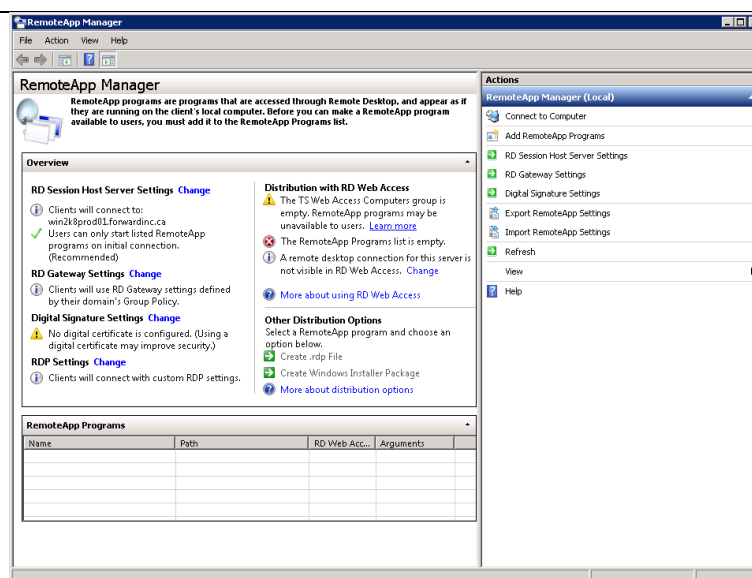
CA ControlMinder web interface can be configured as a RemoteApp on the JumpBox server so the end user can easily access the SAM functionality.

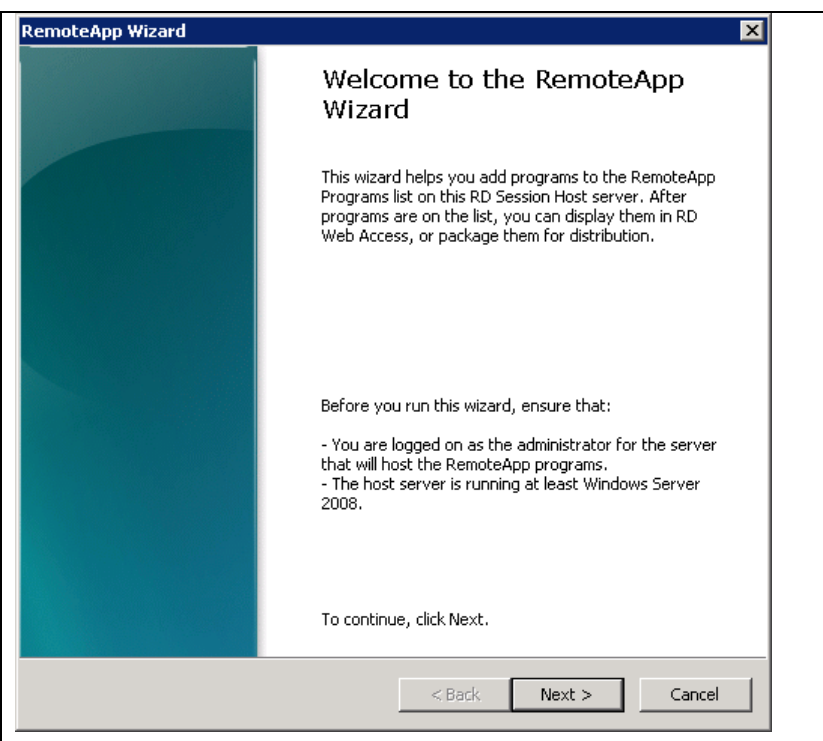
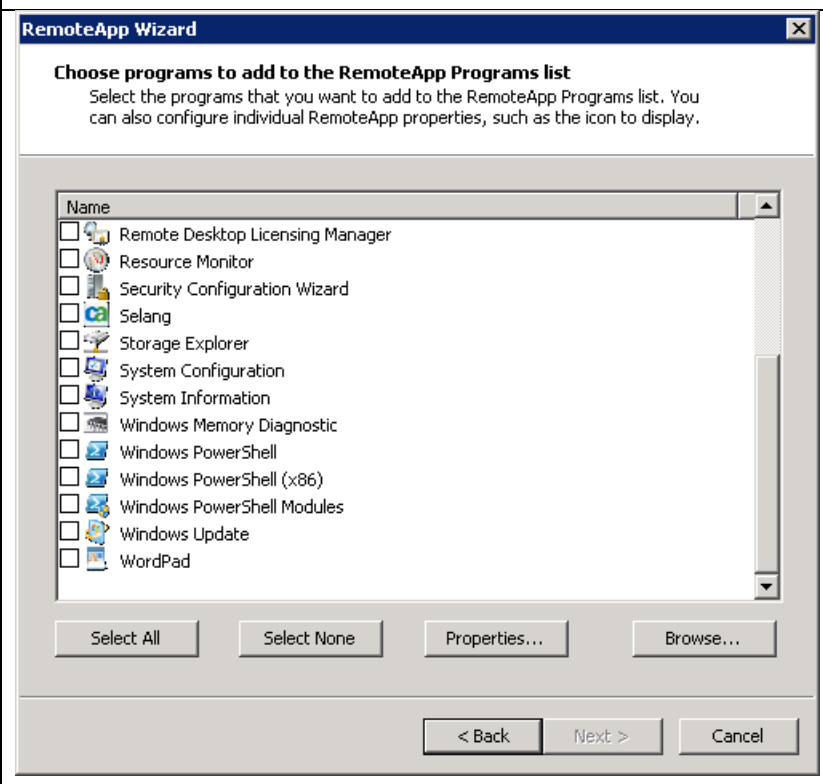
Follow the steps detailed below to create a RemoteApp.

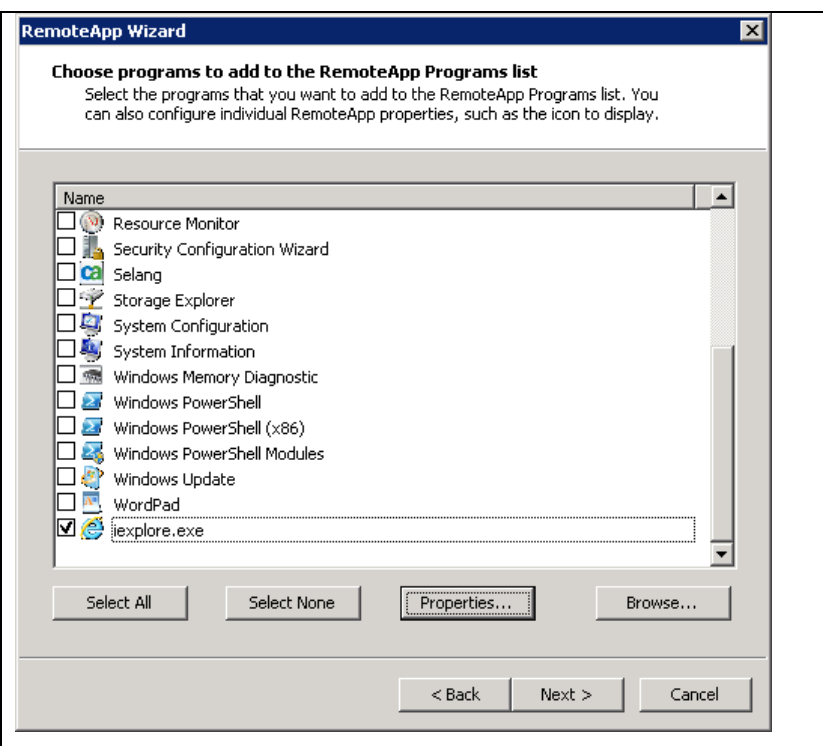
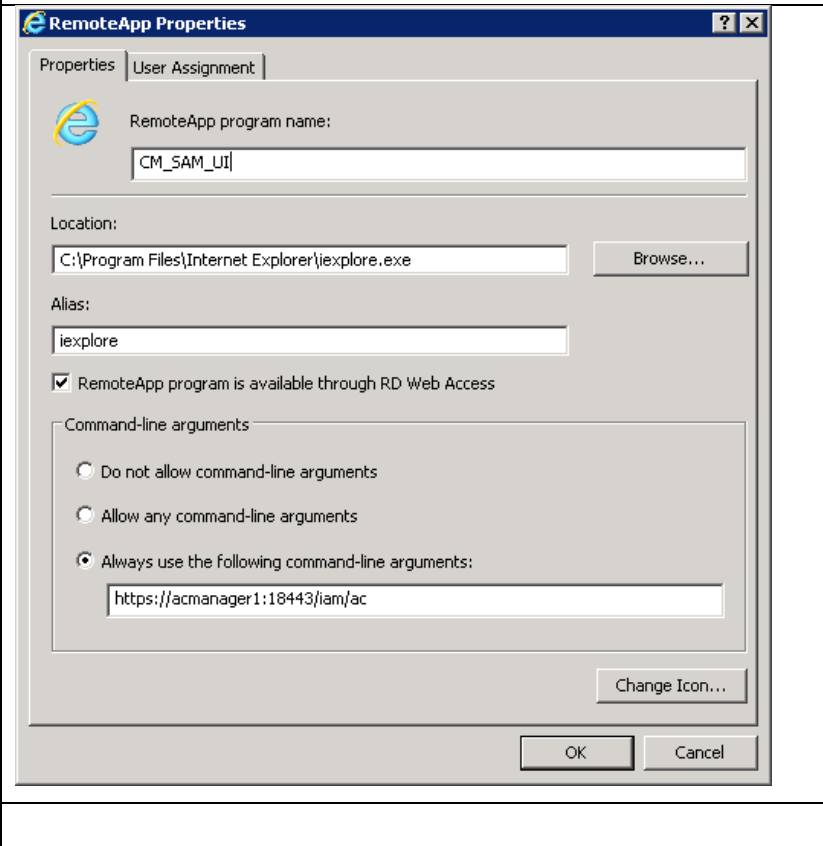
Connect to the JumpBox server.

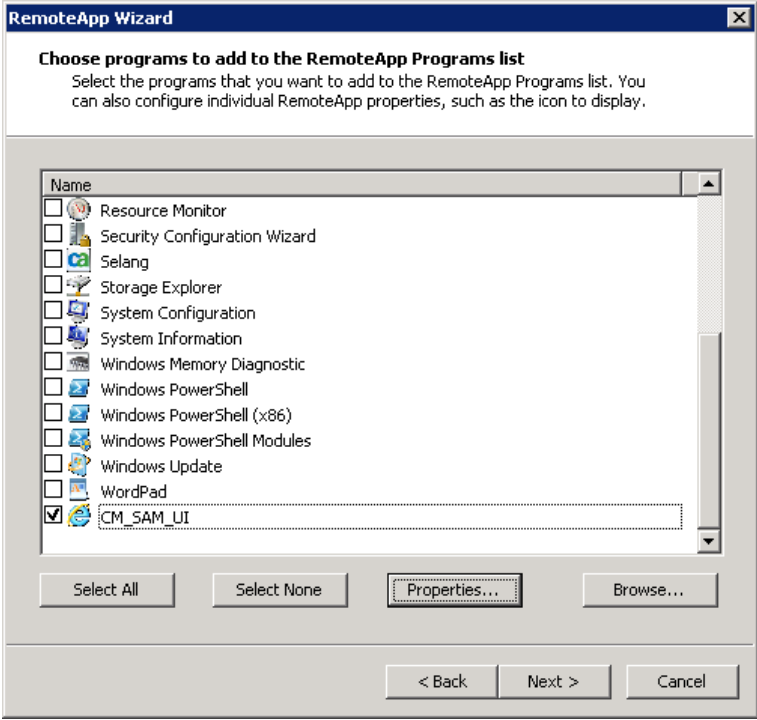
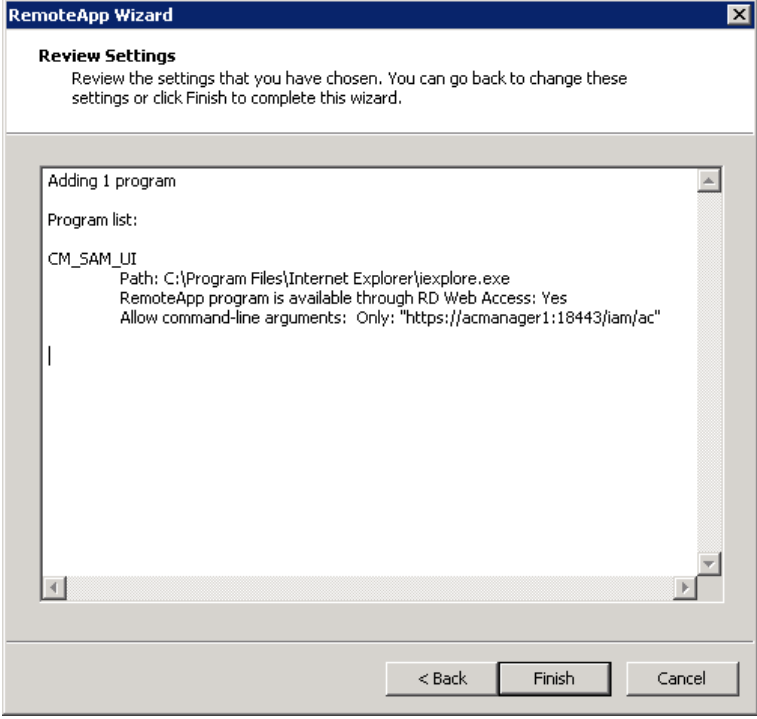
Applications are configured as RemoteApp using the TS RemoteApp Manager tool.

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



<p>Click “Add RemoteApp Program”.</p> <p>This will open RemoteApp Wizard.</p> <p>Click Next to continue.</p>	 <p>The screenshot shows the 'RemoteApp Wizard' window. The title bar says 'RemoteApp Wizard'. The main text reads: 'Welcome to the RemoteApp Wizard'. Below this, it says: '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.' Further down, it says: 'Before you run this wizard, ensure that:' followed by a bulleted list: '- You are logged on as the administrator for the server that will host the RemoteApp programs.' and '- The host server is running at least Windows Server 2008.' At the bottom, it says: 'To continue, click Next.' There are three buttons at the bottom: '&lt; Back', 'Next &gt;', and 'Cancel'.</p>
<p>Browse for the internet browser you want to use.</p> <p>We will be using MS Internet Explorer for the purpose of this guide.</p>	 <p>The screenshot shows the 'RemoteApp Wizard' window at the 'Choose programs to add to the RemoteApp Programs list' step. The title bar says 'RemoteApp Wizard'. The main text reads: 'Choose programs to add to the RemoteApp Programs list'. Below this, it says: '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.' There is a list box with a 'Name' header containing the following items: 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. Each item has a checkbox to its left. Below the list box are four buttons: 'Select All', 'Select None', 'Properties...', and 'Browse...'. At the bottom of the window are three buttons: '&lt; Back', 'Next &gt;', and 'Cancel'.</p>

<p>Click Properties...</p>	 <p>The RemoteApp Wizard dialog box is shown. It has a title bar 'RemoteApp Wizard' and a close button. The main text says 'Choose programs to add to the RemoteApp Programs list' and '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 this is a list box with a 'Name' header. The list contains the following items: 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, WordPad, and iexplore.exe. The 'iexplore.exe' item is selected with a checkmark. At the bottom of the list box are buttons 'Select All', 'Select None', 'Properties...', and 'Browse...'. Below the list box are navigation buttons '&lt; Back', 'Next &gt;', and 'Cancel'.</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>	 <p>The RemoteApp Properties dialog box is shown. It has a title bar 'RemoteApp Properties' and standard window controls. It has two tabs: 'Properties' and 'User Assignment'. The 'Properties' tab is active. It contains the following fields: 'RemoteApp program name:' with the value 'CM_SAM_UI'; 'Location:' with the value 'C:\Program Files\Internet Explorer\iexplore.exe' and a 'Browse...' button; 'Alias:' with the value 'iexplore'; a checked checkbox 'RemoteApp program is available through RD Web Access'; and a section for 'Command-line arguments' with three radio buttons: 'Do not allow command-line arguments', 'Allow any command-line arguments', and 'Always use the following command-line arguments:'. The third option is selected, and the text 'https://acmanager1:18443/iam/ac' is entered in the text box below it. There is a 'Change Icon...' button at the bottom right. At the very bottom are 'OK' and 'Cancel' buttons.</p>

<p>Click Next.</p>	 <p><b>RemoteApp Wizard</b></p> <p><b>Choose programs to add to the RemoteApp Programs list</b> 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.</p> <p>Name</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Resource Monitor</li> <li><input type="checkbox"/> Security Configuration Wizard</li> <li><input type="checkbox"/> Selang</li> <li><input type="checkbox"/> Storage Explorer</li> <li><input type="checkbox"/> System Configuration</li> <li><input type="checkbox"/> System Information</li> <li><input type="checkbox"/> Windows Memory Diagnostic</li> <li><input type="checkbox"/> Windows PowerShell</li> <li><input type="checkbox"/> Windows PowerShell (x86)</li> <li><input type="checkbox"/> Windows PowerShell Modules</li> <li><input type="checkbox"/> Windows Update</li> <li><input type="checkbox"/> WordPad</li> <li><input checked="" type="checkbox"/> CM_SAM_UI</li> </ul> <p>Select All    Select None    Properties...    Browse...</p> <p>&lt; Back    Next &gt;    Cancel</p>
<p>Review the settings and click Finish if they are correct.</p>	 <p><b>RemoteApp Wizard</b></p> <p><b>Review Settings</b> 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</p> <p>Program list:</p> <p>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>&lt; Back    Finish    Cancel</p>

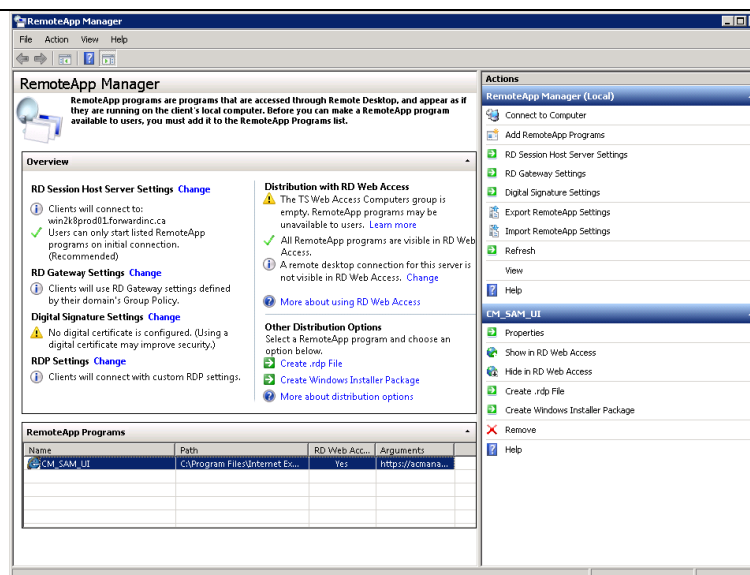


## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

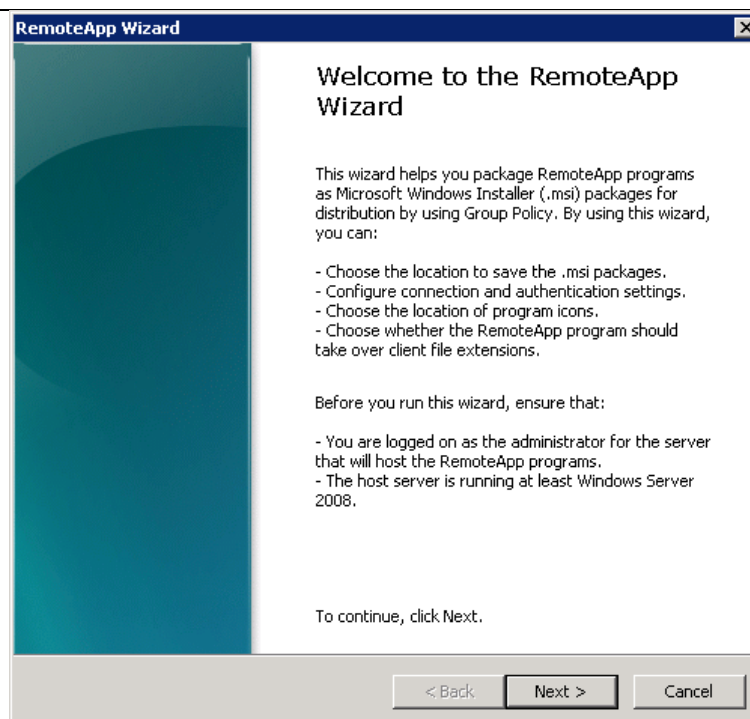
The new RemoteApp will appear in the list.

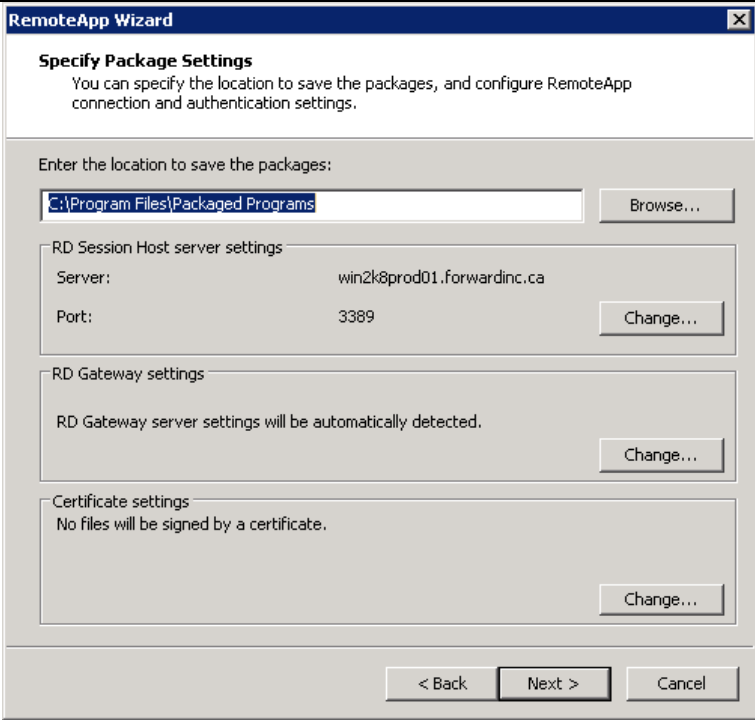
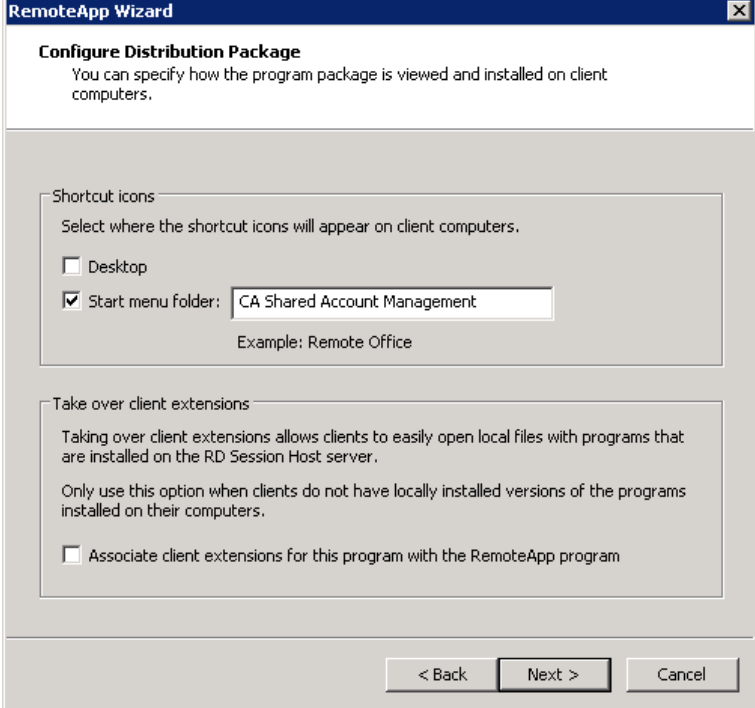
Right click on the application and select “Create Windows Installer Package.”

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

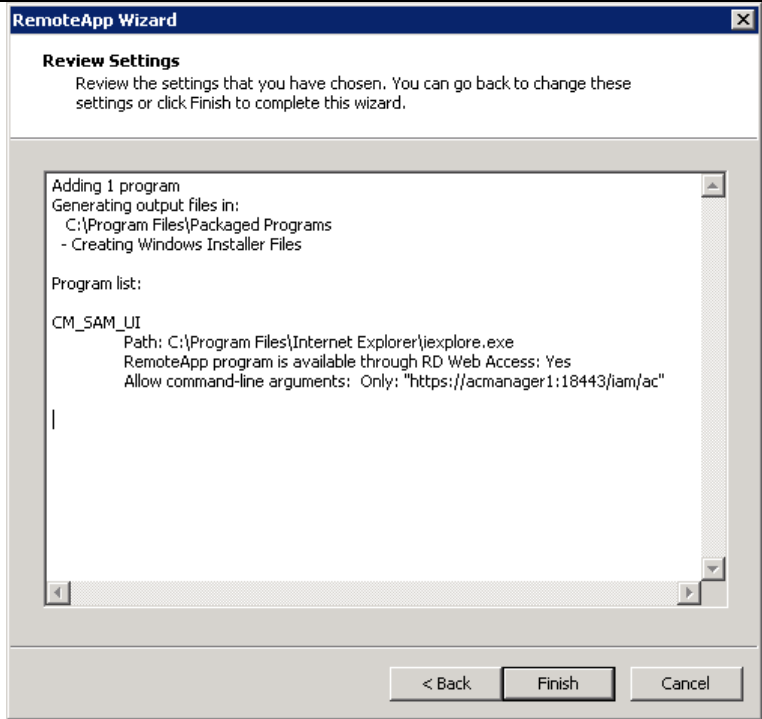
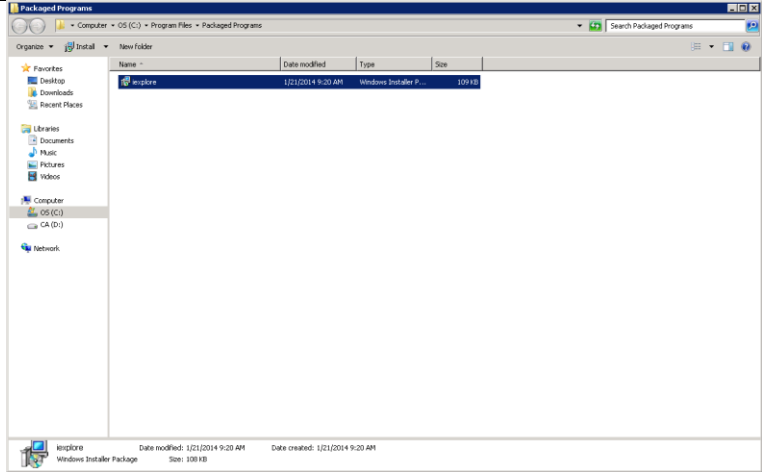


Click Next to start the wizard.



<p>Select the location to save the package to and click Next.</p>	 <p><b>RemoteApp Wizard</b></p> <p><b>Specify Package Settings</b> 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:</p> <p><input type="text" value="C:\Program Files\Packaged Programs"/> <input data-bbox="1226 478 1356 510" type="button" value="Browse..."/></p> <p>RD Session Host server settings</p> <p>Server: win2k8prod01.forwardinc.ca</p> <p>Port: 3389 <input data-bbox="1226 594 1356 625" type="button" value="Change..."/></p> <p>RD Gateway settings</p> <p>RD Gateway server settings will be automatically detected. <input data-bbox="1226 730 1356 762" type="button" value="Change..."/></p> <p>Certificate settings</p> <p>No files will be signed by a certificate. <input data-bbox="1226 867 1356 898" type="button" value="Change..."/></p> <p>&lt; Back <b>Next &gt;</b> Cancel</p>
<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><b>RemoteApp Wizard</b></p> <p><b>Configure Distribution Package</b> You can specify how the program package is viewed and installed on client computers.</p> <p>Shortcut icons</p> <p>Select where the shortcut icons will appear on client computers.</p> <p><input type="checkbox"/> Desktop</p> <p><input checked="" type="checkbox"/> Start menu folder: <input type="text" value="CA Shared Account Management"/>  Example: Remote Office</p> <p>Take over client extensions</p> <p>Taking over client extensions allows clients to easily open local files with programs that are installed on the RD Session Host server.</p> <p>Only use this option when clients do not have locally installed versions of the programs installed on their computers.</p> <p><input type="checkbox"/> Associate client extensions for this program with the RemoteApp program</p> <p>&lt; Back <b>Next &gt;</b> Cancel</p>

## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

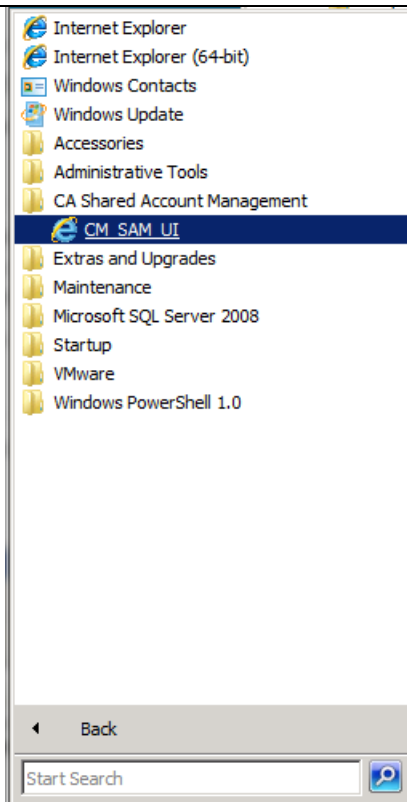
<p>Review the settings and click Finish.</p>	 <p><b>RemoteApp Wizard</b></p> <p><b>Review Settings</b></p> <p>Review the settings that you have chosen. You can go back to change these settings or click Finish to complete this wizard.</p> <p>Adding 1 program Generating output files in: C:\Program Files\Packaged Programs - Creating Windows Installer Files</p> <p>Program list:</p> <p>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>&lt; Back Finish Cancel</p>								
<p>MS Installer Package will be created.</p>	 <p><b>Packaged Programs</b></p> <table><tr><th>Name</th><th>Date modified</th><th>Type</th><th>Size</th></tr><tr><td>iexplore</td><td>1/21/2014 9:20 AM</td><td>Windows Installer P...</td><td>109 KB</td></tr></table> <p>File Explorer 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

Distribute and install this package on the end user workstation using the software distribution tool of your choice or manually.


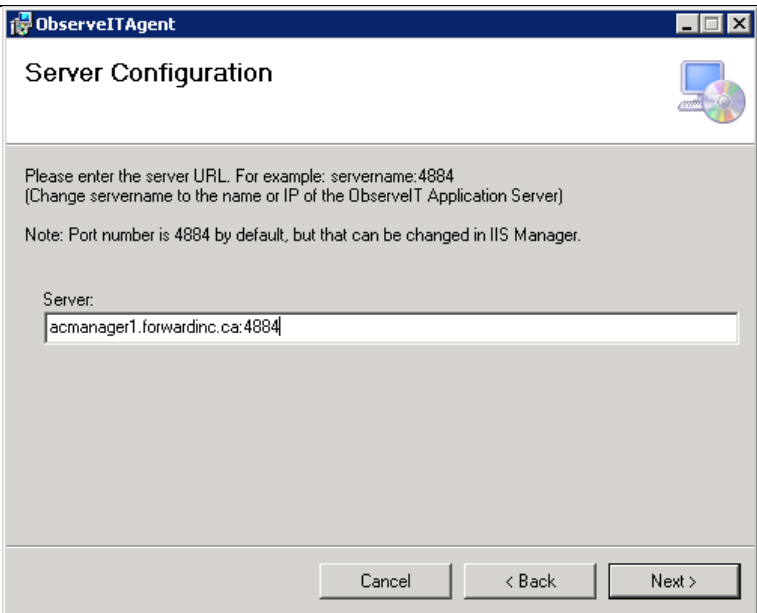
The RemoteApp will be available under Start Menu after installation.

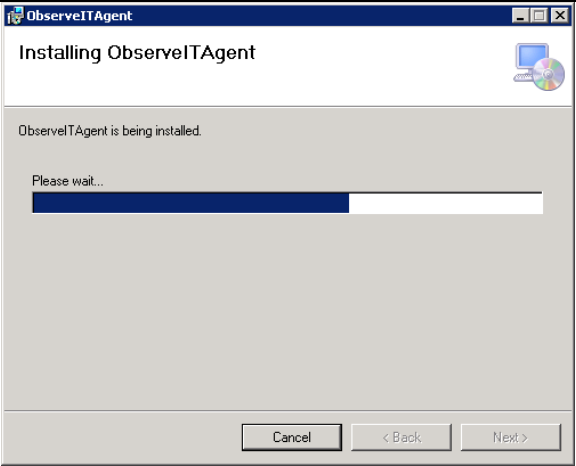
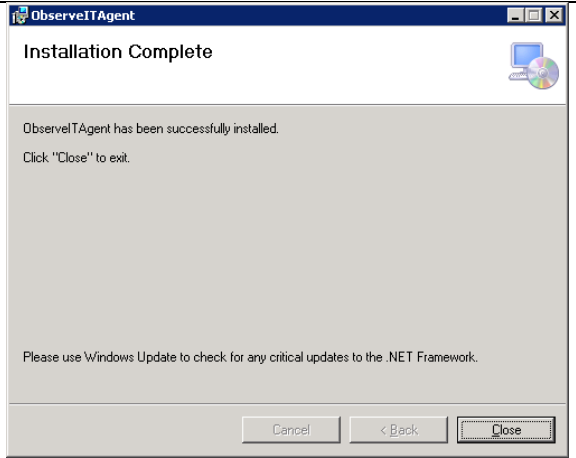

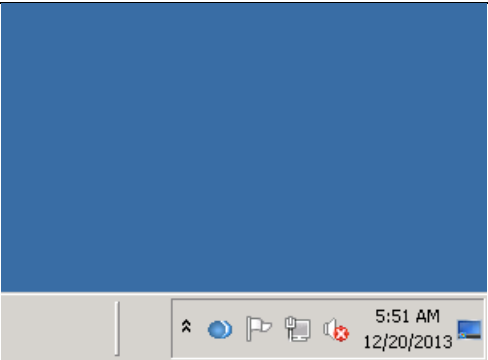
If you configured your MS Terminal Server for single sign on and ControlMinder for integrated MS Windows authentication then the RemoteApp will start CM user interface on the JumpBox and log you in automatically.



## 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>The ObserveITAgent Setup Wizard window is titled "ObserveITAgent". The main heading is "Welcome to the ObserveITAgent Setup Wizard". Below the heading, it states: "The installer will guide you through the steps required to install ObserveITAgent on your computer." A warning message is displayed: "WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law." At the bottom, there are three buttons: "Cancel", "&lt; Back", and "Next &gt;".</p>
<p>Provide the url of the Session Recording server.</p>	 <p>The ObserveITAgent Setup Wizard window is titled "ObserveITAgent". The main heading is "Server Configuration". Below the heading, it states: "Please enter the server URL. For example: servername:4884 (Change servername to the name or IP of the ObserveIT Application Server)". A note is displayed: "Note: Port number is 4884 by default, but that can be changed in IIS Manager." A text box labeled "Server:" contains the text "acmanager1.forwardinc.ca:4884". At the bottom, there are three buttons: "Cancel", "&lt; Back", and "Next &gt;".</p>

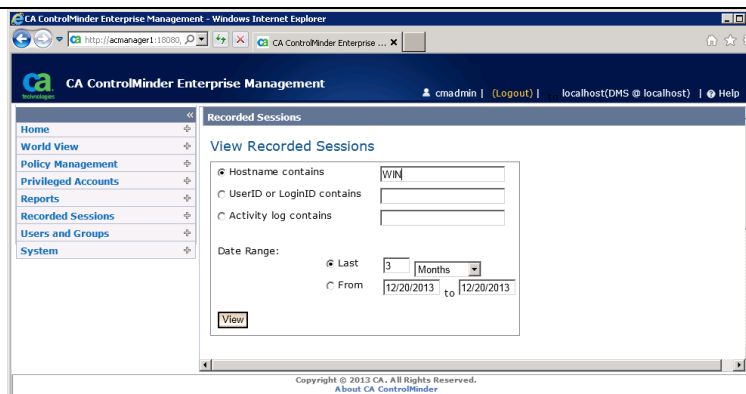
	
<p>Click Close to finish the installation.</p>	
<p>You will see a blue icon</p>  <p>on your taskbar that indicates that the session recording is running.</p> <p>All the sessions on this computer are being recorded from now on.</p> <p>This is the default configuration.</p>	

## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

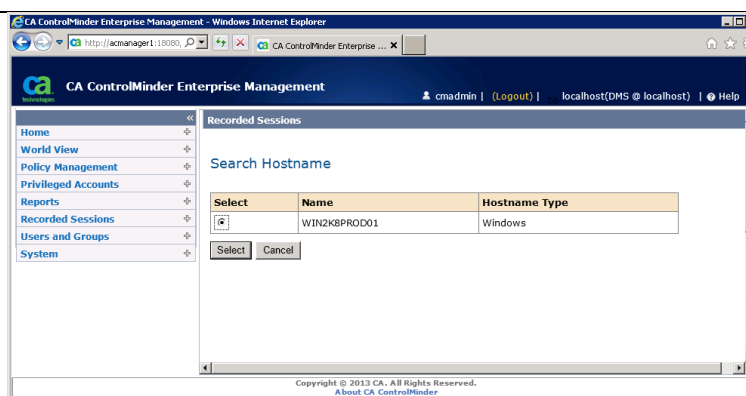
Start CM ENTM and verify that all the sessions on the JumpBox are being recorded.

Navigate to Recorded Sessions.

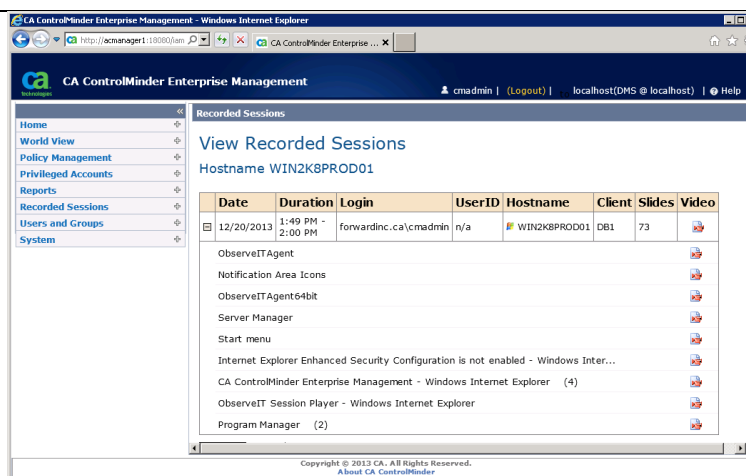
Search for the hostname of your JumpBox.



Select your JumpBox.



Verify that all the sessions initiated after the installation of the agent are being recorded.


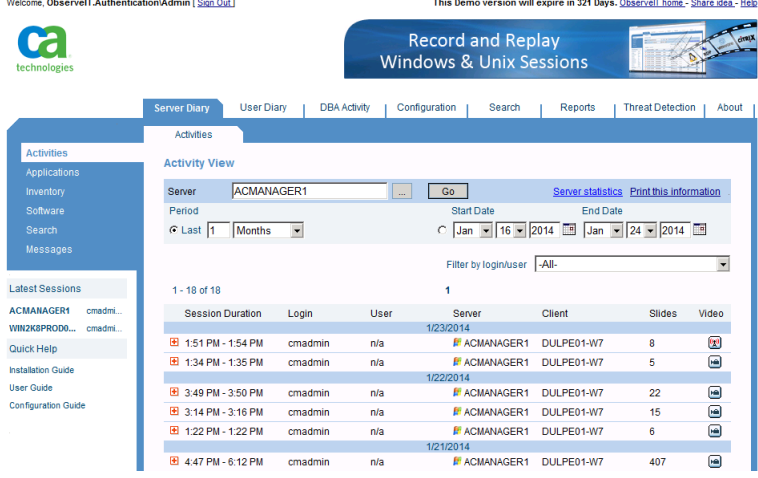


## Change The Recording Behavior

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.

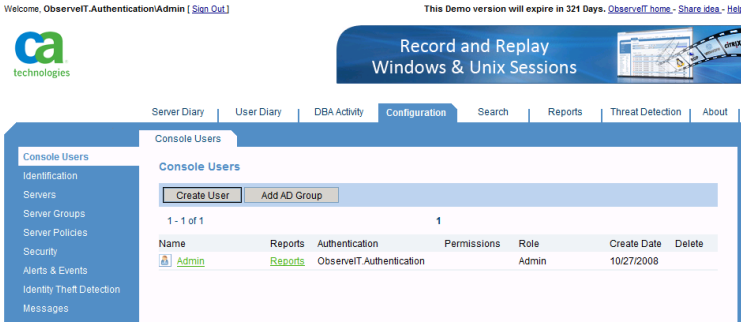
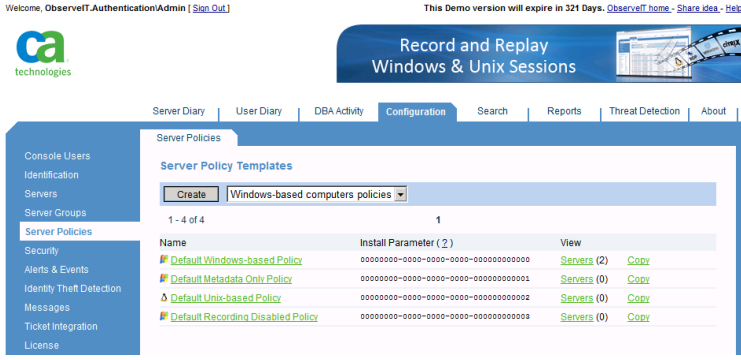
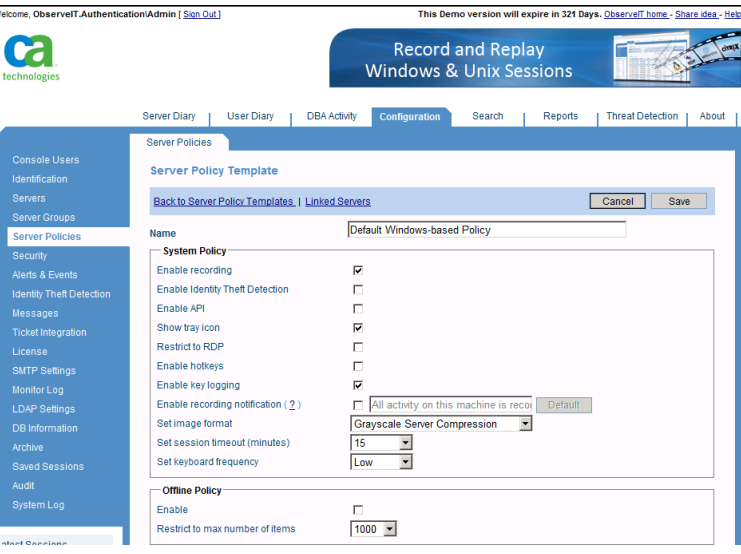
If you do not want to record everything that is happening on the JB then you can change the recording behavior to record only the sessions that are started from ControlMinder UI using login applications. In this case you will need to use the VBS scripts for the login applications that initiate the recording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

To change the recording behaviors follow these steps.

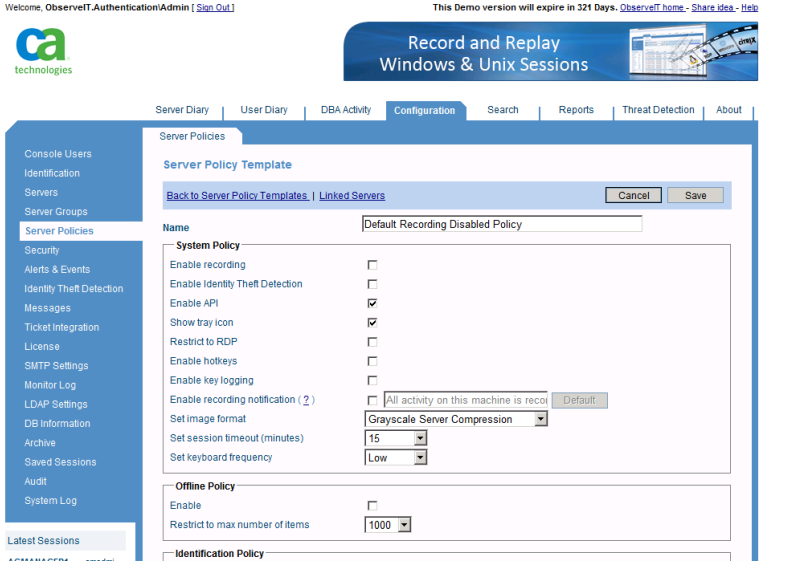
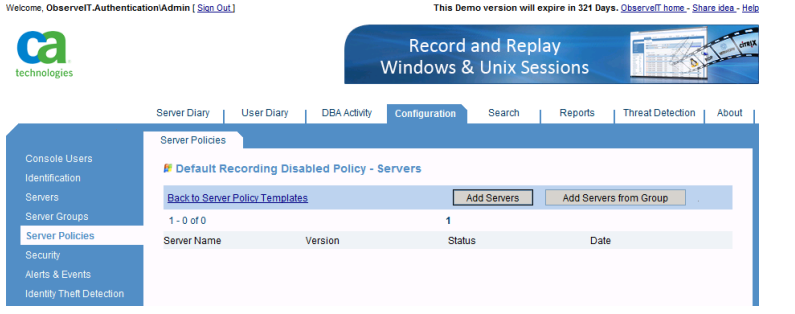
<p>Connect to the session recording console.</p>																																																		
<p>Go to Configuration tab.</p>	 <table border="1"> <thead> <tr> <th>Session Duration</th> <th>Login</th> <th>User</th> <th>Server</th> <th>Client</th> <th>Slides</th> <th>Video</th> </tr> </thead> <tbody> <tr> <td>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>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>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	1:51 PM - 1:54 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	8		1:34 PM - 1:35 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	5		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		4:47 PM - 6:12 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	407	
Session Duration	Login	User	Server	Client	Slides	Video																																												
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																																													
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																																													
4:47 PM - 6:12 PM	cmadmin	n/a	ACMANAGER1	DULPE01-W7	407																																													



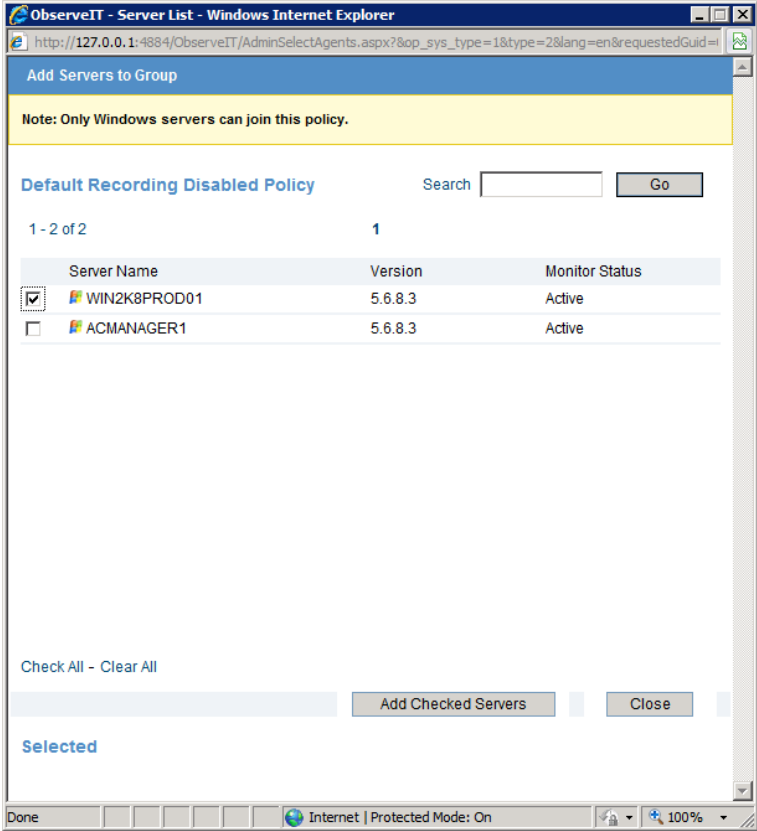
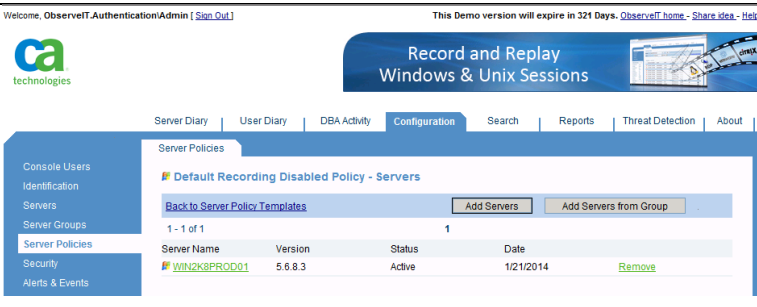
## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Select Server Policies.</p>	 <p>Welcome, ObserverrT.Authentication/Admin [Sign Out] This Demo version will expire in 321 Days. <a href="#">ObserverrT home</a> - <a href="#">Share idea</a> - <a href="#">Help</a></p> <p><b>Record and Replay Windows &amp; Unix Sessions</b></p> <p>Server Diary   User Diary   DBA Activity   <b>Configuration</b>   Search   Reports   Threat Detection   About</p> <p><b>Console Users</b></p> <p>Create User Add AD Group</p> <p>1 - 1 of 1 1</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Reports</th> <th>Authentication</th> <th>Permissions</th> <th>Role</th> <th>Create Date</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>Admin</td> <td>Reports</td> <td>ObserverrT.Authentication</td> <td></td> <td>Admin</td> <td>10/27/2008</td> <td></td> </tr> </tbody> </table>	Name	Reports	Authentication	Permissions	Role	Create Date	Delete	Admin	Reports	ObserverrT.Authentication		Admin	10/27/2008		
Name	Reports	Authentication	Permissions	Role	Create Date	Delete										
Admin	Reports	ObserverrT.Authentication		Admin	10/27/2008											
<p>The MS Windows agents are placed by default into “Default Windows-based Policy”</p>	 <p>Welcome, ObserverrT.Authentication/Admin [Sign Out] This Demo version will expire in 321 Days. <a href="#">ObserverrT home</a> - <a href="#">Share idea</a> - <a href="#">Help</a></p> <p><b>Record and Replay Windows &amp; Unix Sessions</b></p> <p>Server Diary   User Diary   DBA Activity   <b>Configuration</b>   Search   Reports   Threat Detection   About</p> <p><b>Server Policies</b></p> <p>Create Windows-based computers policies</p> <p>1 - 4 of 4 1</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Install Parameter (2)</th> <th>View</th> </tr> </thead> <tbody> <tr> <td>Default Windows-based Policy</td> <td>00000000-0000-0000-0000-000000000000</td> <td>Servers (2) <a href="#">Copy</a></td> </tr> <tr> <td>Default Metadata Only Policy</td> <td>00000000-0000-0000-0000-000000000001</td> <td>Servers (0) <a href="#">Copy</a></td> </tr> <tr> <td>Default Unix-based Policy</td> <td>00000000-0000-0000-0000-000000000002</td> <td>Servers (0) <a href="#">Copy</a></td> </tr> <tr> <td>Default Recording Disabled Policy</td> <td>00000000-0000-0000-0000-000000000003</td> <td>Servers (0) <a href="#">Copy</a></td> </tr> </tbody> </table>	Name	Install Parameter (2)	View	Default Windows-based Policy	00000000-0000-0000-0000-000000000000	Servers (2) <a href="#">Copy</a>	Default Metadata Only Policy	00000000-0000-0000-0000-000000000001	Servers (0) <a href="#">Copy</a>	Default Unix-based Policy	00000000-0000-0000-0000-000000000002	Servers (0) <a href="#">Copy</a>	Default Recording Disabled Policy	00000000-0000-0000-0000-000000000003	Servers (0) <a href="#">Copy</a>
Name	Install Parameter (2)	View														
Default Windows-based Policy	00000000-0000-0000-0000-000000000000	Servers (2) <a href="#">Copy</a>														
Default Metadata Only Policy	00000000-0000-0000-0000-000000000001	Servers (0) <a href="#">Copy</a>														
Default Unix-based Policy	00000000-0000-0000-0000-000000000002	Servers (0) <a href="#">Copy</a>														
Default Recording Disabled Policy	00000000-0000-0000-0000-000000000003	Servers (0) <a href="#">Copy</a>														
<p>This policy is configured to record all sessions.</p>	 <p>Welcome, ObserverrT.Authentication/Admin [Sign Out] This Demo version will expire in 321 Days. <a href="#">ObserverrT home</a> - <a href="#">Share idea</a> - <a href="#">Help</a></p> <p><b>Record and Replay Windows &amp; Unix Sessions</b></p> <p>Server Diary   User Diary   DBA Activity   <b>Configuration</b>   Search   Reports   Threat Detection   About</p> <p><b>Server Policies</b></p> <p>Server Policy Template</p> <p><a href="#">Back to Server Policy Templates</a>   <a href="#">Linked Servers</a> <span>Cancel Save</span></p> <p>Name: Default Windows-based Policy</p> <p><b>System Policy</b></p> <p>Enable recording <input checked="" type="checkbox"/>      Enable Identity Theft Detection <input type="checkbox"/>      Enable API <input type="checkbox"/>      Show tray icon <input checked="" type="checkbox"/>      Restrict to RDP <input type="checkbox"/>      Enable hotkeys <input type="checkbox"/>      Enable key logging <input checked="" type="checkbox"/>      Enable recording notification (2) <input type="checkbox"/> All activity on this machine is recorded <input type="button" value="Default"/>      Set image format: Grayscale Server Compression      Set session timeout (minutes): 15      Set keyboard frequency: Low</p> <p><b>Offline Policy</b></p> <p>Enable <input type="checkbox"/>      Restrict to max number of items: 1000</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>Click “Add Servers”</p>	

## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Select your JB Server and click “Add Checked Servers”.</p>	 <p><b>ObserveIT - Server List - Windows Internet Explorer</b></p> <p>http://127.0.0.1:4884/ObserveIT/AdminSelectAgents.aspx?&amp;op_sys_type=1&amp;type=2&amp;lang=en&amp;requestedGuid=</p> <p><b>Add Servers to Group</b></p> <p>Note: Only Windows servers can join this policy.</p> <p><b>Default Recording Disabled Policy</b> Search <input type="text"/> Go</p> <p>1 - 2 of 2 1</p> <table border="1"> <thead> <tr> <th></th> <th>Server Name</th> <th>Version</th> <th>Monitor Status</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>WIN2K8PROD01</td> <td>5.6.8.3</td> <td>Active</td> </tr> <tr> <td><input type="checkbox"/></td> <td>ACMANAGER1</td> <td>5.6.8.3</td> <td>Active</td> </tr> </tbody> </table> <p>Check All - Clear All</p> <p>Add Checked Servers Close</p> <p>Selected</p>		Server Name	Version	Monitor Status	<input checked="" type="checkbox"/>	WIN2K8PROD01	5.6.8.3	Active	<input type="checkbox"/>	ACMANAGER1	5.6.8.3	Active
	Server Name	Version	Monitor Status										
<input checked="" type="checkbox"/>	WIN2K8PROD01	5.6.8.3	Active										
<input type="checkbox"/>	ACMANAGER1	5.6.8.3	Active										
<p>Your JumpBox will now be recording only the sessions initiated through API. These are the sessions started by the recording VBS auto login scripts.</p>	 <p>Welcome, ObserveIT.AuthenticationAdmin [Sign Out] This Demo version will expire in 321 Days. ObserveIT home - Share Idea - Help</p> <p><b>Record and Replay Windows &amp; Unix Sessions</b></p> <p>Server Diary   User Diary   DBA Activity   Configuration   Search   Reports   Threat Detection   About</p> <p><b>Server Policies</b></p> <p>Default Recording Disabled Policy - Servers</p> <p>Back to Server Policy Templates Add Servers Add Servers from Group</p> <p>1 - 1 of 1 1</p> <table border="1"> <thead> <tr> <th>Server Name</th> <th>Version</th> <th>Status</th> <th>Date</th> </tr> </thead> <tbody> <tr> <td>WIN2K8PROD01</td> <td>5.6.8.3</td> <td>Active</td> <td>1/21/2014</td> </tr> </tbody> </table> <p>Remove</p>	Server Name	Version	Status	Date	WIN2K8PROD01	5.6.8.3	Active	1/21/2014				
Server Name	Version	Status	Date										
WIN2K8PROD01	5.6.8.3	Active	1/21/2014										

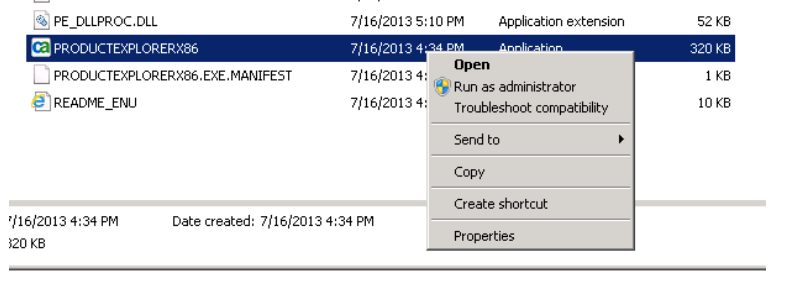
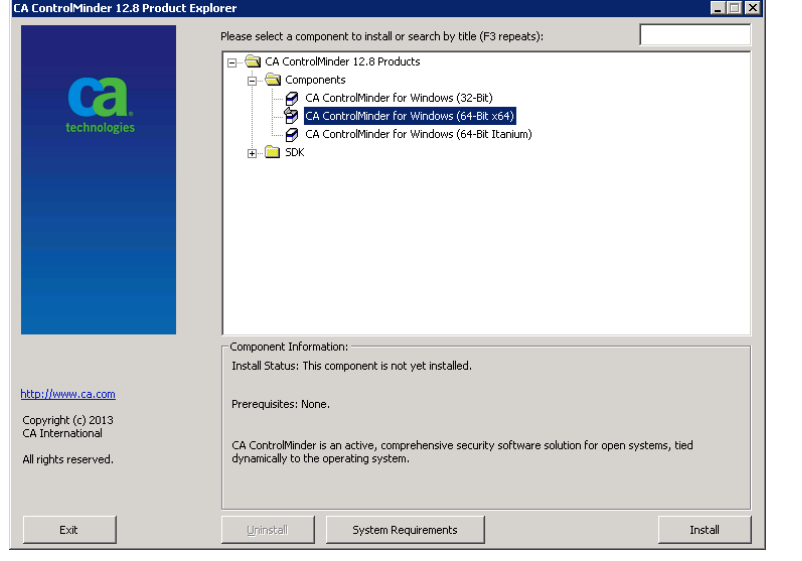
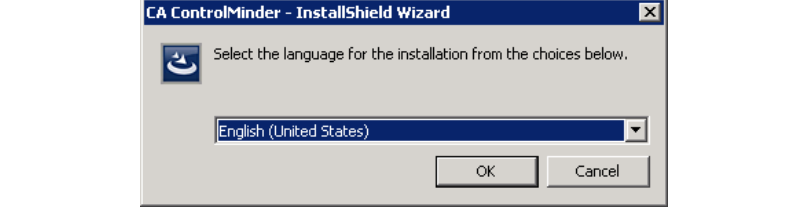
## Install ControlMinder Endpoint Software On The JumpBox

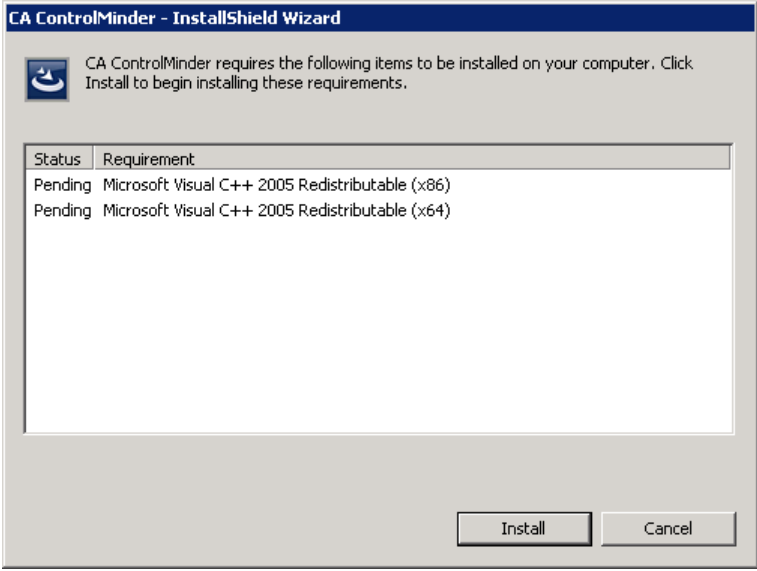
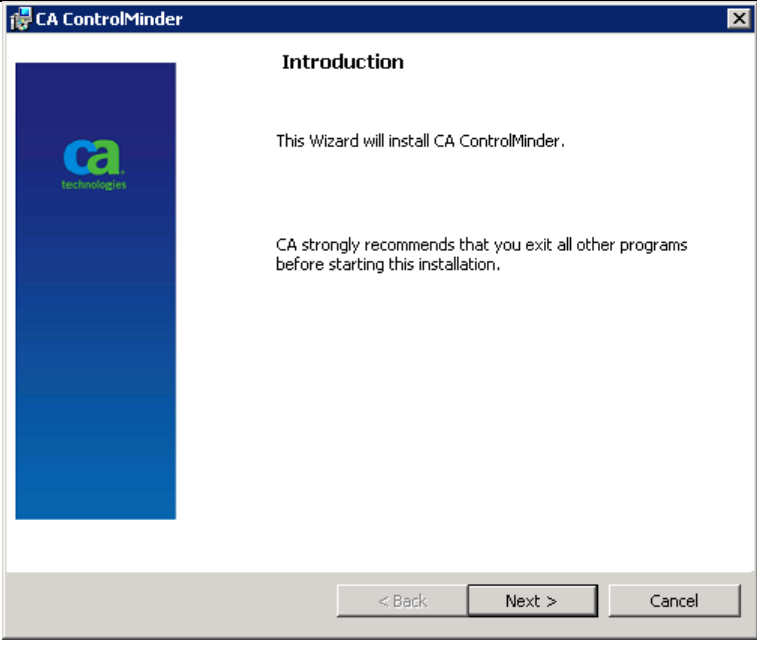
You can use ControlMinder Endpoint software to protect the JumpBox.

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

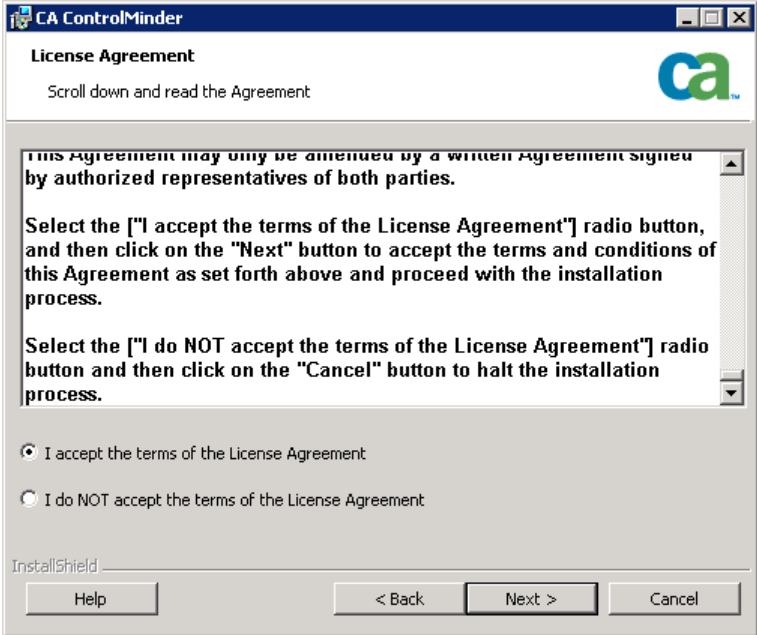
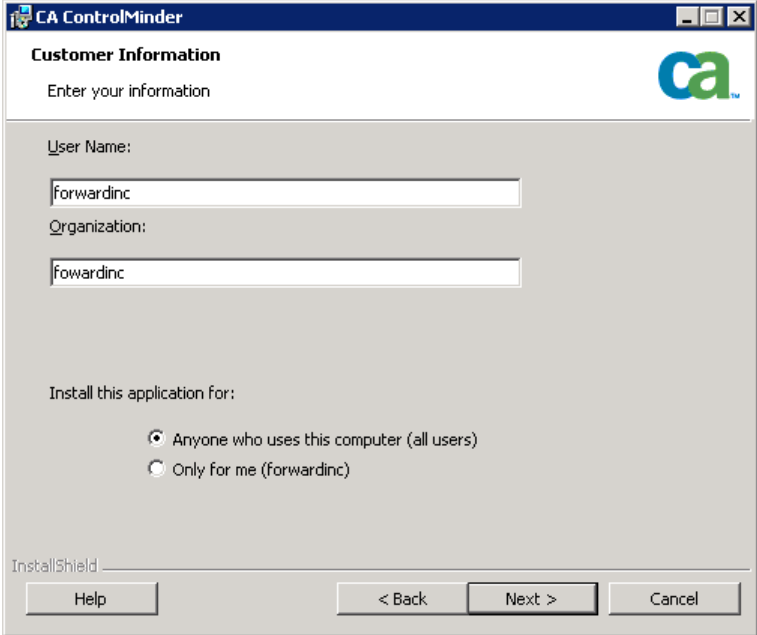
You must be a member of the local Administrators group to perform the installation of ControlMinder Endpoint components.

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.

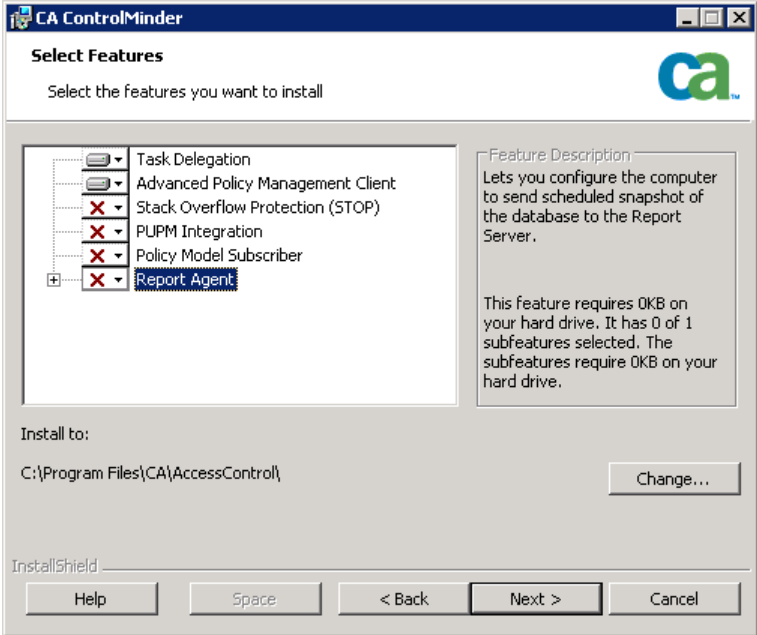
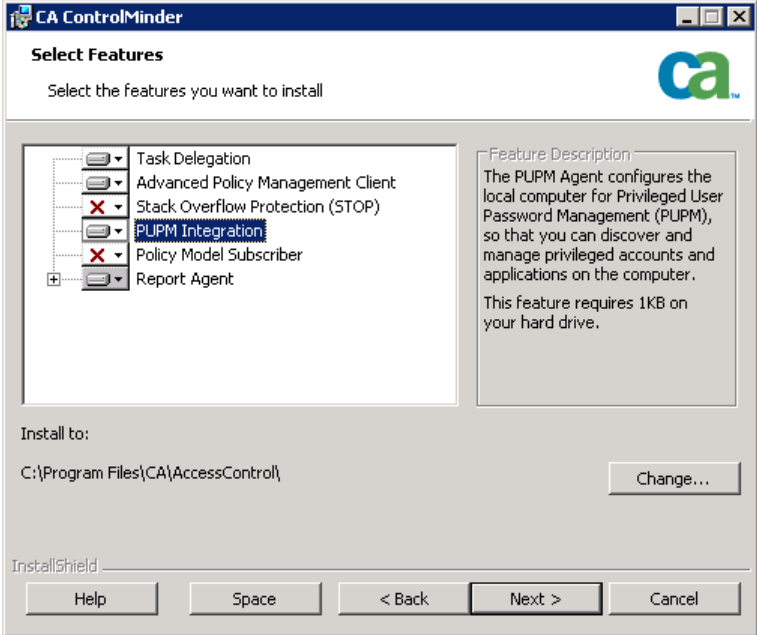
<p>Locate the PRODUCTEXPLORERX86.EXE executable. Right-click the executable and choose <u>Run as administrator</u> to start the installation.</p>	
<p>This example assumes that the endpoint is a 64-bit Intel/AMD architecture. From the Components folder of the Product Explorer, select <u>CA ControlMinder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

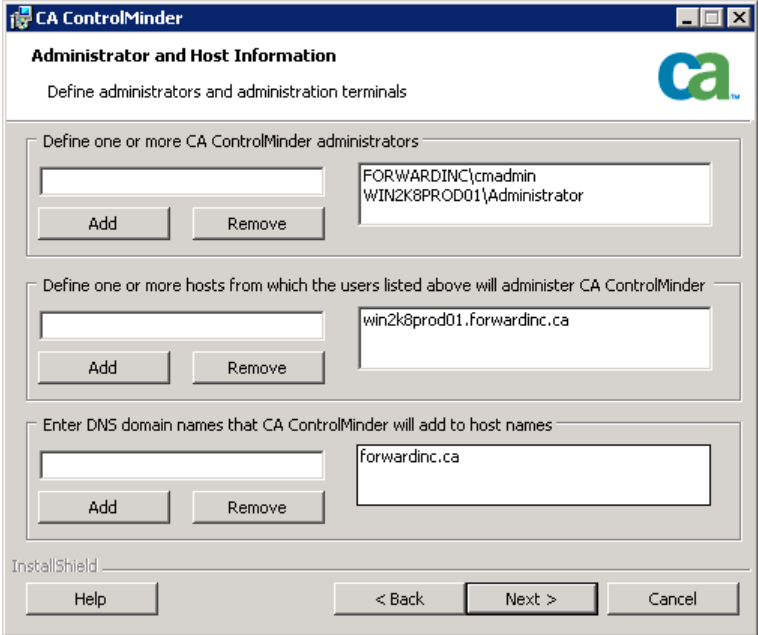
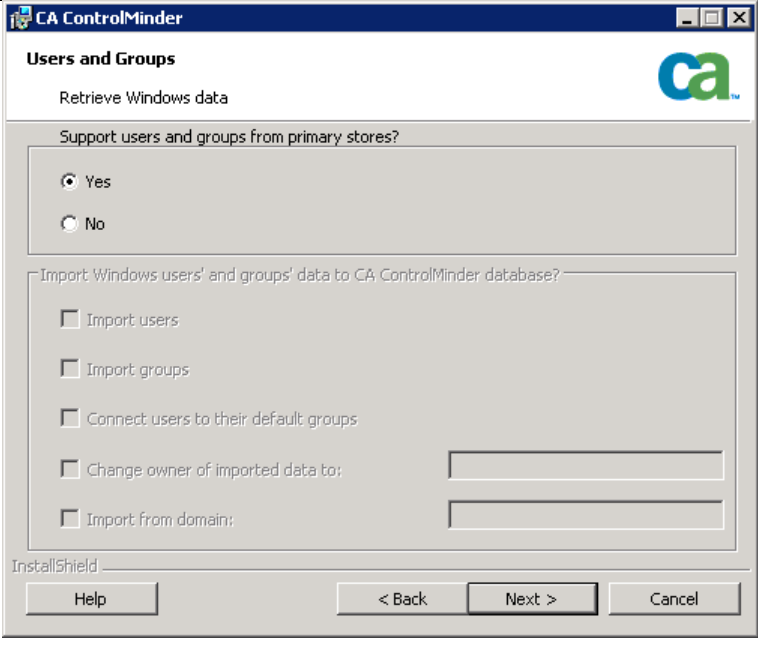
<p>If prompted to install Microsoft Visual C++ Redistributable libraries, click the Install button.</p>	
<p>Click the Next button to proceed with the ControlMinder endpoint software installation.</p>	

# 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>The screenshot shows the 'License Agreement' window of the CA ControlMinder installer. It contains a scrollable text area with the following text: 'This Agreement may only be amended by a written Agreement signed by authorized representatives of both parties. Select the ["I accept the terms of the License Agreement"] radio button, and then click on the "Next" button to accept the terms and conditions of this Agreement as set forth above and proceed with the installation process. Select the ["I do NOT accept the terms of the License Agreement"] radio button and then click on the "Cancel" button to halt the installation process.' Below the text are two radio buttons: 'I accept the terms of the License Agreement' (which is selected) and 'I do NOT accept the terms of the License Agreement'. At the bottom are buttons for 'Help', '&lt; Back', 'Next &gt;', and 'Cancel'.</p>
<p>Provide customer information.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'Customer Information' window of the CA ControlMinder installer. It prompts the user to 'Enter your information'. There are two text input fields: 'User Name:' with the value 'forwardinc' and 'Organization:' with the value 'fowardinc'. Below these fields, it asks 'Install this application for:' with two radio buttons: 'Anyone who uses this computer (all users)' (which is selected) and 'Only for me (forwardinc)'. At the bottom are buttons for 'Help', '&lt; Back', 'Next &gt;', and 'Cancel'.</p>

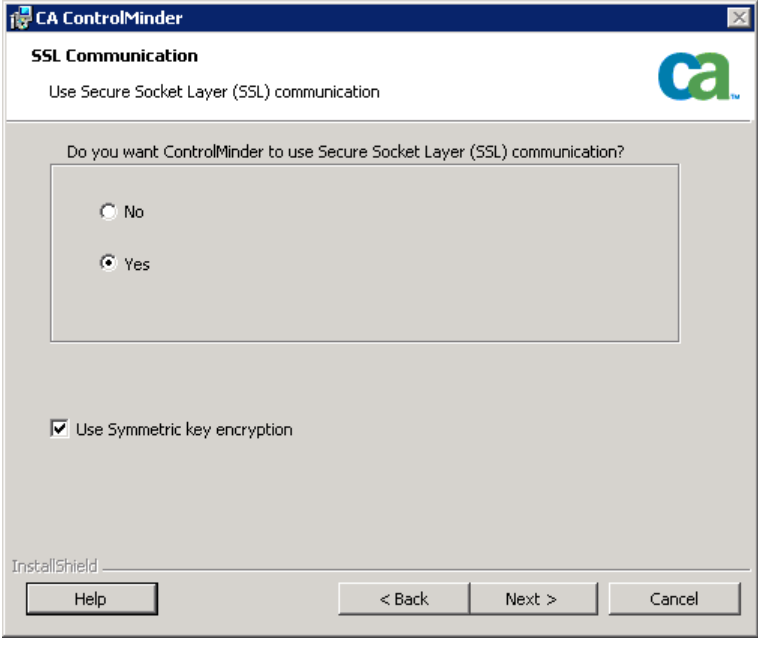
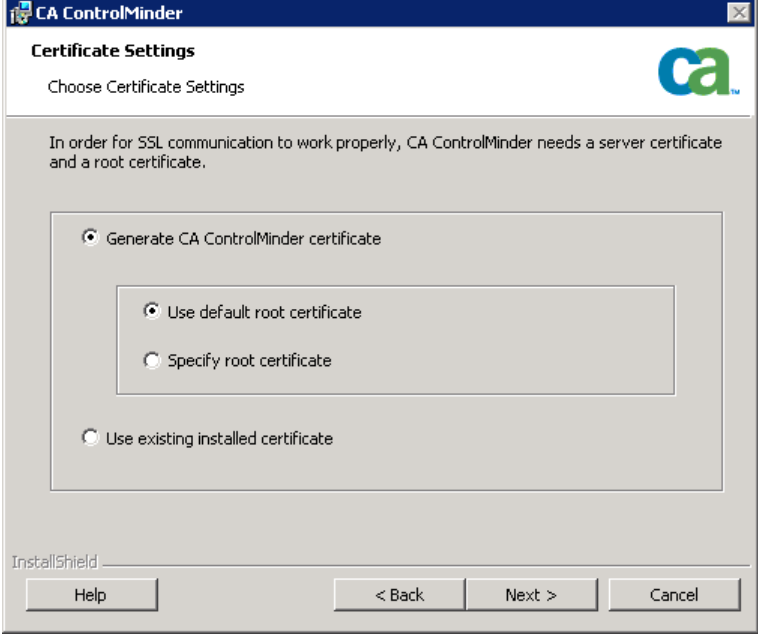
## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

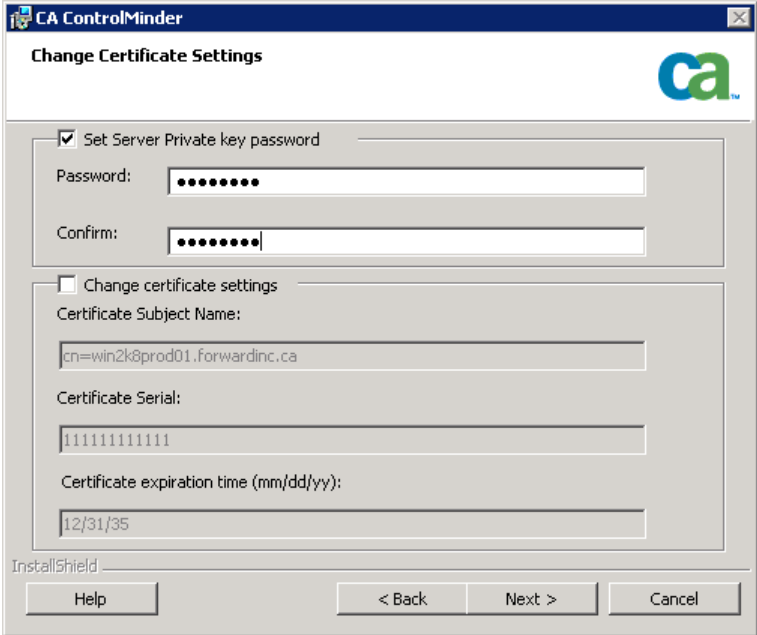
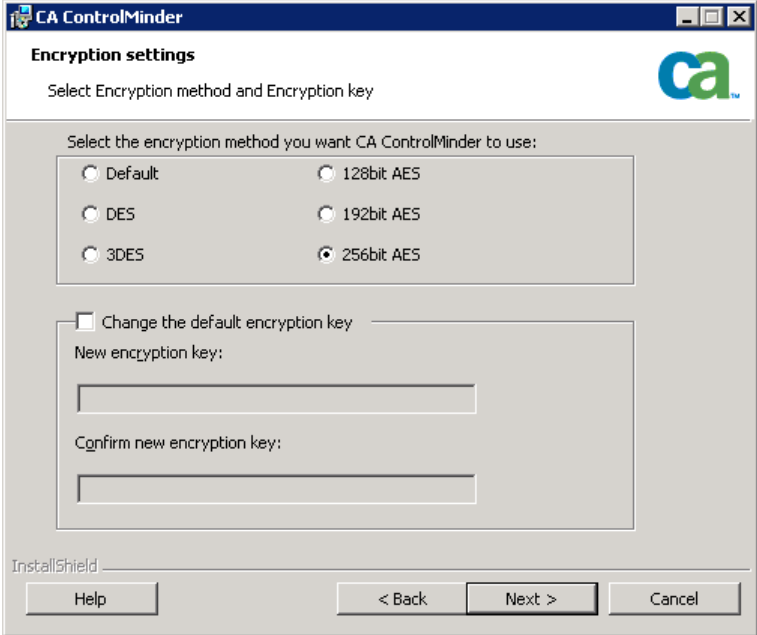
<p>Select the installation directory and the components to be installed.</p> <p>Add “PUPM Integration” and “Report Agent” out of those no selected by default.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'CA ControlMinder Select Features' dialog box. The 'Task Delegation' tree is expanded, showing 'Advanced Policy Management Client' (selected), 'Stack Overflow Protection (STOP)' (deselected), 'PUPM Integration' (deselected), 'Policy Model Subscriber' (deselected), and 'Report Agent' (deselected). The 'Feature Description' pane on the right describes the 'Report Agent' feature, stating it requires 0KB on the hard drive. The 'Install to:' field shows 'C:\Program Files\CA\AccessControl\'. The 'Next &gt;' button is highlighted.</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>The screenshot shows the 'CA ControlMinder Select Features' dialog box. The 'Task Delegation' tree is expanded, showing 'Advanced Policy Management Client' (selected), 'Stack Overflow Protection (STOP)' (deselected), 'PUPM Integration' (selected), 'Policy Model Subscriber' (deselected), and 'Report Agent' (selected). The 'Feature Description' pane on the right describes the 'PUPM Integration' feature, stating it requires 1KB on the hard drive. The 'Install to:' field shows 'C:\Program Files\CA\AccessControl\'. The 'Next &gt;' button is highlighted.</p>

<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><b>DO NOT REMOVE THIS USER!!</b></p> <p><b>If this user is removed then the installation will fail!</b></p> <p><b>This user can be removed after the installation has completed.</b></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 in the CA ControlMinder installer. 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 are 'Help', '&lt; Back', 'Next &gt;', 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 in the CA ControlMinder installer. 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 are 'Help', '&lt; Back', 'Next &gt;', and 'Cancel' buttons.</p>

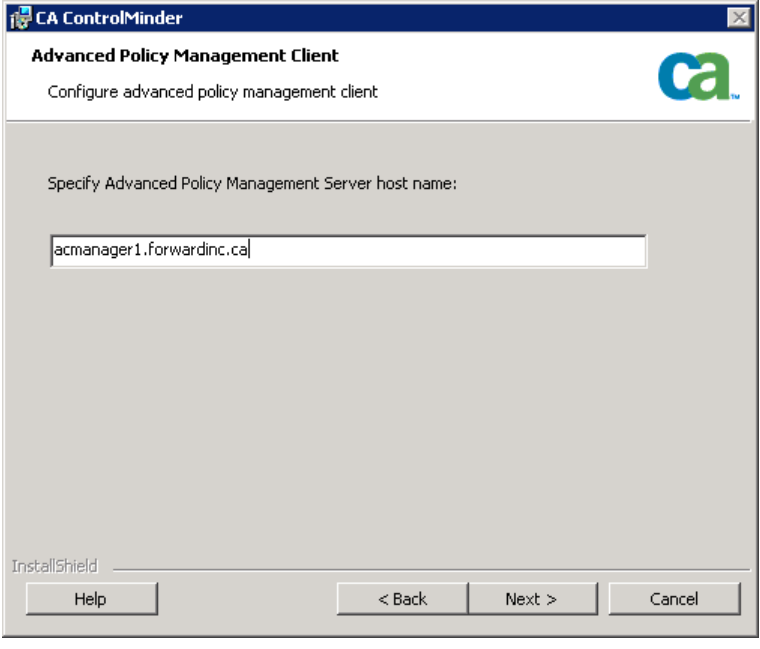
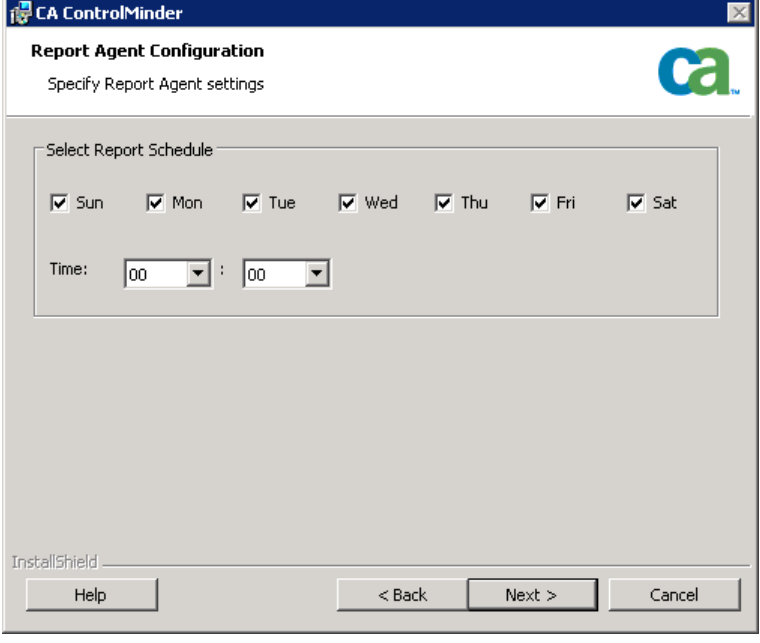


## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

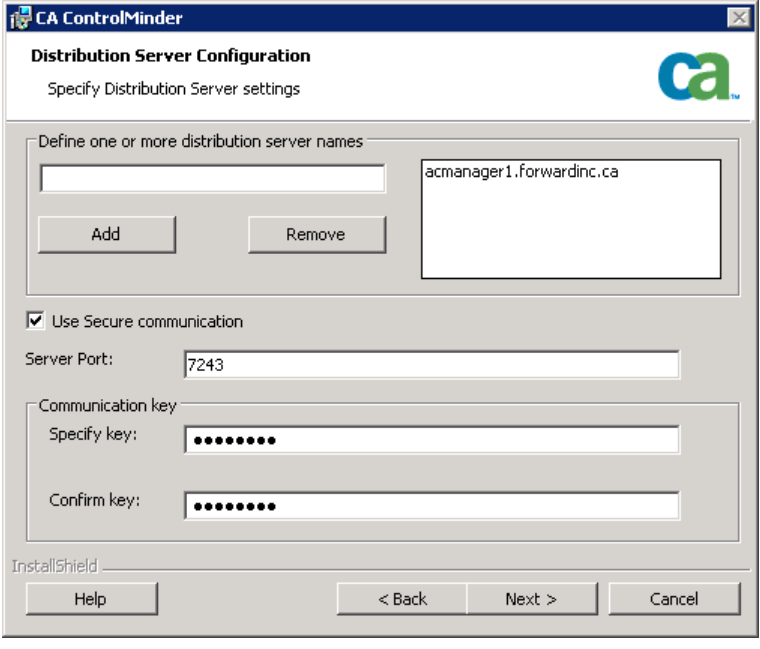
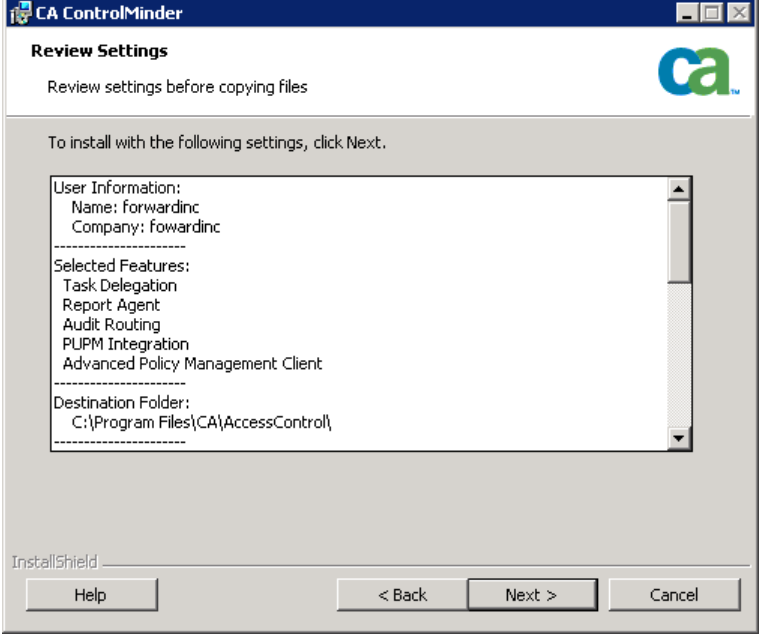
<p>Click the radial button for Yes to use Secure Socket Layer (SSL) communication.</p> <p>Leave the <u>Use Symmetric key encryption</u> checkbox checked.</p> <p>Note that SSL is enabled by default on CM ENTM server.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'CA ControlMinder SSL Communication' dialog box. It has a title bar with the CA logo and a close button. The main text says 'Use Secure Socket Layer (SSL) communication'. Below this, it asks 'Do you want ControlMinder to use Secure Socket Layer (SSL) communication?' with two radio buttons: 'No' and 'Yes'. The 'Yes' button is selected. Below the radio buttons is a checkbox labeled 'Use Symmetric key encryption', which is checked. At the bottom, there is an 'InstallShield' logo and three buttons: 'Help', '&lt; Back', and 'Next &gt;', and a 'Cancel' button.</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 'CA ControlMinder Certificate Settings' dialog box. It has a title bar with the CA logo and a close button. The main text says 'Choose Certificate Settings'. Below this, it explains 'In order for SSL communication to work properly, CA ControlMinder needs a server certificate and a root certificate.' There are four radio buttons: 'Generate CA ControlMinder certificate' (selected), 'Use default root certificate', 'Specify root certificate', and 'Use existing installed certificate'. The 'Generate CA ControlMinder certificate' option is selected. At the bottom, there is an 'InstallShield' logo and three buttons: 'Help', '&lt; Back', and 'Next &gt;', and a 'Cancel' button.</p>

<p>Provide the password of the certificate's private key.</p> <p>Click the Next button.</p>	 <p>The dialog box is titled "CA ControlMinder" and "Change Certificate Settings". It has a "ca" logo in the top right. The "Set Server Private key password" checkbox is checked. Below it are "Password:" and "Confirm:" fields, both containing masked text (dots). The "Change certificate settings" checkbox is unchecked. Below it are "Certificate Subject Name:" (containing "cn=win2k8prod01.forwardinc.ca"), "Certificate Serial:" (containing "111111111111"), and "Certificate expiration time (mm/dd/yy):" (containing "12/31/35"). At the bottom are "Help", "&lt; Back", "Next &gt;", and "Cancel" buttons. The "InstallShield" logo is in the bottom left.</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>	 <p>The dialog box is titled "CA ControlMinder" and "Encryption settings". It has a "ca" logo in the top right. The text "Select Encryption method and Encryption key" is at the top. Below it is the instruction "Select the encryption method you want CA ControlMinder to use:". There are six radio button options: "Default", "DES", "3DES", "128bit AES", "192bit AES", and "256bit AES". "256bit AES" is selected. Below this is a section "Change the default encryption key" with an unchecked checkbox. It contains "New encryption key:" and "Confirm new encryption key:" fields, both empty. At the bottom are "Help", "&lt; Back", "Next &gt;", and "Cancel" buttons. The "InstallShield" logo is in the bottom left.</p>

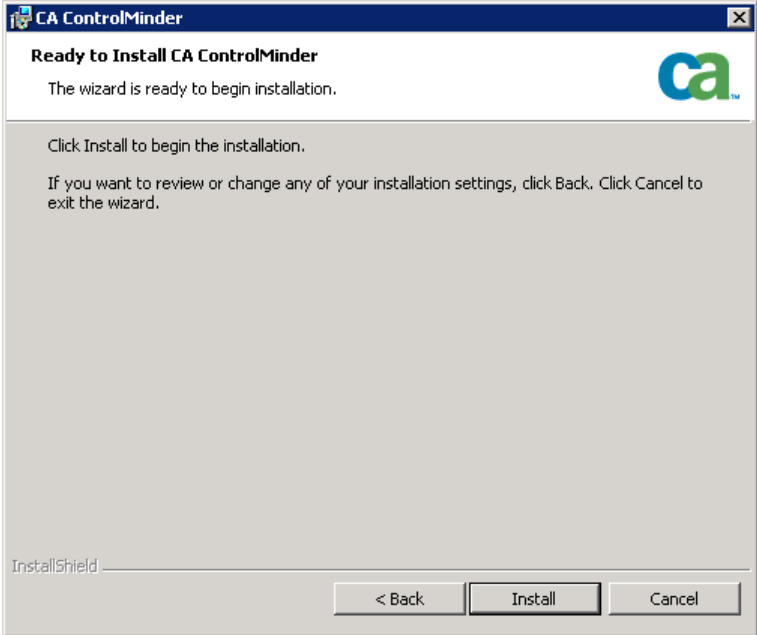
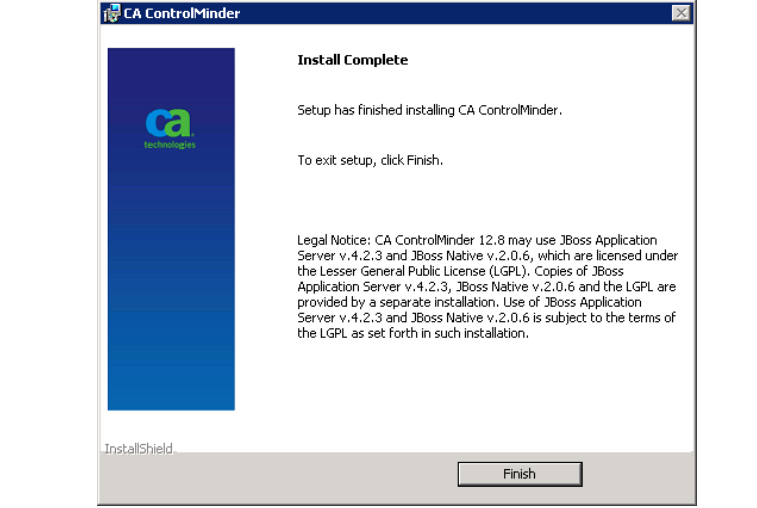
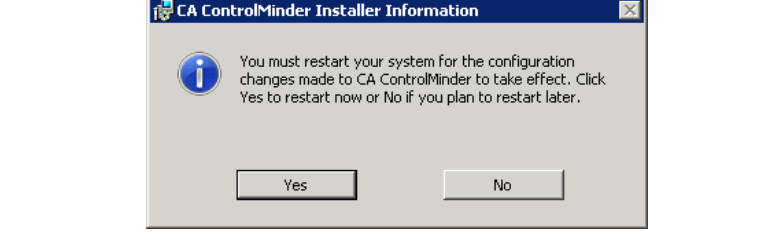
## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<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>The screenshot shows the 'CA ControlMinder Advanced Policy Management Client' dialog box. The title bar says 'CA ControlMinder'. The main title is 'Advanced Policy Management Client' with a subtitle 'Configure advanced policy management client'. The CA Technologies logo is in the top right. The instruction is 'Specify Advanced Policy Management Server host name:'. A text box contains 'acmanager1.forwardinc.ca'. At the bottom, there are buttons for 'Help', '&lt; Back', 'Next &gt;', and 'Cancel'. The 'InstallShield' logo is in the bottom left corner.</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>The screenshot shows the 'CA ControlMinder Report Agent Configuration' dialog box. The title bar says 'CA ControlMinder'. The main title is 'Report Agent Configuration' with a subtitle 'Specify Report Agent settings'. The CA Technologies logo is in the top right. The instruction is 'Select Report Schedule'. There are seven checkboxes for days of the week: Sun, Mon, Tue, Wed, Thu, Fri, and Sat, all of which are checked. Below the checkboxes is a 'Time:' label followed by two dropdown menus, both set to '00'. At the bottom, there are buttons for 'Help', '&lt; Back', 'Next &gt;', and 'Cancel'. The 'InstallShield' logo is in the bottom left corner.</p>

## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<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' window in the CA ControlMinder installer. The title bar reads 'CA ControlMinder'. The main heading is 'Distribution Server Configuration' with the subtitle 'Specify Distribution Server settings'. The CA logo is in the top right. The window contains a section 'Define one or more distribution server names' with a text input field (empty) and a list box containing 'acmanager1.forwardinc.ca'. Below these are 'Add' and 'Remove' buttons. A checkbox 'Use Secure communication' is checked. The 'Server Port' is set to '7243'. There are two password fields: 'Communication key' and 'Confirm key', both masked with dots. At the bottom, there are 'Help', '&lt; Back', 'Next &gt;', and 'Cancel' buttons. The 'InstallShield' logo is in the bottom left.</p>
<p>Review the installation parameters and click the Next button.</p>	 <p>The screenshot shows the 'Review Settings' window in the CA ControlMinder installer. The title bar reads 'CA ControlMinder'. The main heading is 'Review Settings' with the subtitle 'Review settings before copying files'. The CA logo is in the top right. The window contains a list of settings to be reviewed: 'User Information' (Name: forwardinc, Company: forwardinc), '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', '&lt; Back', 'Next &gt;', and 'Cancel' buttons. The 'InstallShield' logo is in the bottom left.</p>

## CA ControlMinder Rapid Implementation Guide – SAM JumpBox

<p>Click the Install button.</p>	 <p>The screenshot shows the 'Ready to Install CA ControlMinder' dialog box. It contains the text: 'The wizard is ready to begin installation.' and 'Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.' At the bottom, there are three buttons: '&lt; Back', 'Install', and 'Cancel'.</p>
<p>After the installation has completed, click the Finish button.</p>	 <p>The screenshot shows the 'Install Complete' dialog box. It contains the text: 'Setup has finished installing CA ControlMinder. To exit setup, click Finish.' Below this is a 'Legal Notice' section. At the bottom, there is a 'Finish' button.</p>
<p>The installation may require a reboot to load ControlMinder kernel drivers. Click the Yes button to reboot now or click the No button to manually reboot at a later time.</p>	 <p>The screenshot shows the 'CA ControlMinder Installer Information' dialog box. It contains an information icon and the text: 'You must restart your system for the configuration changes made to CA ControlMinder to take effect. Click Yes to restart now or No if you plan to restart later.' At the bottom, there are two buttons: 'Yes' and 'No'.</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.