CA Technologies

CA ControlMinder™ Rapid Implementation Guide

Amazon EC2 Deployment

CA Technologies
8/30/2013

Contents

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 HTLM 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

Glossary

AC	Access Control
ACNT	Account
ACWS	Access Control Web Service
APM	Advanced Policy Management
APMS	Advanced Policy Management Server
AWS	Amazon Web Services
CA	formerly Computer Associates – now CA Technologies
CM	ControlMinder (formerly Access Control)
CMPE	ControlMinder Premium Edition
CMVE	ControlMinder for Virtual Environments
CS	Connector Server
DH	Distribution Host
DMS	Distribution Management Server
DN	Distinguished Name
DR	Disaster Recovery
DS	Distribution Server
EC2	Elastic Compute Cloud
ELM	Enterprise Log Manager
ENTM	Enterprise Manager
EP	Endpoint (server)
GECOS	GE Comprehensive Operating System (finger field in passwd file)
GID	Group ID
HA	High Availability
IAM	Identity and Access Manager
JDK	Java Development Kit
MS	Microsoft Corporation
MSADS	Microsoft Active Directory Server / Services
MSSQL	Microsoft SQL/Server
MQ	Message Queue
NSS	Network System Services
OS	Operating System
PAM	Pluggable Authentication Module
PCI	Payment Card Industry
PR	Production
PUPM	Privileged User Password Management
RIA	Rapid Implementation Architecture
RIG	Rapid Implementation Guide
RS	Report Server
RSS	Resident Security System
SAM	Security Account Manager (formerly PUPM)
SeOS	Security for Open Systems
UARM	User Access Reporting Module (formerly ELM)
UAT	User Acceptance Test
UID	User ID
UNAB	UNIX Authentication Broker
VPC	Virtual Private Cloud
W2K3	Windows 2003
W2K8	Windows 2008
WAS	Web Application Server

Prerequisites

It is assumed that you are using existing Amazon deployed services and have:

- An Amazon EC2 account (if not, create one at: http://aws.amazon.com/ec2/)

ControlMinder Enterprise Management is a browser-based administration interface, you need one of the following web browsers:

- Microsoft® Internet Explorer® 7 or higher with Java 7 version 1.7.0_03 or higher
- Firefox (latest version) with Java 7 version 1.7.0_03 or higher

The web interface has been tested to work only with the browsers listed above.

To view the ControlMinder user manuals, you can use:

- A web browser to view the documentation in HTML format.
- Adobe® Reader® or any other compatible PDF viewer

Introduction

This document presents the process of deploying ControlMinder 12.8 Endpoints on Amazon EC2 instances (Windows and Linux), and managing this deployment through an ENTM and Distribution Server also located in an Amazon EC2 instance.

The deployment architecture presented in this document is shown in the following diagram.

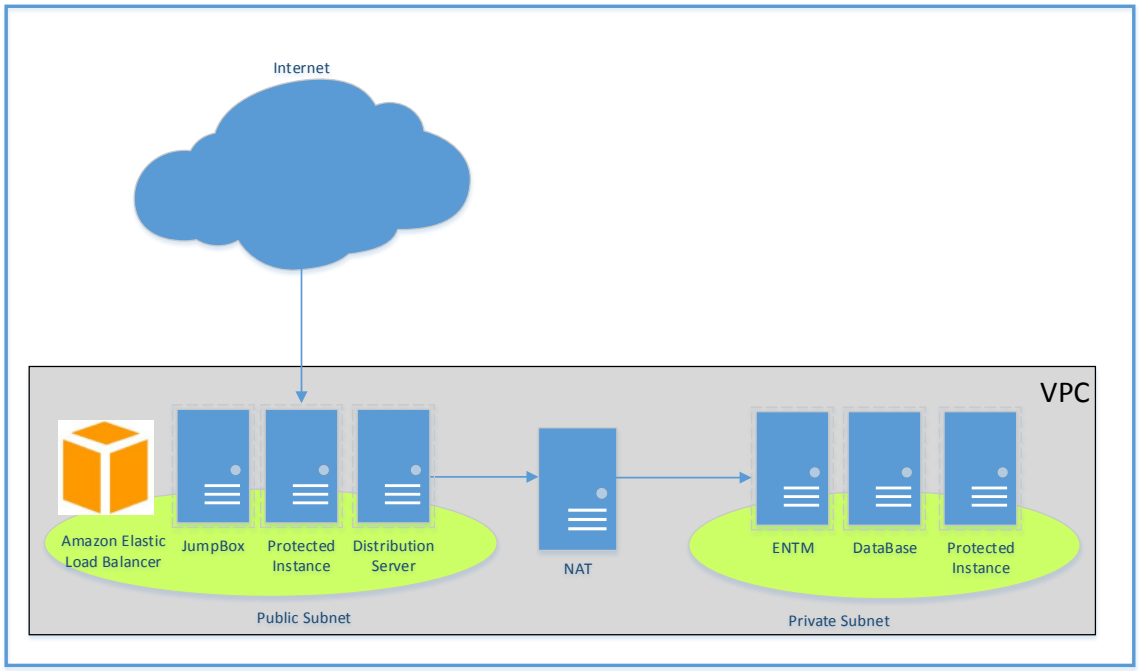


Figure 1 – Reference Deployment Architecture

Solution Highlights

ENTM and its Database (MS SQL or Oracle) are deployed on a Private Subnet (Amazon VPC) which prevents users from directly accessing them.

ENTM can be managed through the internet by exposing its HTTP services through Amazon Elastic Load Balancer. The load balancer bridges internet HTTP traffic into the ENTM deployed on the private subnet.

ControlMinder Endpoints are deployed on every Amazon Instance which needs security protection. These endpoints communicate with ENTM through Distribution Servers, deployed on the same subnet as the protected instances.

Instances Summary

Amazon EC2 instances are the fundamental building blocks (virtual servers) located in the Amazon Web Service (AWS) cloud. Each instance is created from a standard server profile that is sized (and priced) to meet the general needs of low to high-end application requirements.

Instances may be created from the Amazon Machine Image (AMI) template where the image represents a standard server and OS configuration, or may be created using a client-owned OS and application software. If a standard configuration is used then this may be viewed as renting the server hardware and software whereas in the second configuration model one is renting the hardware but owns the software.

In order to setup a ControlMinder deployment environment on Amazon EC2 you will need the instances shown in the following table.

Table 1 – Required Amazon EC2 Instances

Name	Type	Subnet	Comments
Enterprise Management Server (ENTM)	M1 Large Windows 2008 R2	Private subnet (VPC)	
Distribution Server (DS)	M1 Medium Windows 2008 R2	Every subnet that contains ControlMinder endpoints	
MS SQL Database	M1 Large Windows 2008 R2	Private subnet (VPC)	
JumpBox	M1 Medium Windows 2008 R2	Public subnet	Needed for connecting to the MSSQL or ENTM instances (the instances are not connected to the internet)
Amazon Elastic Load Balancer Server		Public subnet	Used to expose browser access to the ENTM server from the internet.

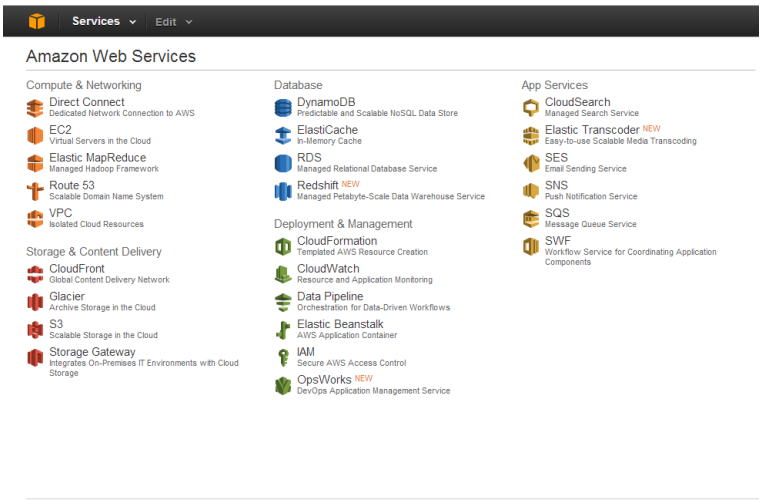
Prerequisites and Getting Started

This document assumes that you have signed up for Amazon Web Services (AWS) and you are able to navigate in AWS Management Console. The AWS Management Console provides a simple web interface for Amazon Web Services.

You need to log in using your AWS account name and password to perform the configuration.

You can the console at:

https://console.aws.amazon.com/console/home



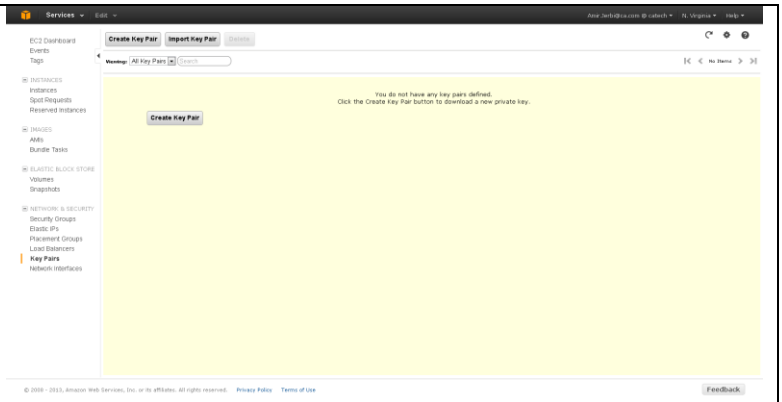
Generating a Key Pair

To log in to your instances you must first create a key pair. Specify the name of the key pair when you launch the instance and provide the private key when you connect to the instance.

Linux/UNIX instances have no password, and you use a key pair to log in using SSH.

With Windows instances, you use a key pair to obtain the administrator password and then log in using RDP.

If you currently use any of Amazon's deployed services, you will have created a certificate key pair already. If you are new to Amazon's deployed services, follow the steps below to create a key pair.

Select AWS Services to create a Key Pair.	
Enter a name in the Key Pair Name field, for example “IT GROUP”. A private key is created and you are prompted to save it.	
Select Close once the Key Pair has been created. Save the private key file to your local machine and remember the location. Note that the Key Pair is downloaded to your browser and once the downloaded Key Pair has been retrieved then you cannot retrieve the Key Pair from Amazon again.	

Creating a Virtual Private Cloud

Amazon Virtual Private Cloud (VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined.

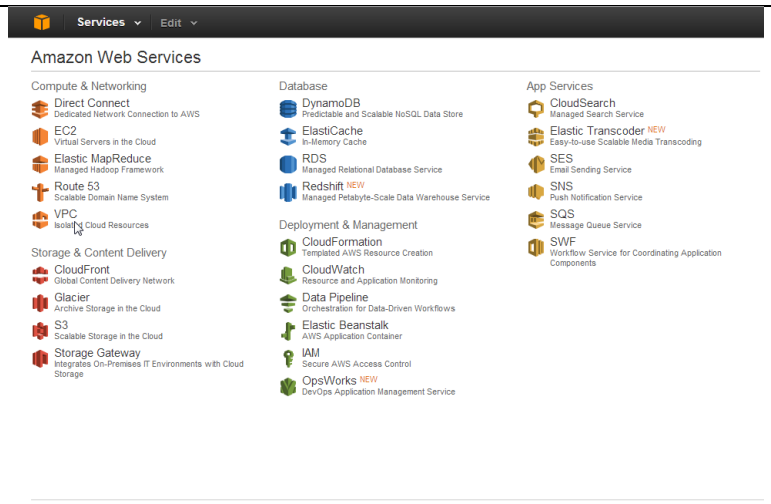
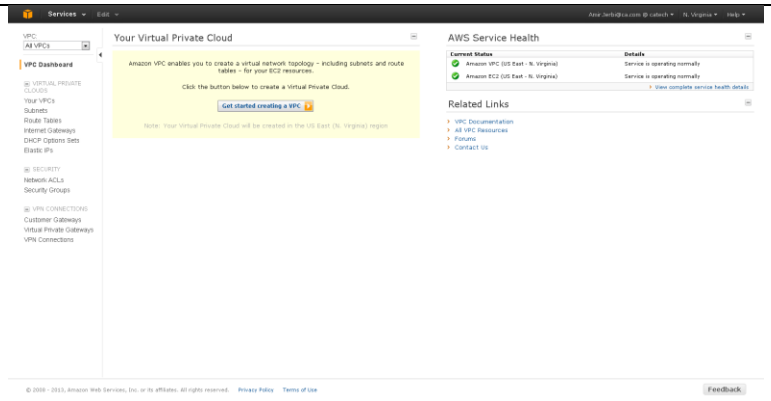
This virtual network closely resembles a traditional network that you operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

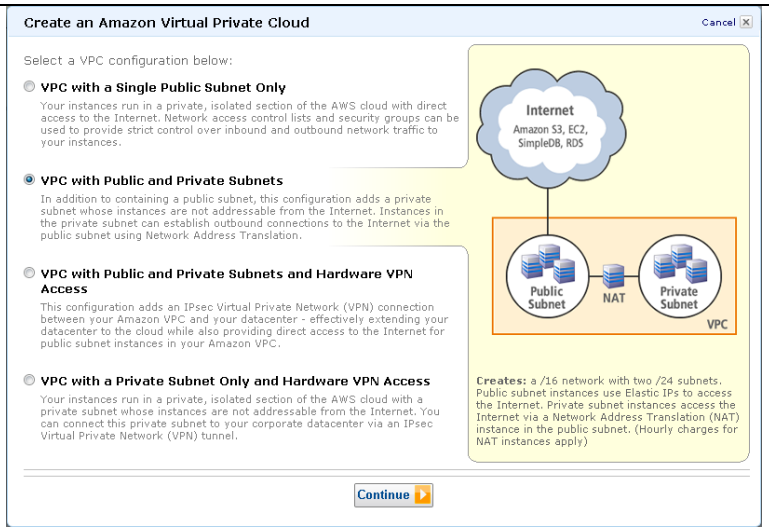
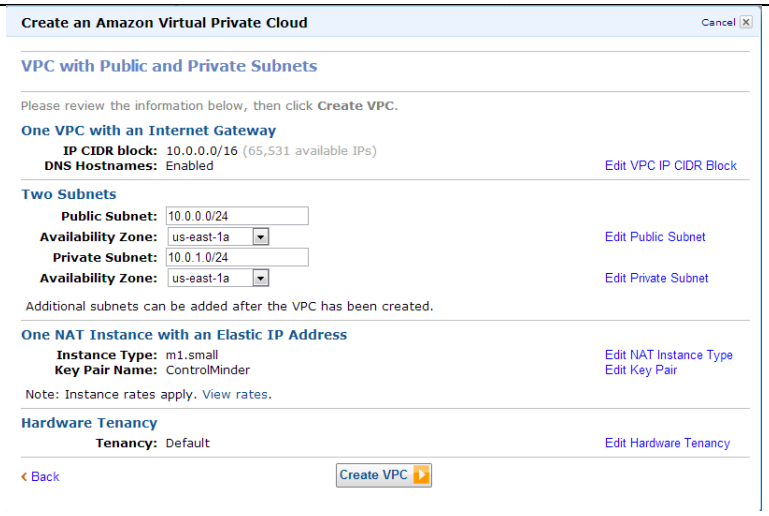
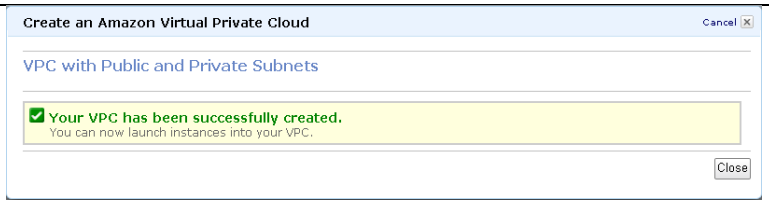
We will create 2 subnets:

- Public subnet
- Private subnet

Internet access can be allowed to instances in the public subnet.

The ENTM server and the Microsoft SQL Server will be located on the private subnet to further limit access.

Login to the AWS Console. Click VPC,	
Click the Get started creating a VPC button (ensure that correct region has been selected in which to create the VPC).	

For this example, "VPC with Public and Private Subnets" was chosen. The ENTM server and the Microsoft SQL server will be isolated on the private subnet. Other instances will be public facing. Choose the type of VPC that meets your needs. Click the Continue button to proceed.	
This VPC has two subnets: • a public subnet (10.0.0.0/24) • a private subnet (10.0.1.0/24) Verify that both subnets are deployed on the same availability zone. Click the Create VPC button.	
You will see confirmation that the VPC was successfully created.	

Defining Security Groups

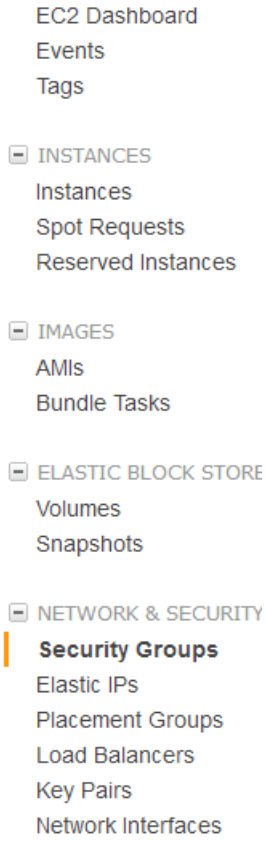
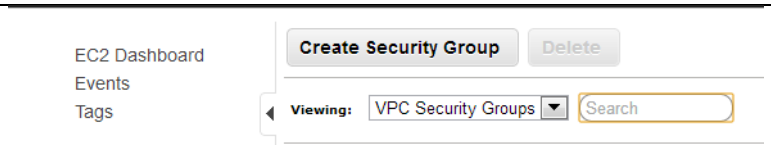
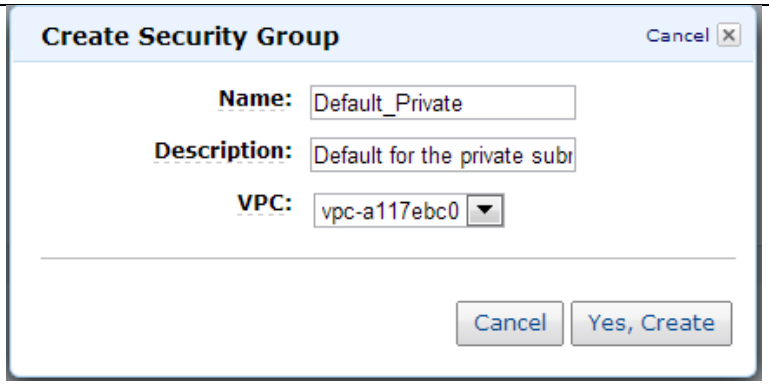
A security group acts as a firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.

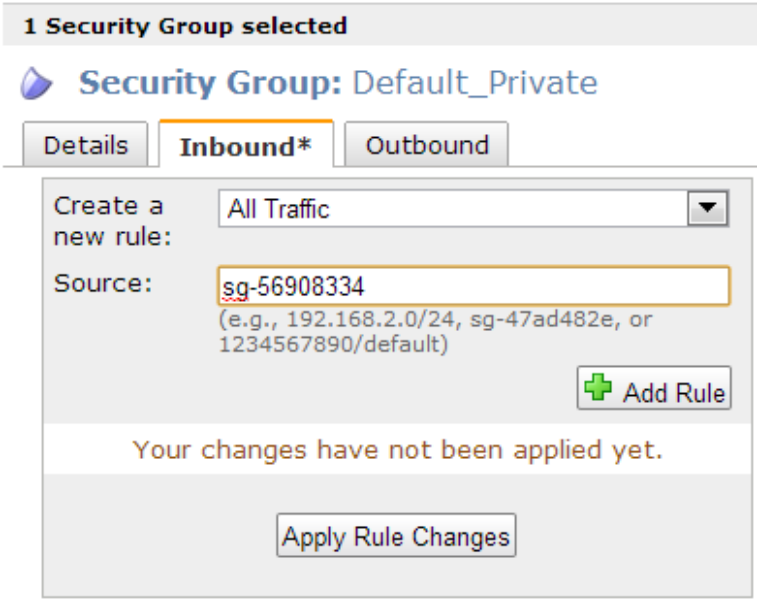
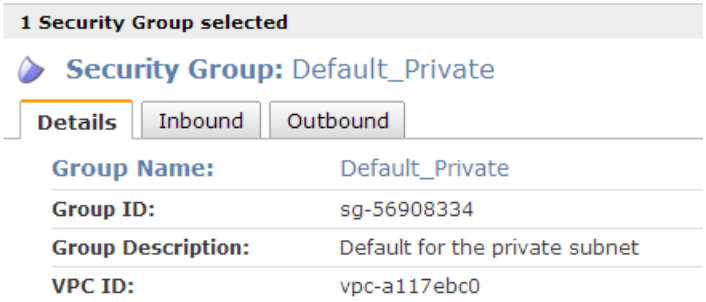
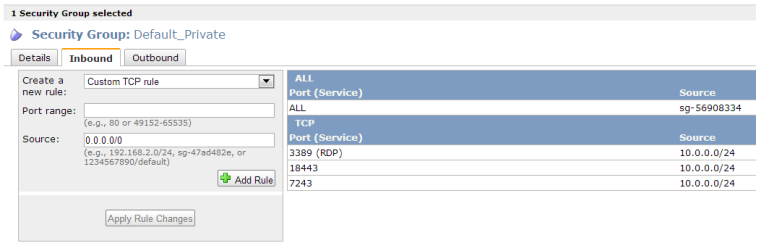
You need to create security groups to open all the necessary ports for implementing and running CA ControlMinder.

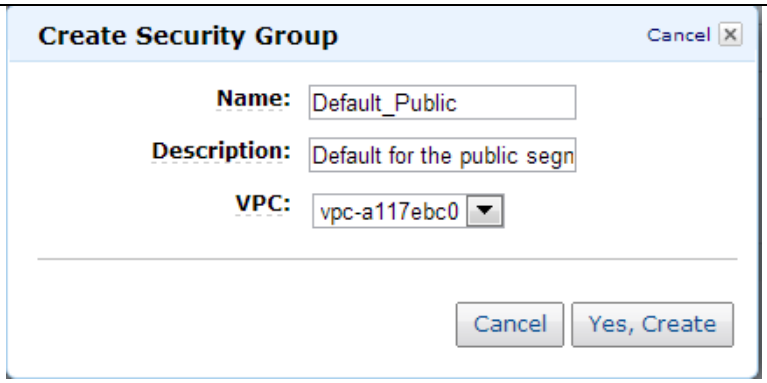
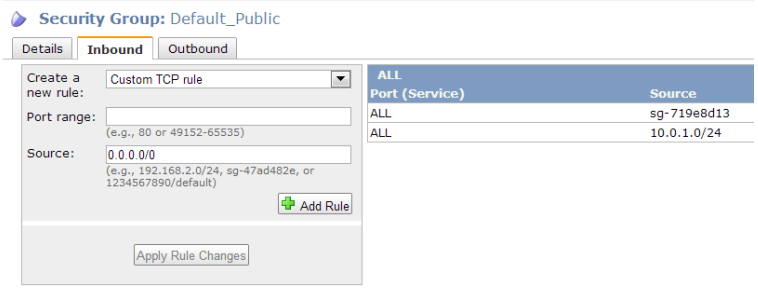
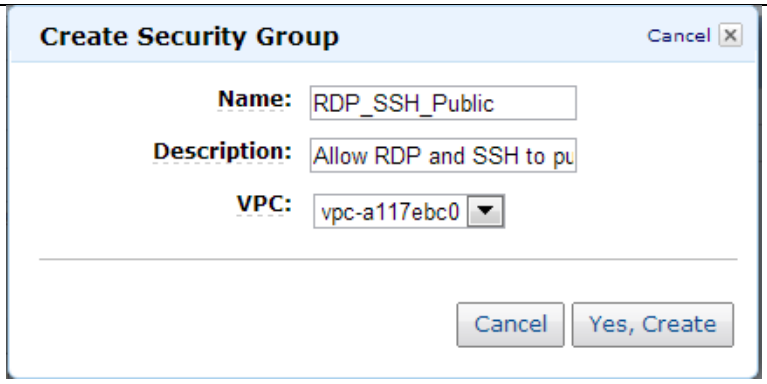
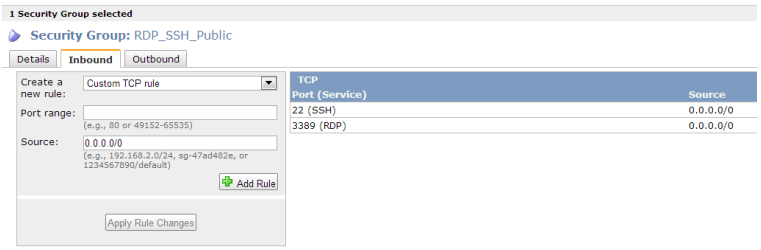
We will use the following groups:

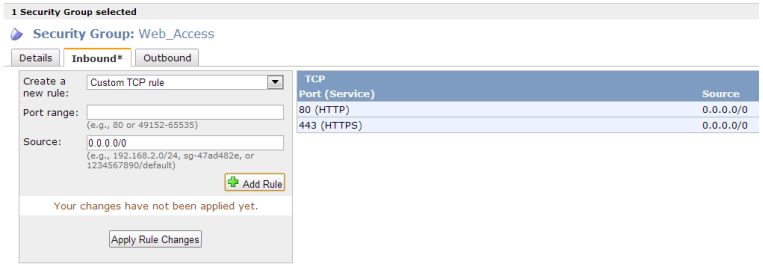
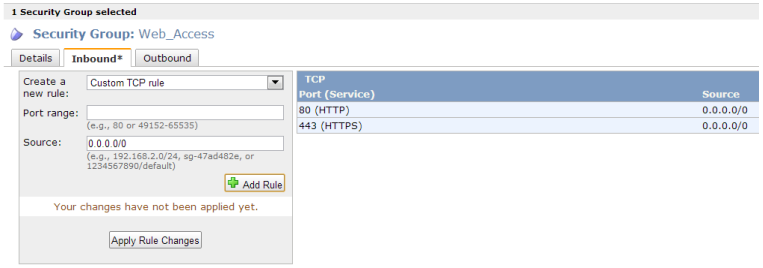
- Default_Private - Defines default access to the private subnet.
- Default_Public - Defines default access to the public subnet.
- RDP_SSH_Public – Allow Remote Desktop (RDP) and Secure Shell (SSH) access to members of this group from the internet. NOTE: Only instances on the public subnet can be members of this group. Instances on the private subnet cannot be accessed from the internet.
- Web_Access – Allow web browser access to members of this group from the internet. NOTE: Only instances on the public subnet can be members of this group. Instances on the private subnet cannot be accessed from the internet.

Follow the steps below to create the security groups.

Go to Amazon AWS console and select EC2. Select “Security Groups” from the EC2 dashboard.	
Click “Create Security Group”. Select “VPC Security Groups”	
Provide the name and description for the group and select the VPC you created previously. You will use Default_Private for the group name.	

Create a rule that permits all access between members of the private subnet. This is accomplished by adding an “All Traffic” rule with the Source field set to the Security Group of the private subnet..	 
Add rules to allow members of the public subnet access to members of the private subnet (10.0.0.x in our case).over the following ports: • Remote Desktop (3389) • Browser access over SSL (18443) • Tibco Message Queue (7243) Click “Apply Rule Changes”	

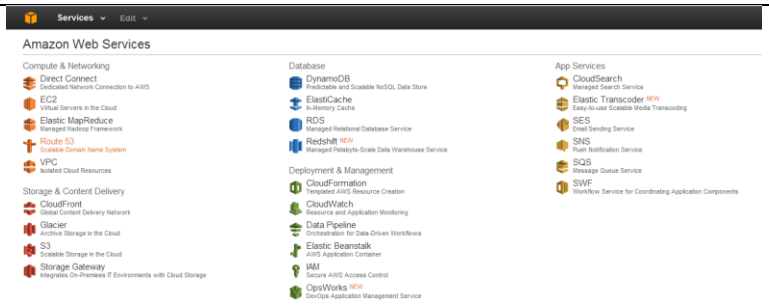
Create group Default_Public”	
Add rules that permit access from all members of the public subnet and all members of the private subnet. This is achieved by adding the security group ID of the public subnet as the source and All Traffic as the port/service. Allow also all the communication from the private segment (10.0.1.x in our case).	
Create a Security Group to allow Remote Desktop (RDP) and Secure Shell (SSH) access to group members.	
Add rules to allow members of the public subnet access to members of the private subnet over the following ports: • Remote Desktop (3389) • Secure Shell (22) This example allows access to group members from the public subnet, the private subnet, and the internet. Limit access further to meet your specific requirements. Click “Apply Rule Changes”	

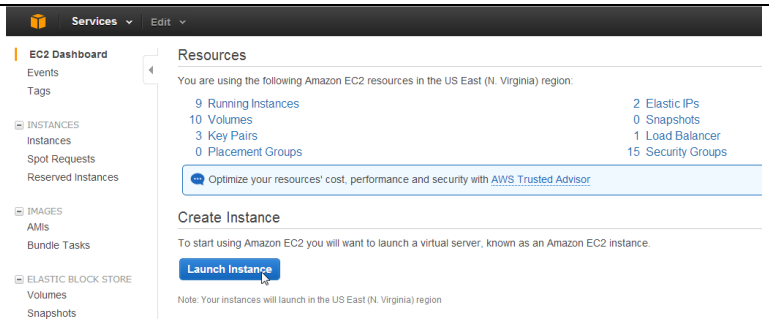
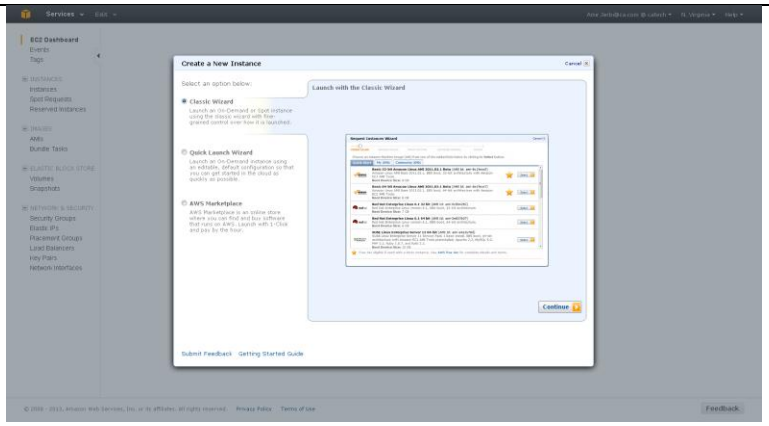
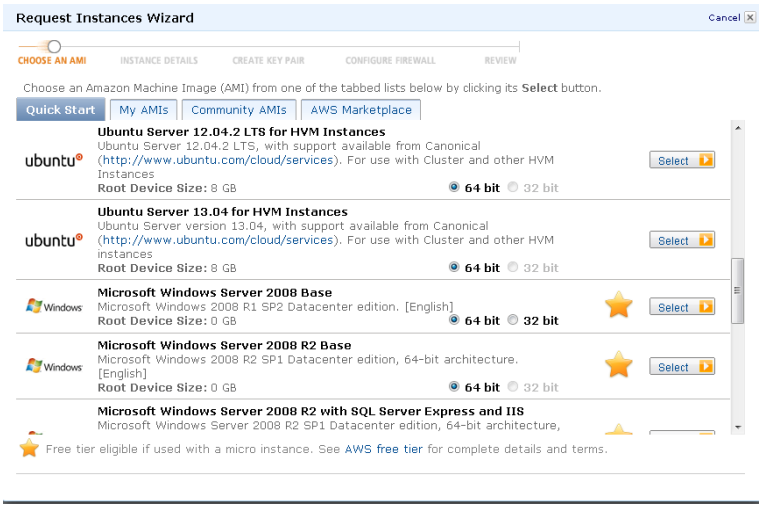
Create the Web_Access group to allow browser access.	
Allow browser access to the: • Default HTTP port (80) • Default HTTPS port (443) This example allows access to group members from the public subnet, the private subnet, and the internet. Limit access further to meet your specific requirements.	

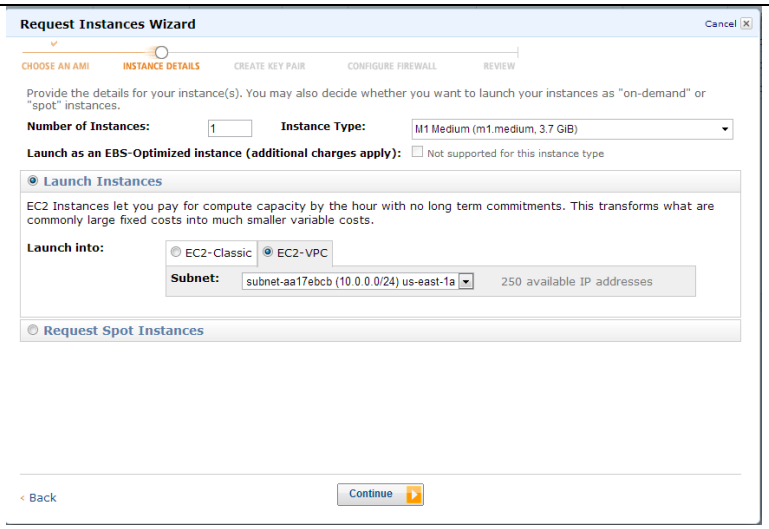
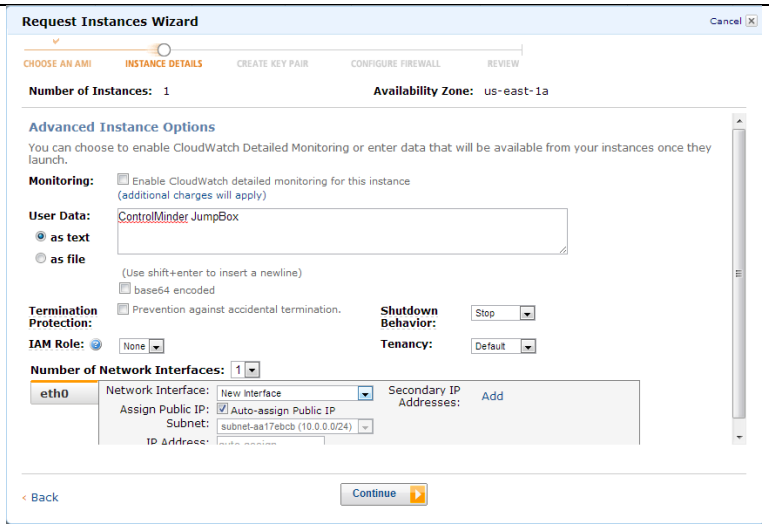
Setting Up a Jump Box

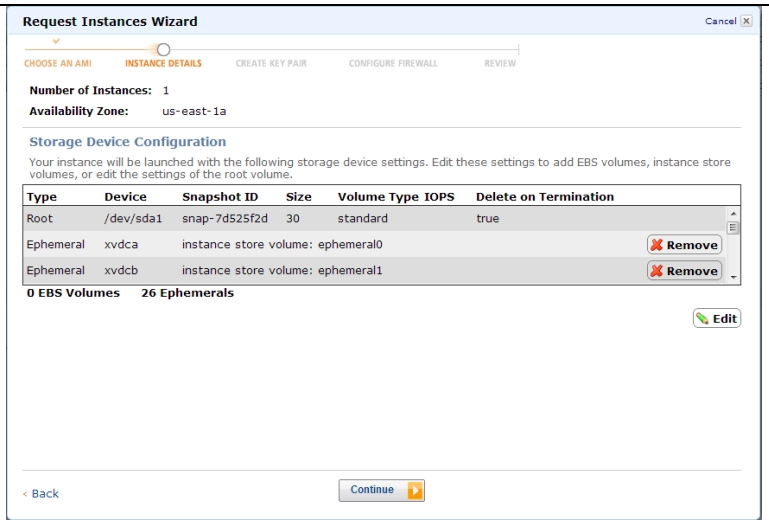
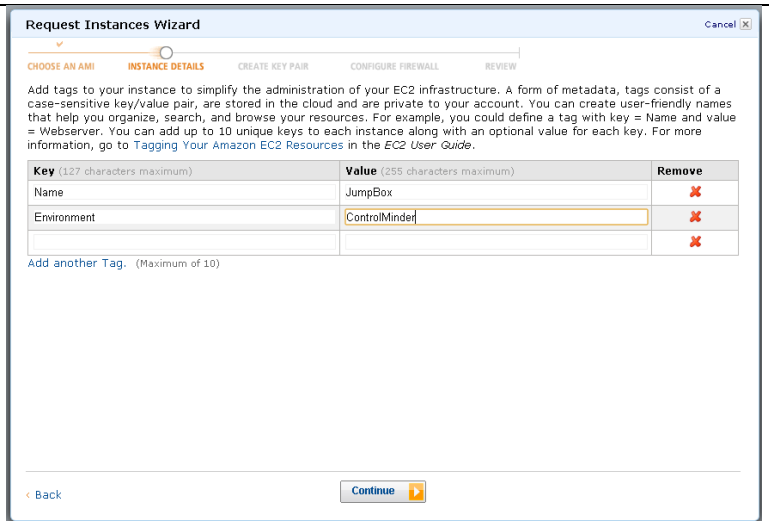
Since the ENTM server and Microsoft SQL server will be on the private subnet, you will need an internet accessible JumpBox on the public subnet to connect to and maintain instances on the private subnet.

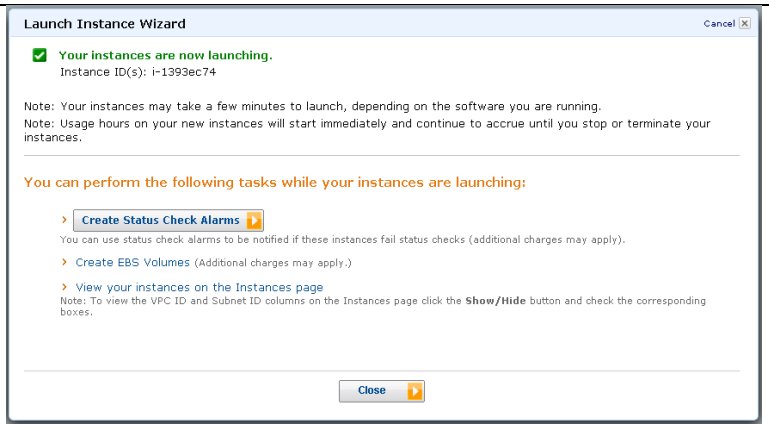
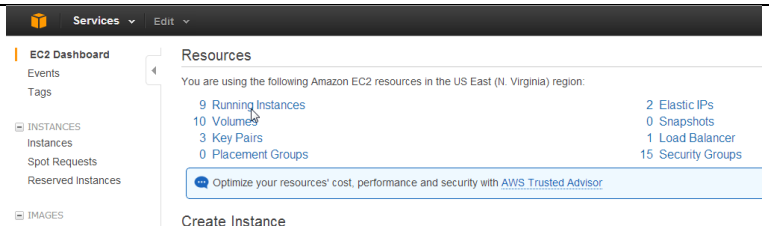
We will deploy a medium-sized Windows 2008 R2 instance on the public subnet as the JumpBox.

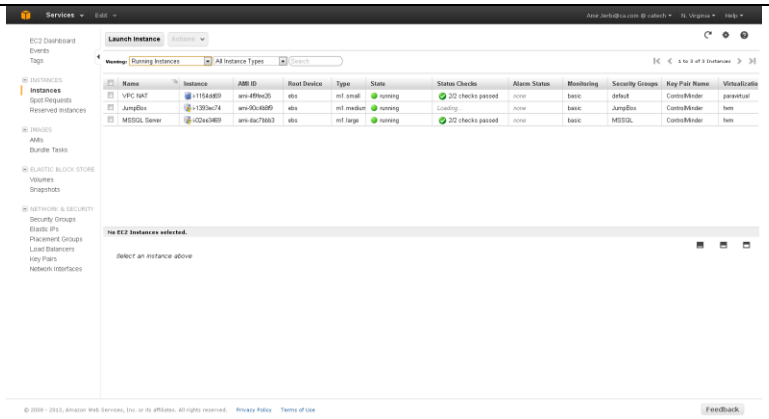
Click the EC2 tab on the Amazon Web Services (AWS) Console.	

Click the “Launch Instances” button.	
Click the radial button for the Classic Wizard.	
Scroll through the Quick Start list of Amazon Machine Images (AMIs) and select Microsoft Windows 2008 R2 Base.	

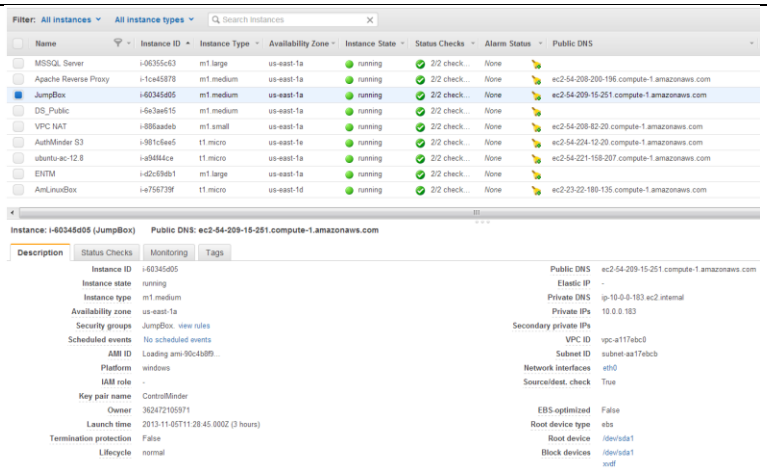
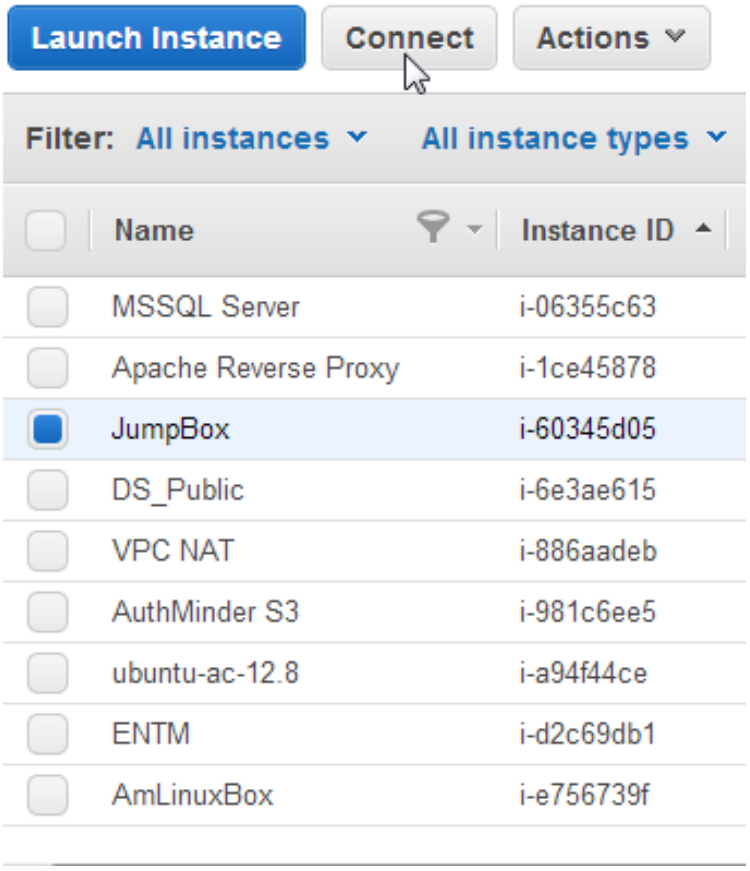
Select M1 Medium instance. Ensure that the JumpBox is deployed on the public subnet (10.0.0.0/24). Click the Continue button.	
Provide User data to identify your instance. Ensure that the Auto assign Public IP option is chosen to make the JumpBox internet accessible. Click the Continue button.	

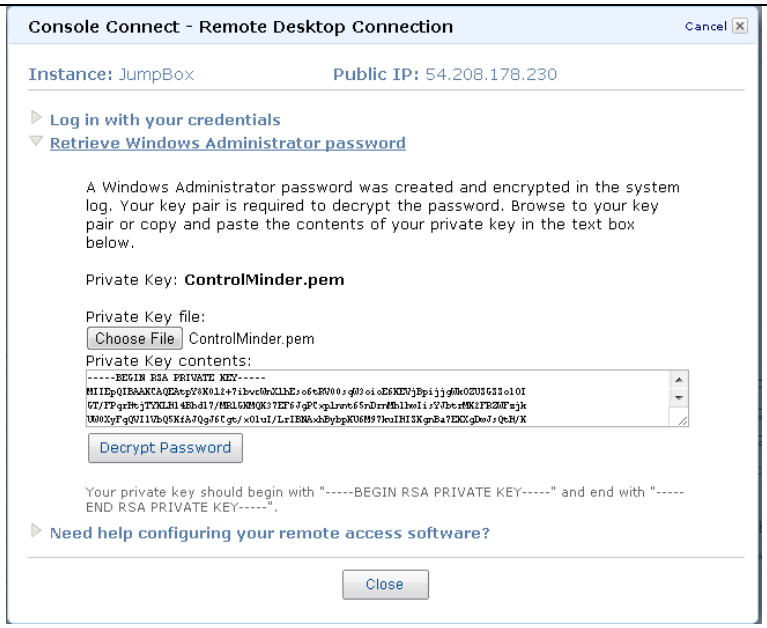
Keep the default storage configuration. 30 gigabytes of disk storage is sufficient for the JumpBox server.	
Name your instance and provide any additional tags as required.	
Use the key pair associated you're your AWS ECS Account.	

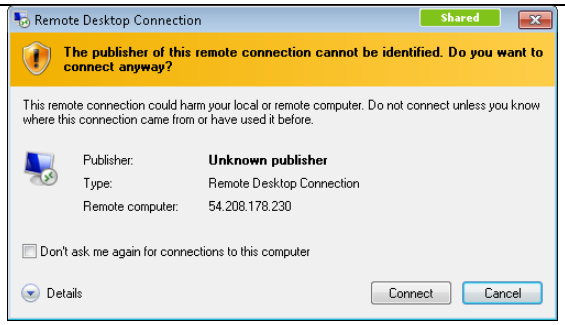
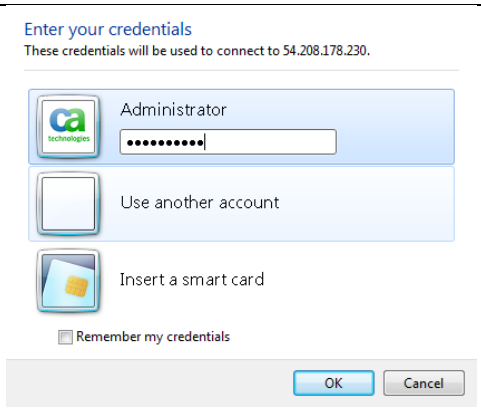
Assign the following Security Groups to the JumpBox: • Default_Public • RDP_SSH_Public	
Click the "Launch" button.	
	
Click on "Running Instances" on the EC2 Dashboard to verify that your instance is up and running.	

Wait until the “Status Check” for the instance changes to “2/2 checks passed”.	

Connecting to the JumpBox

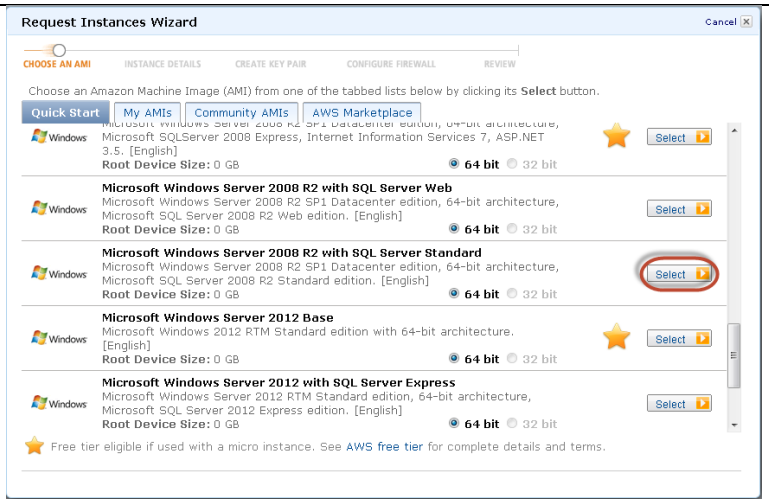
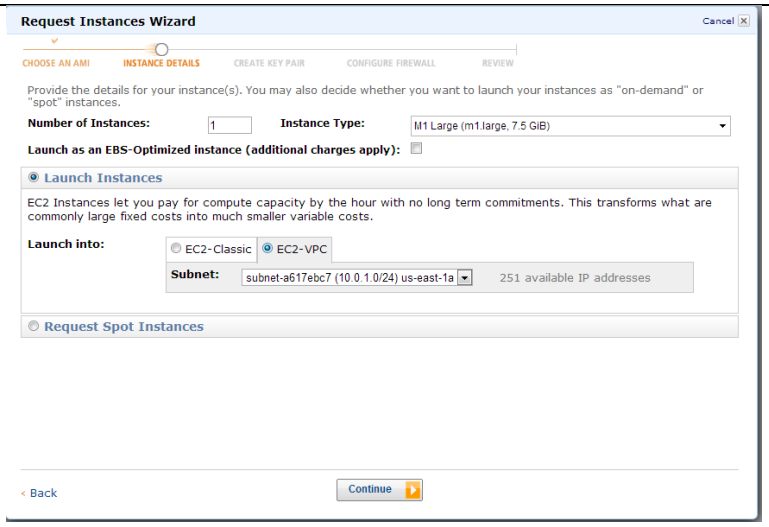
Go to the list of running instances and select the JumpBox instance. The instance properties are displayed. Note the Public DNS, which you will use to access the JumpBox via RDP.	
Click “Connect”.	

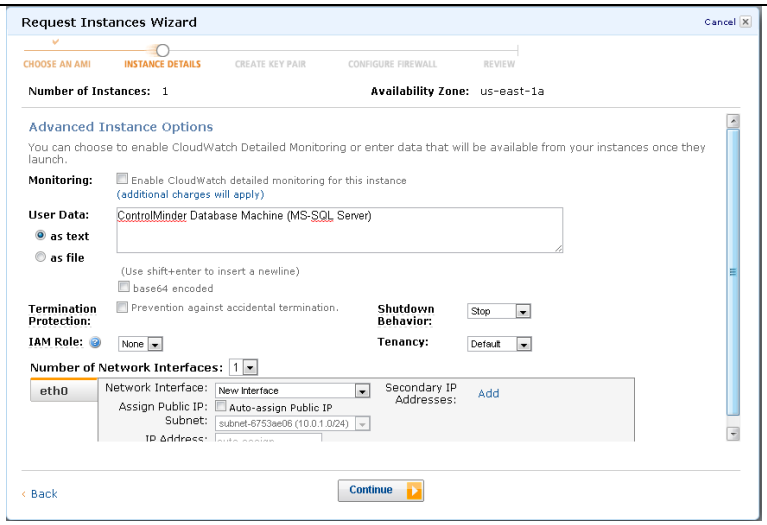
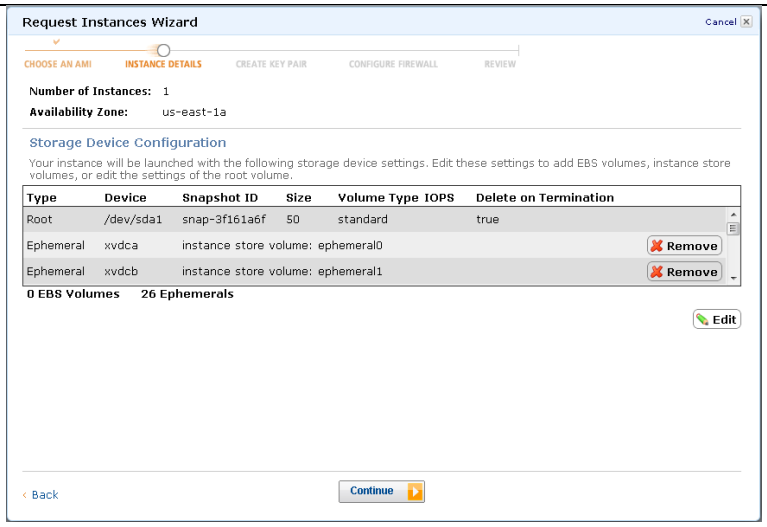
Click the Retrieve Windows Administrator password link. To retrieve the Windows Administrator password for the JumpBox server, you need to provide the Private Key file associated with your AWS EC2 Account. Click the Decrypt Password button and record the password.	
Click the Log in with your credentials link. Click the Download shortcut file link.	

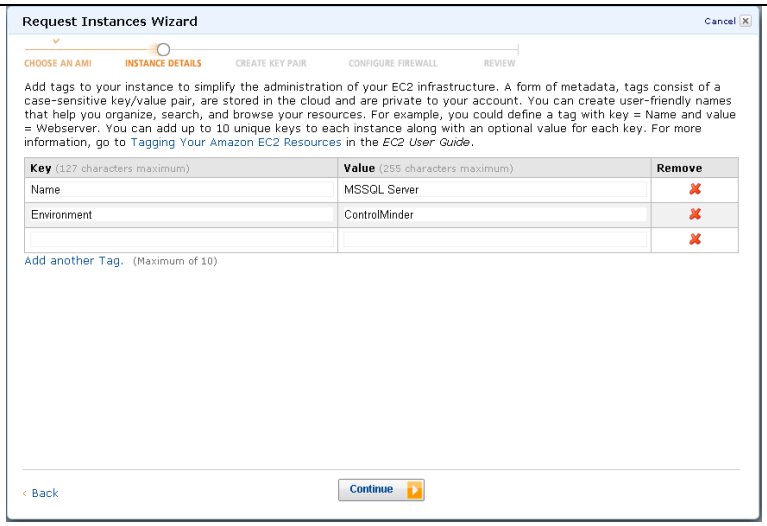
Click “Download shortcut file”	
Click the Connect button on the Remote Desktop Connection form.	
Enter the credentials that will be used to connect to 54.208.178.230. From the JumpBox server you may connect to the ENTM server the Microsoft SQL server by starting RPD on the JumpBox server.	

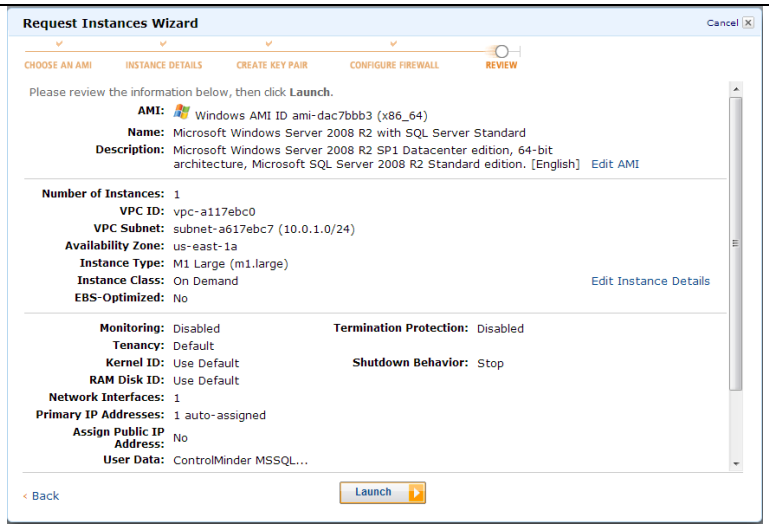
Deploying the RDBMS Using Microsoft SQL Server

Create the Microsoft SQL Server Instance on the private subnet.

Following similar steps as described above, launch another instance. This time select "Windows 2008 R2 with SQL Server Standard".	
Deploy the instance on the private subnet.	

Provide “User data” to identify your instance. Click the Continue button.	
Click the Continue button to accept the default allocation of 50 gigabytes of disk storage.	

Name your instance and provide any additional tags as required.	
Use the key pair associated you're your AWS ECS Account.	
Add the Default_Private Security Group to this instance.	

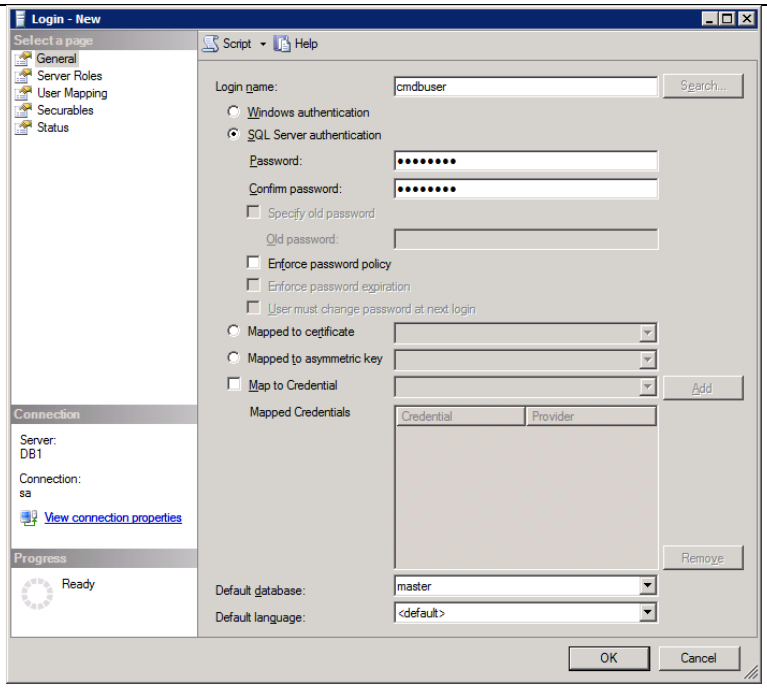
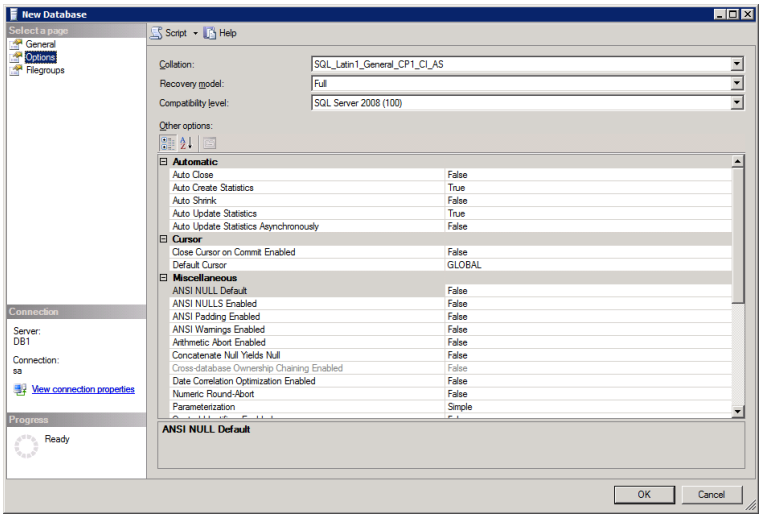
Launch the instance by clicking the Launch button.	

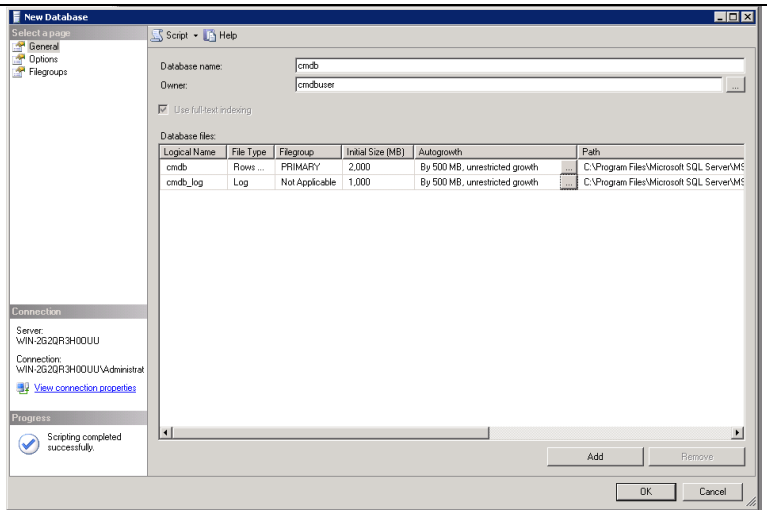
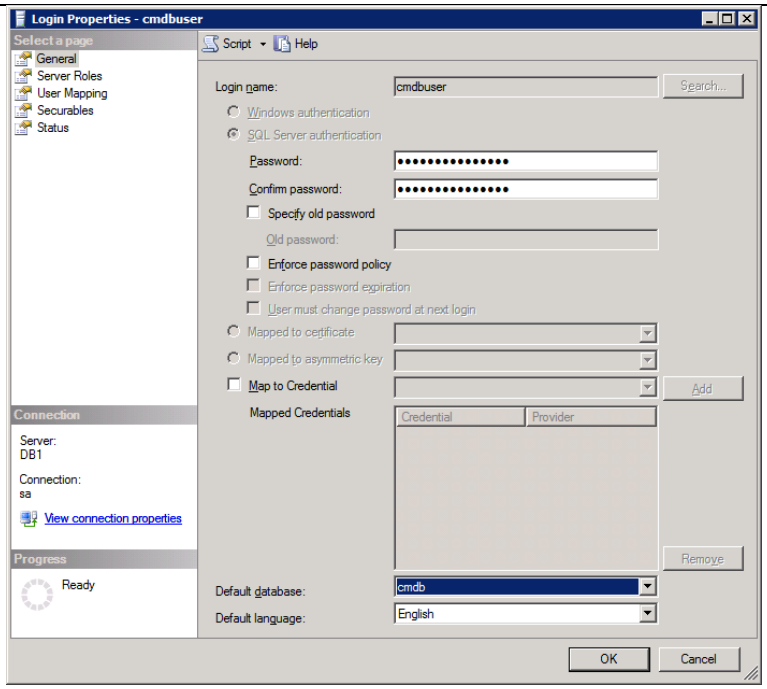
Preparing the Database

From the JumpBox server connect to the Microsoft SQL Server via RDP.

You can obtain the IP address of the Microsoft SQL Server from its instance properties.

Create an empty database using **Microsoft SQL Server Management Studio**.

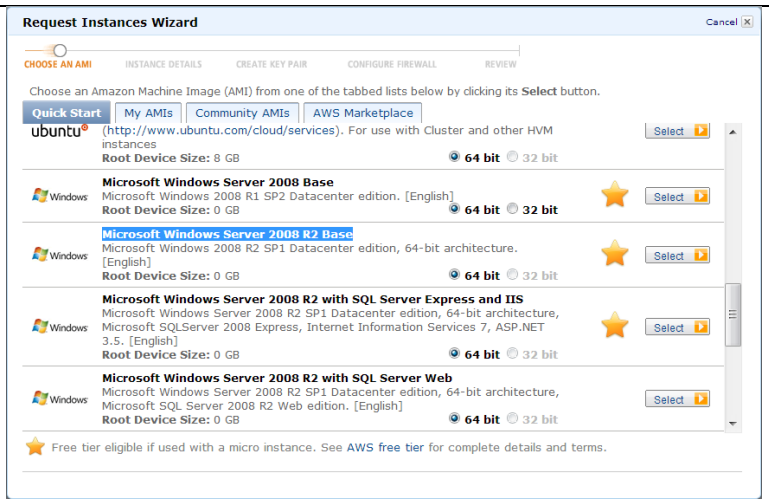
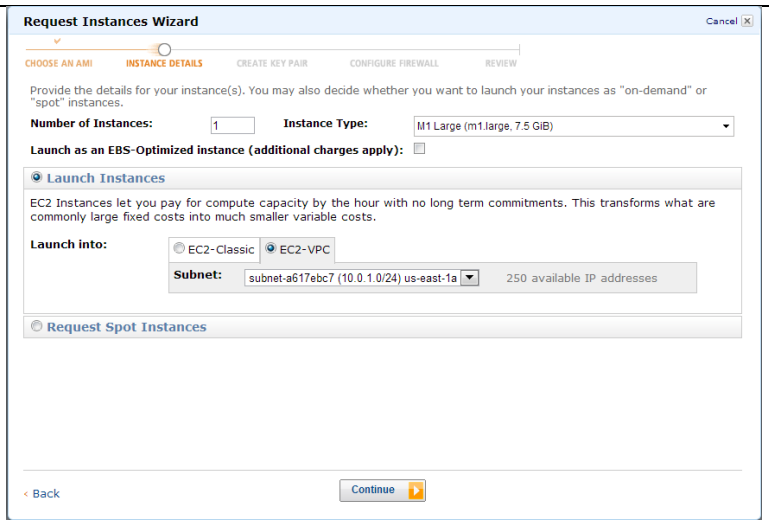
Create the database owner Create a database user. Select SQL Server authentication for this user. Define this user's password and deselect Enforce password policy. In the example, the Login name of the database user is set to cmdbuser.	
Create the database When creating the database, set Collation to: **SQL_Latin1_General_CP1_CI_AS** Failure to configure the correct settings may cause lookup problems later. Set the database owner to the user previously created. If that user is set as the owner (dbo) then no other access rights are required. For the example, assume the name of the database is cmdb.	

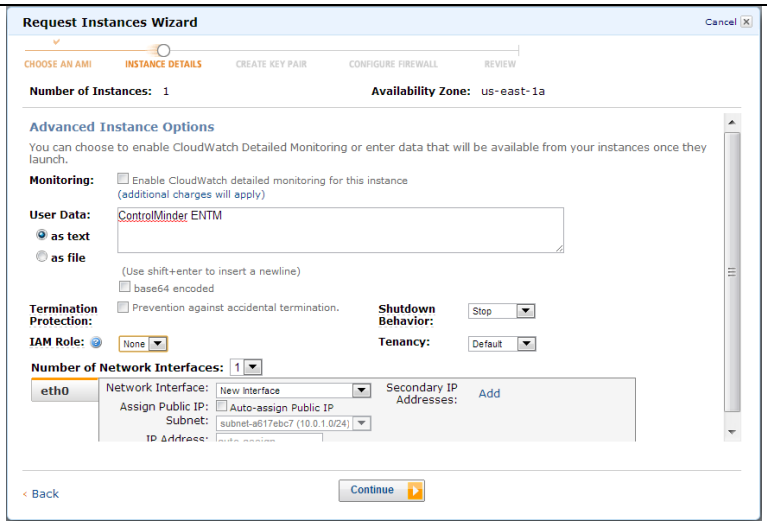
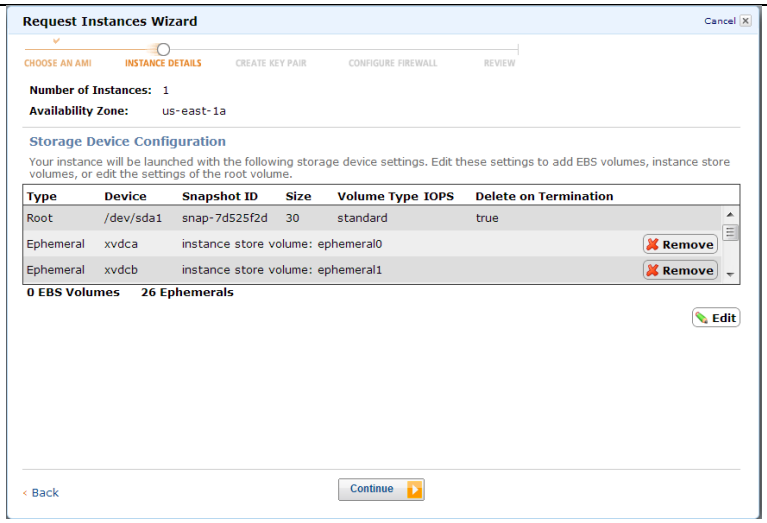
It is important to pre-allocate sufficient database space to hold configuration information and snapshot data. In the example above we pre-allocated 2 GB of data space and 1 GB of log space. This is sufficient for small environments. Please refer to the "Sizing the Implementation" section of the *CA ControlMinder Premium Edition Implementation Guide* for more details.	
Update the properties of the database user setting the new database as the user's default database.	

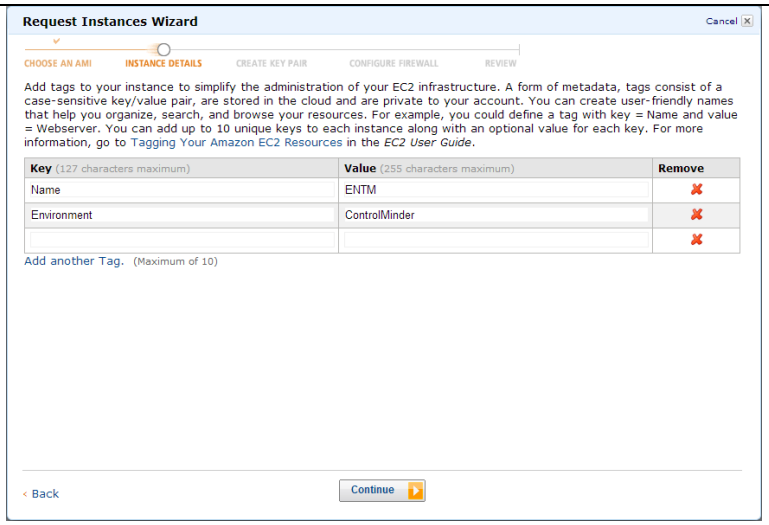
Deploying Enterprise Management

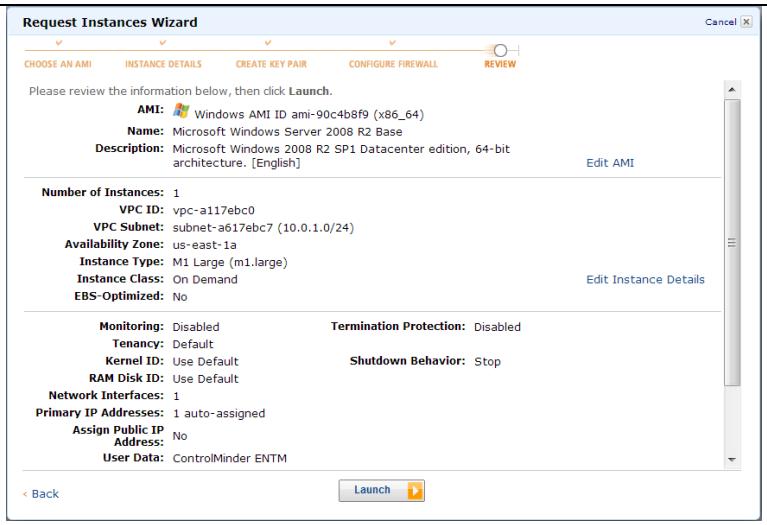
Create a Windows 2008 R2 instance on the private subnet and install CA ControlMinder Enterprise Management.

Create ENTM Instance

Create another instance using the Classic Wizard. Select "Microsoft Windows Server 2008 R2 Base" 64 bit.	
Set Instance Type to M1 Large. For the Launch into information, select the radial button for EC2-VPC and set the subnet to the private subnet (10.0.1.0/24). Click the Continue button.	

Provide User Data to identify your instance. Keep default values for all other Settings. Click the Continue button.	
Click the Continue button. 30 gigabytes of disk storage is sufficient for the ENTM Server.	

Name your instance and provide any additional tags as required.	
Use the key pair associated you're your AWS ECS Account.	
Add the Default_Private Security Group to this instance	

Launch the instance by clicking the Launch button.	

Transferring the Software

From support.ca.com, download the ControlMinder software to the JumpBox server.

You will also need to download software that emulates a DVD drive. The ISO images of the ControlMinder software will be mounted in a virtual DVD drive.

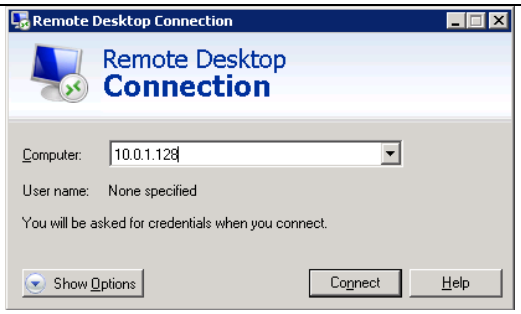
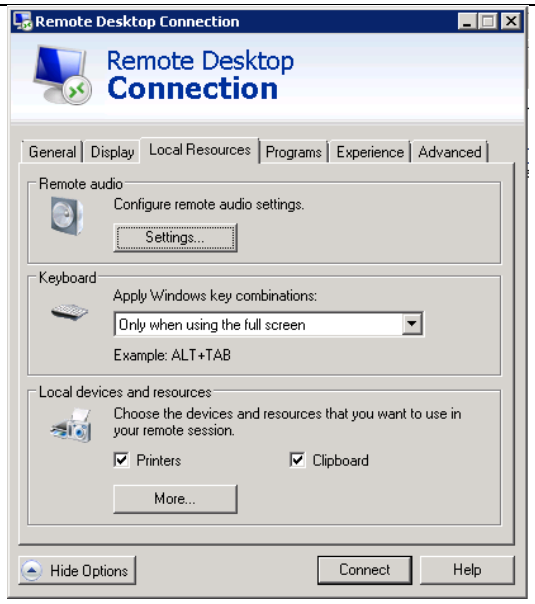
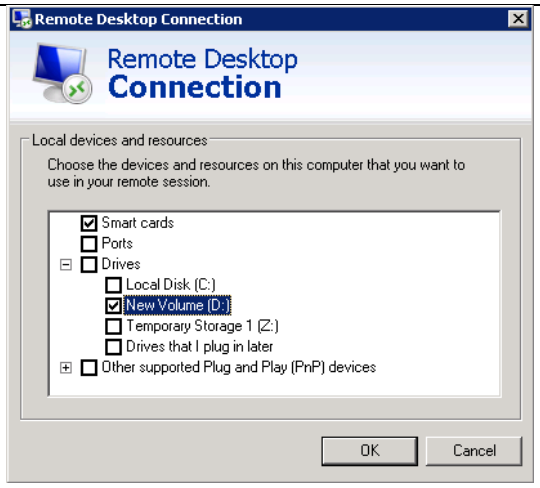
From the JumpBox server, copy the software to the ENTM Server.

Go to the list of running instances on the EC2 dashboard and select the ENTM instance.

Note the IP address of the ENTM server.

Name	Instance	AMI ID	Root Device
MSSQL Server	i-06355c63	ami-dac7bbb3	ebs
JumpBox	i-60345d05	ami-90c4b8f9	ebs
VPC NAT	i-886aadeb	ami-4f9fee26	ebs
ENTM	i-d2c69db1	ami-90c4b8f9	ebs

Scheduled Events:	No scheduled events
VPC ID:	vpc-a117ebc0
Source/Dest. Check:	enabled
Placement Group:	
RAM Disk ID:	-
Key Pair Name:	ControlMinder
Monitoring:	basic
Elastic IP:	-
Root Device Type:	ebs
IAM Role:	-
EBS Optimized:	false
Block Devices:	sda1
Network Interfaces:	eth0
Public DNS:	
Private DNS:	ip-10-0-1-128.ec2.internal
Private IPs:	10.0.1.128
Secondary Private IPs:	

From the JumpBox server, use Remote Desktop to connect to the ENTM Server. Before clicking the Connect button, click the Show Options button.	
Click the Local Resources tab. Click the More button.	
Select the local drive to the JumpBox server where you already downloaded the ControlMinder software. Click the OK button and then click the Connect button. To obtain the Windows Administrator password for the ENTM Server follow the same steps described as described for the JumpBox server. Copy the software to the Temporary Storage available on the ENTM Server.	

ENTM Installation

Steps to install Enterprise Management include:

- Install the DVD Drive emulator.
- Install the third party prerequisite components.
- Install the Enterprise Management software.
- Reboot the server.

The installation process typically requires from as little as 15 minutes up to 60 minutes.

After you install the DVD drive emulator, mount the CA ControlMinder Third-Party Components ISO image.

Always run the installation utilities as administrator. On Windows 2008 R2 servers, this implies right-clicking the installation binary and selecting Run as administrator from the menu. An example is noted in a screenshot below.

The following installation example loads the product ISO images in the D: drive. Adjust the drive letter as required for your environment.

The drive letter of the target disk drive is not important, but it is important to pick a disk drive with sufficient disk storage. The **minimum space** required is :

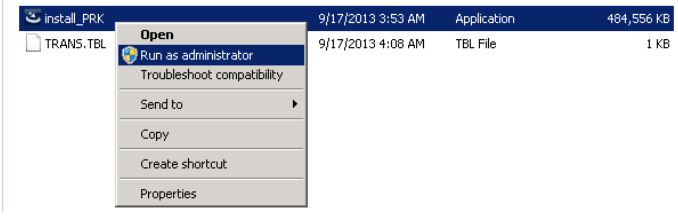
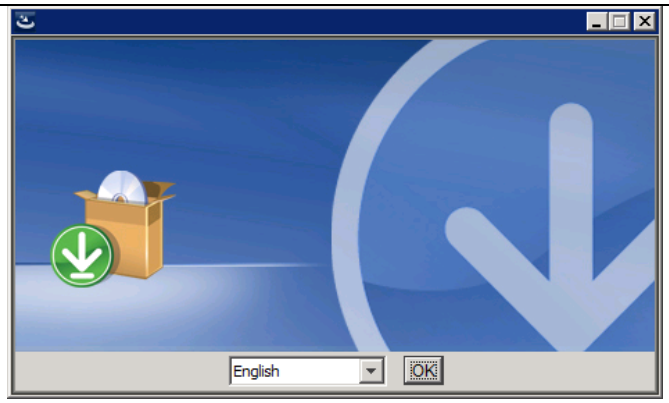
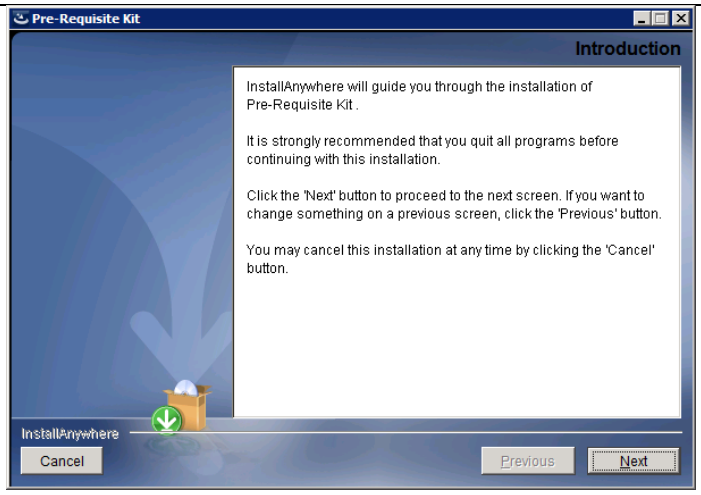
- JDK (from the Third-Party Components) 200 MB
- JBoss (from the Third-Party Components) 850 MB
- Enterprise Management 1.10 GB

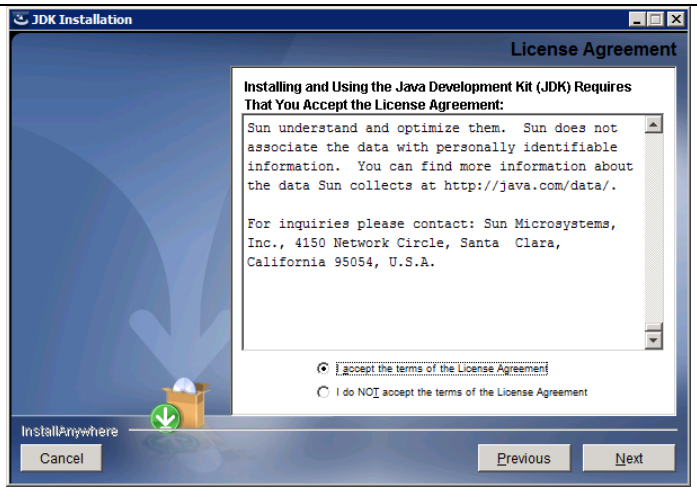
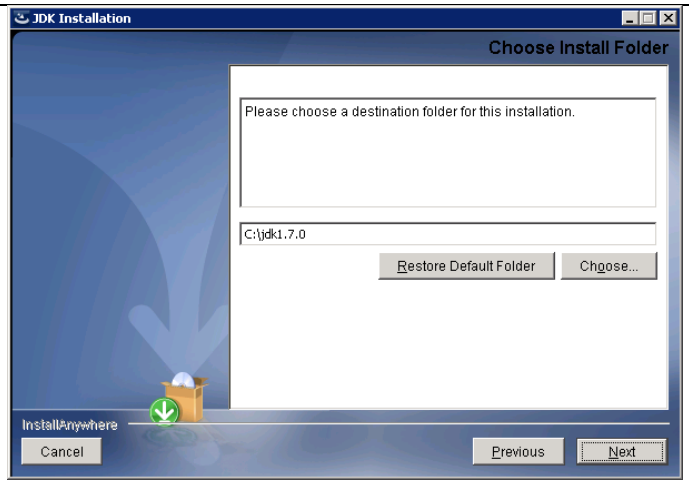
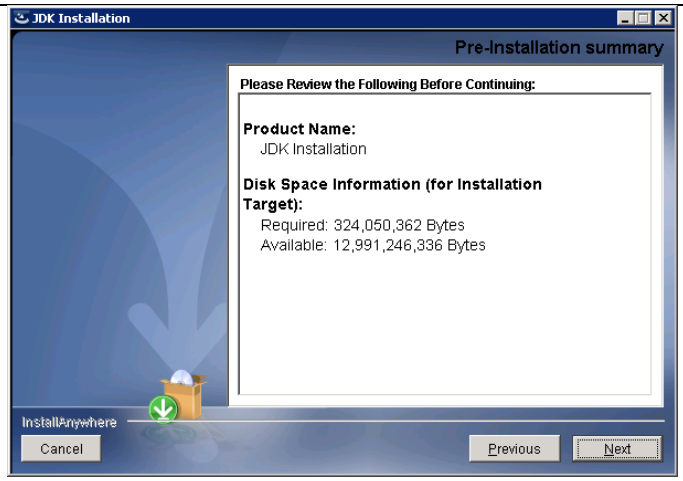
Install Third-Party Components

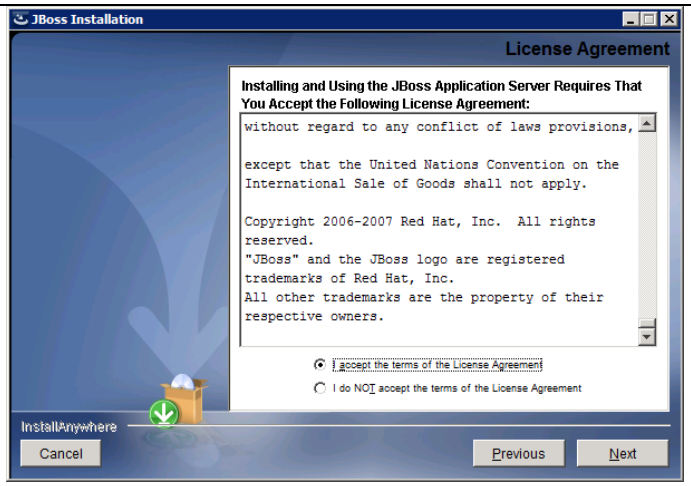
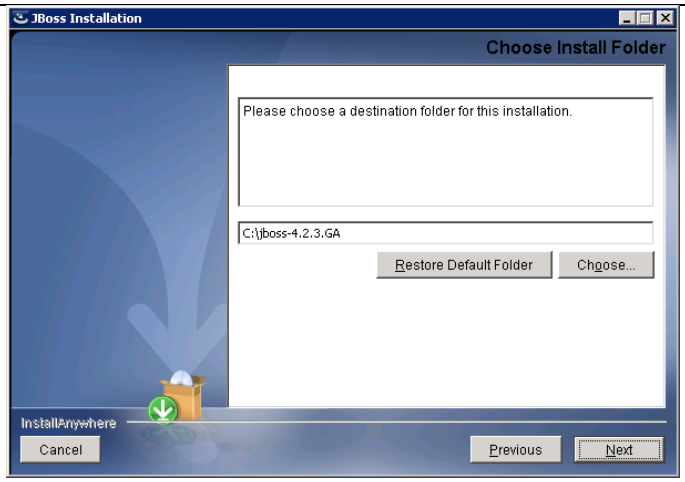
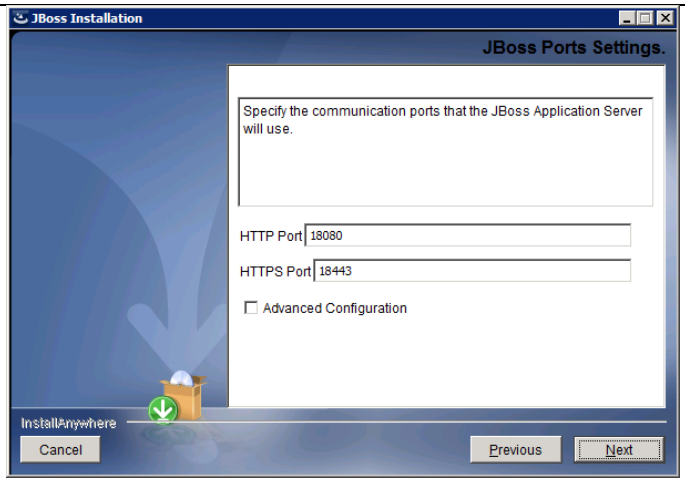
Login to the ENTM Server as a member of the local Administrators group.

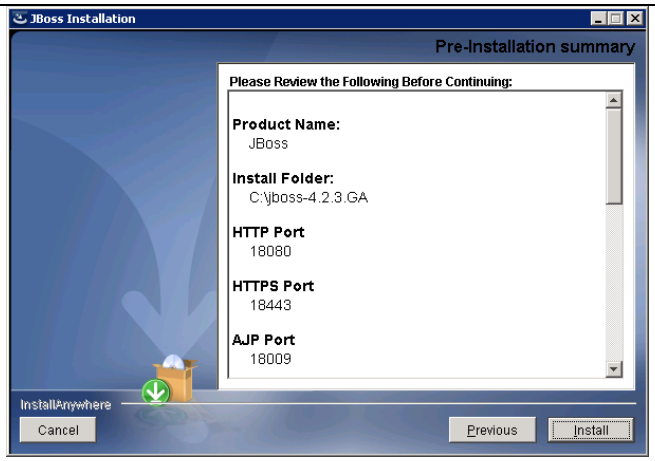
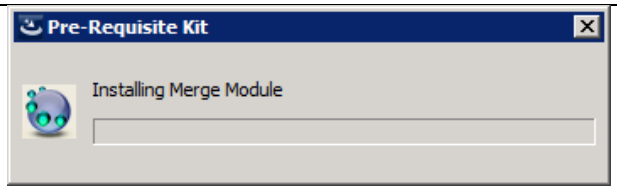
Mount the ISO image containing CA ControlMinder Third-Party Components for Windows.

Important: Do not use a UNC path or remote share to specify the software location

Locate install_PRK.exe found in the PrereqInstaller directory of the Third-Party Components ISO image. Start the installation by right-clicking **Install_PRK.exe** and selecting Run as administrator from the menu. This will install the Java Development Kit and JBoss.	
Click the OK button to accept English as the installation language.	
Click the Next button.	

JDK Installation Read the License Agreement as you use the scrollbar to advance through the document. Click the radial button noting I accept the terms of the License Agreement. Click the Next button.	
Select the destination folder. Click the Next button.	
Click the Next button.	

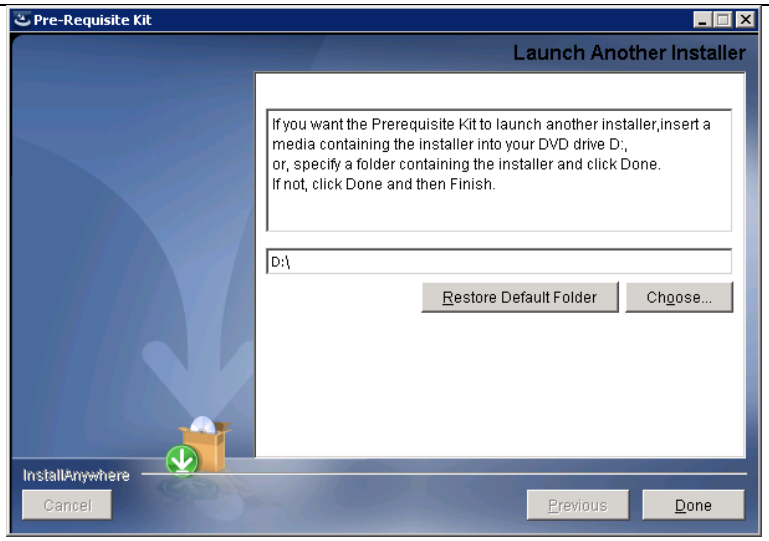
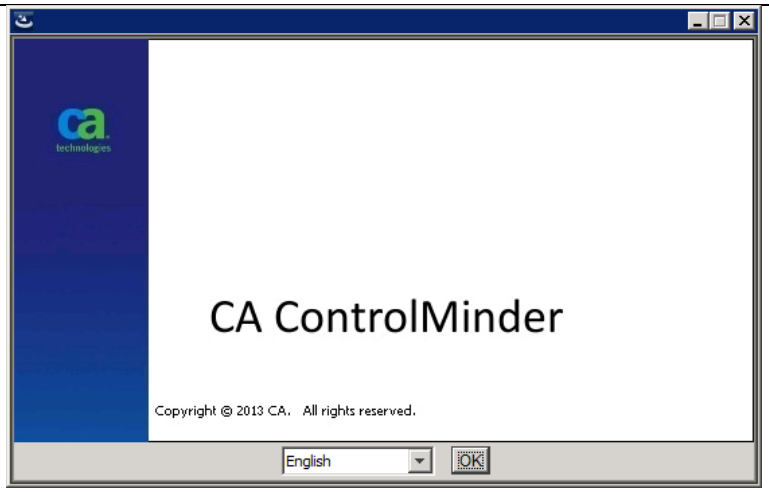
JBoss Installation Read the License Agreement as you use the scrollbar to advance through the document. Click the Next button.	
Select the destination folder. Click the Next button.	
Click the Next button.	

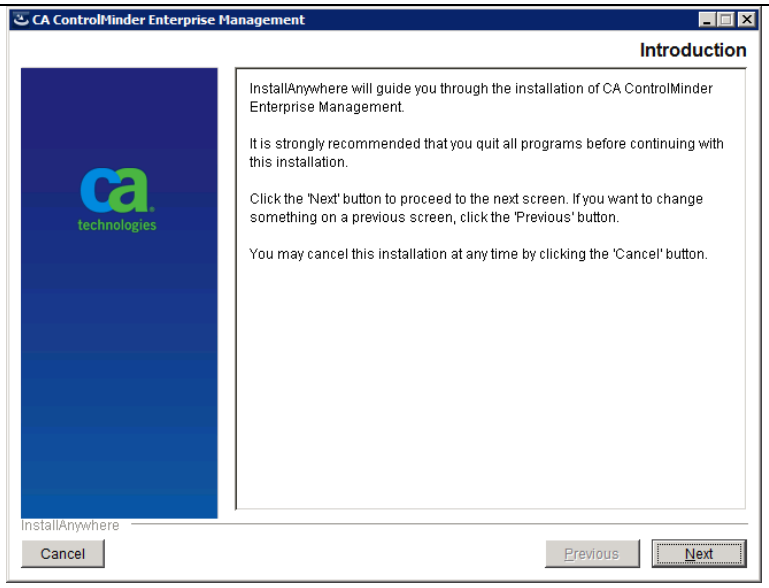
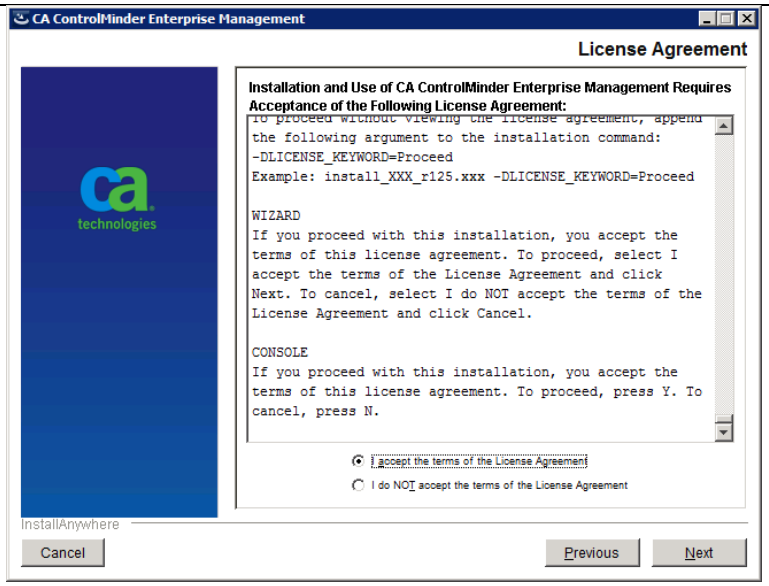
Click the Install button.	
Wait for installation to complete	

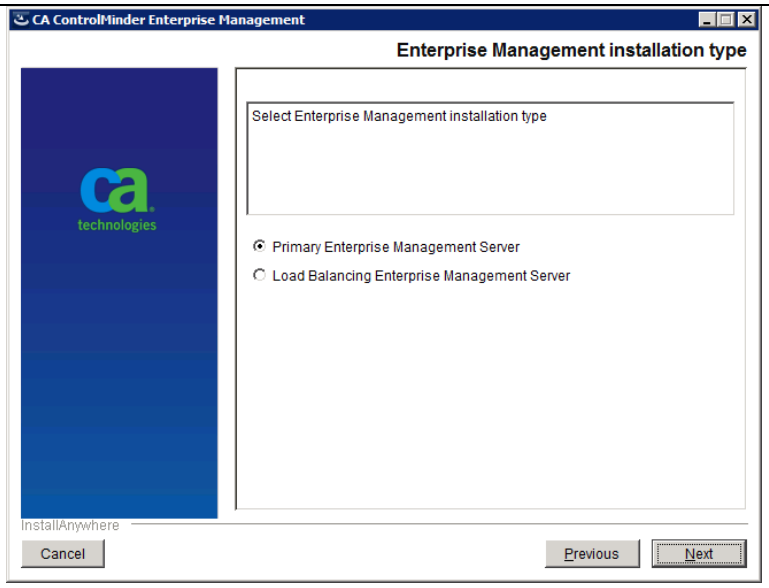
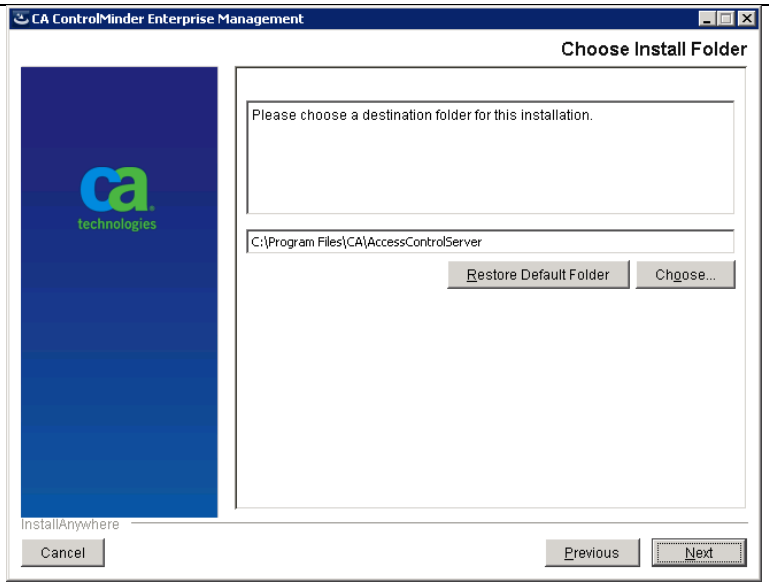
Install Enterprise Management

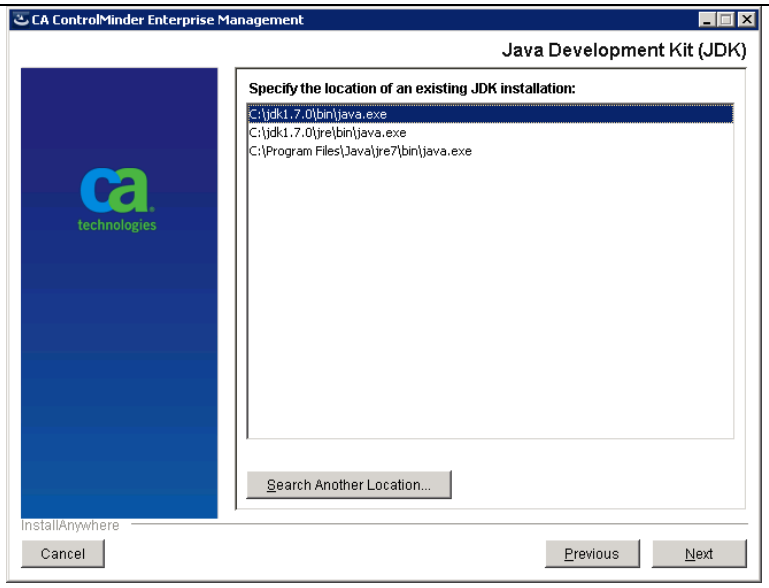
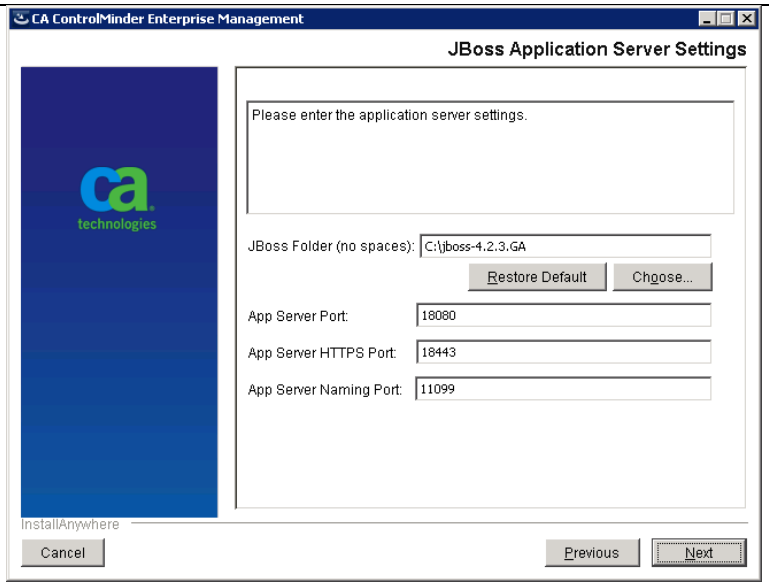
Either the Third-Party Components installer can launch the Enterprise Management installation, or you can manually start the installer by running ProductExplorer from the CA ControlMinder Server Components ISO image.

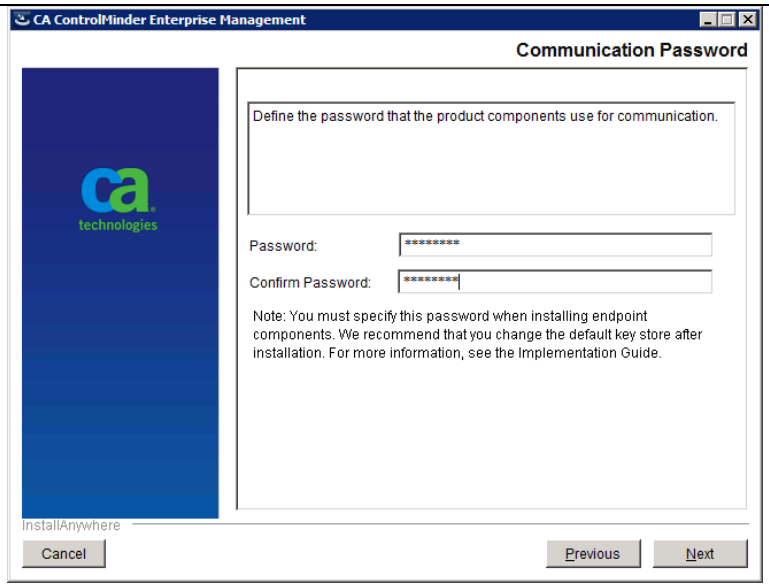
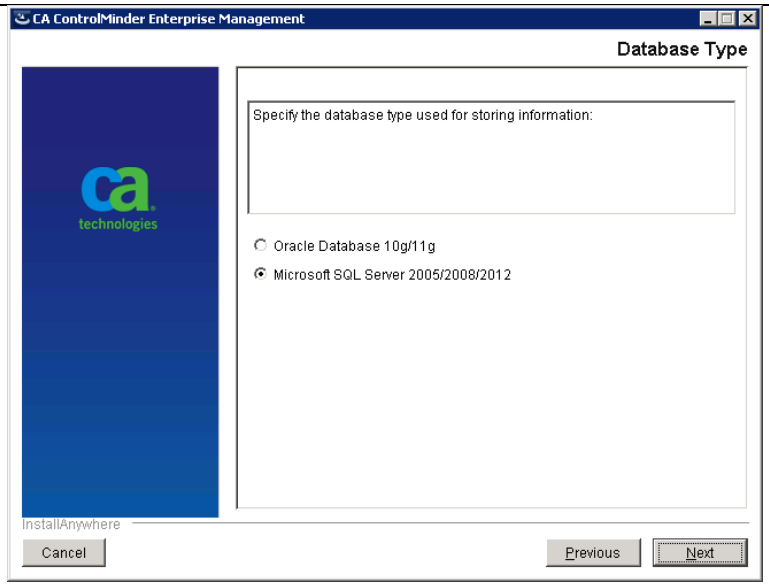
The following example has the Third-Party Components installer start the Enterprise Management installation.

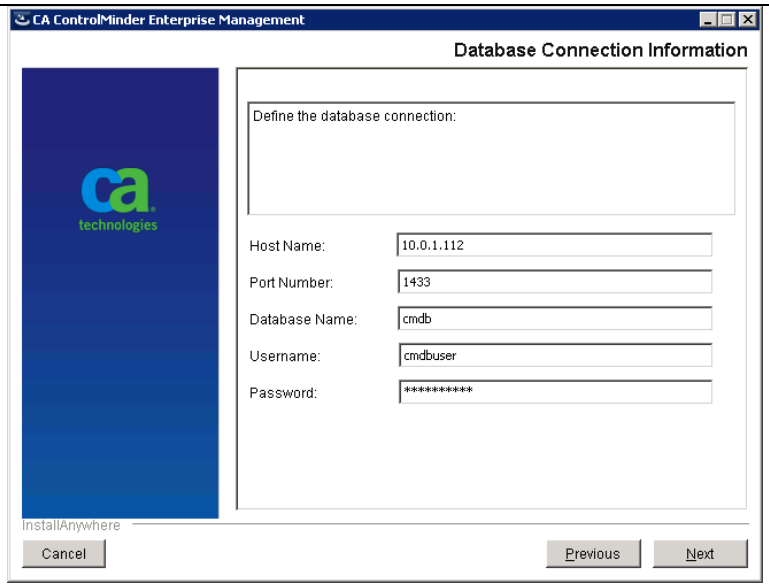
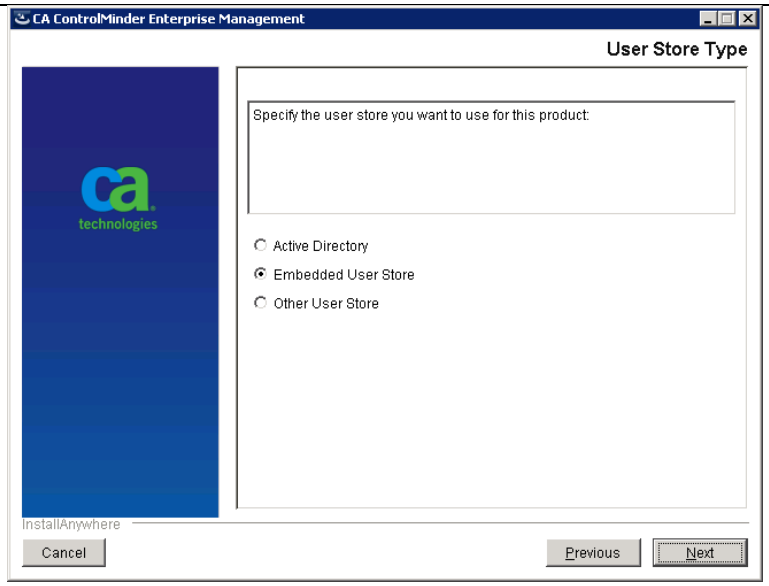
Mount the CA ControlMinder Server Components ISO image in the same virtual DVD drive where the Third-Party Components ISO image was installed. Click the Done button.	
If ProductExplorer is started manually, select Enterprise Management from the available choices.	
Click the OK button to accept English as the installation language.	

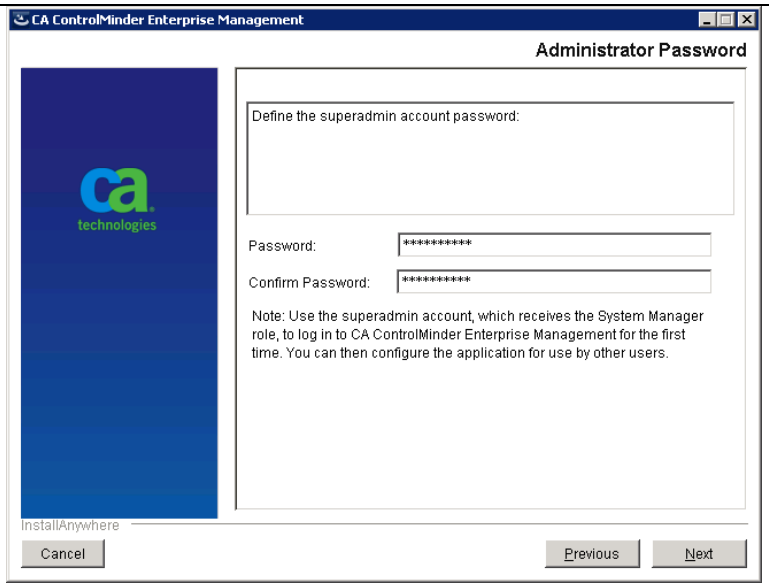
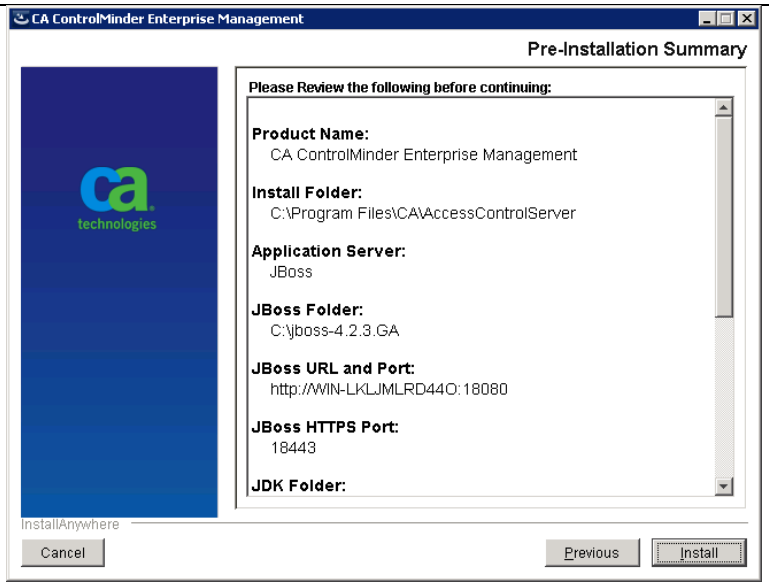
Click the Next button.	
Read the License Agreement as you use the scrollbar to advance through the document. Click the Next button.	

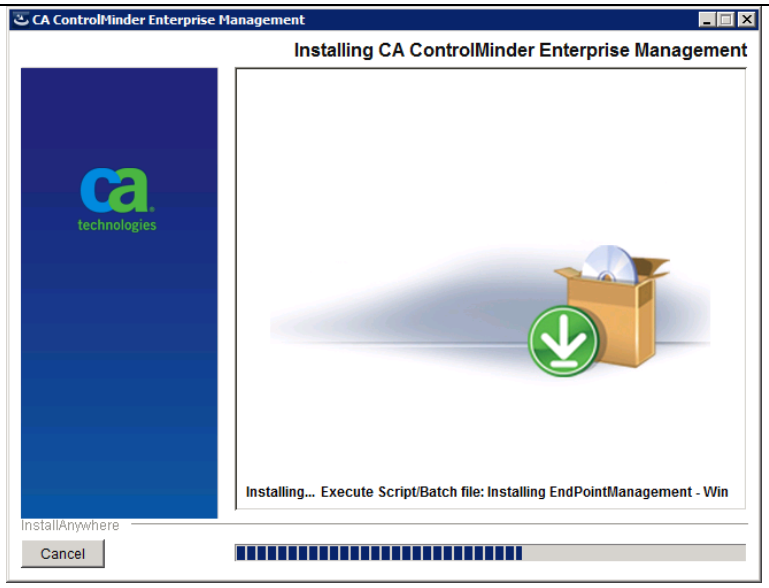
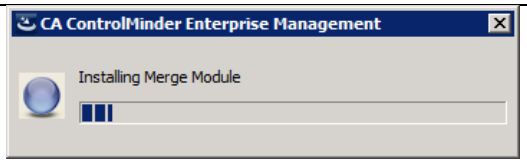
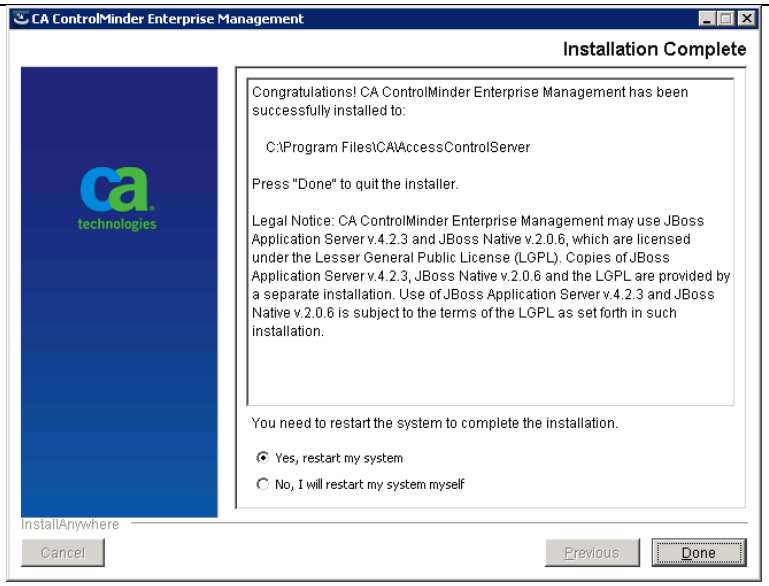
Select the radial button next to Primary Enterprise Management Server Click the Next button.	
Select the destination folder. Click the Next button.	

Specify the location where you installed the Java JDK from the Third-Party Components ISO image. **Note**: This page will only appear if you started the installation manually from ProductExplorer.	
Verify the JBoss settings. NOTE: The JBoss service must NOT be running at this time. Click the Next button.	

Provide the communication password. **NOTE**: This password Is used internally by Enterprise Management components. Click the Next button.	
Select the radial button for Microsoft SQL Server as the Database Type. Click the Next button.	

Enter the connection information for the Microsoft SQL Server database. Click the Next button.	
Select the radial button for Embedded User Store as the User Store Type. Account information for all Enterprise Management users will be stored in the Microsoft SQL Server database. Click the Next button.	

Provide the password for the superadmin account. This will be the only user available after the installation. The superadmin account is assigned the System Manager role. Click the Next button.	
Review the installation details. Click the Install button.	

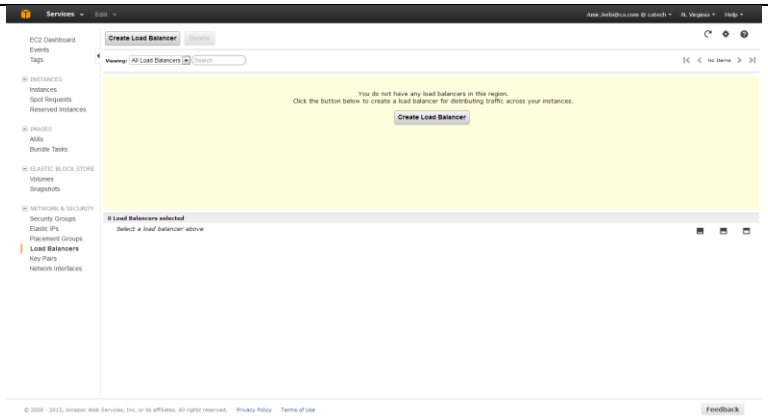
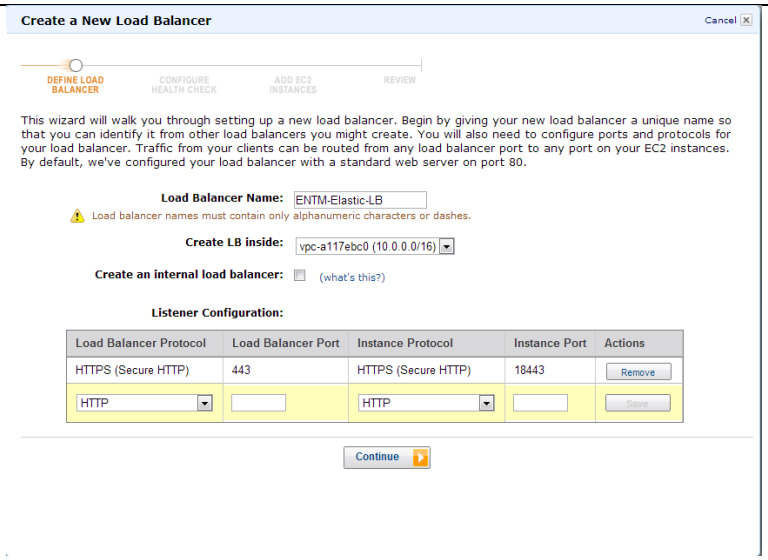
Wait for the installation to complete Important: If the installation does not appear to start, an installation confirmation window may be hiding under the current window. Move the top window and check for an underlying window.	
The installation is expected to take from 15 to 60 minutes to complete	
After the installation successfully completes, click the Done button to reboot the server and finalize the installation.	

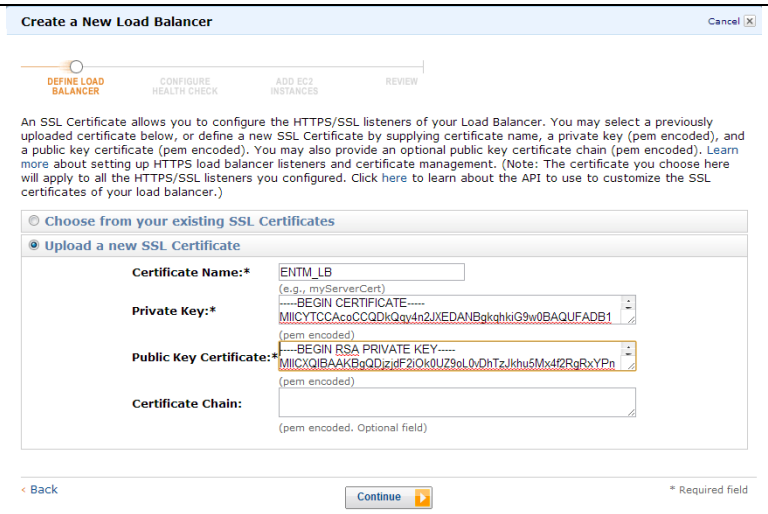
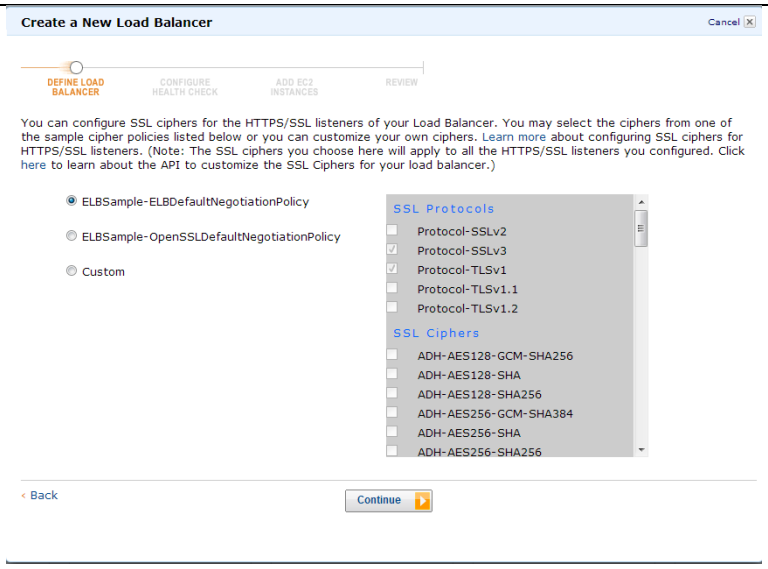
Create Amazon Elastic Load Balancer

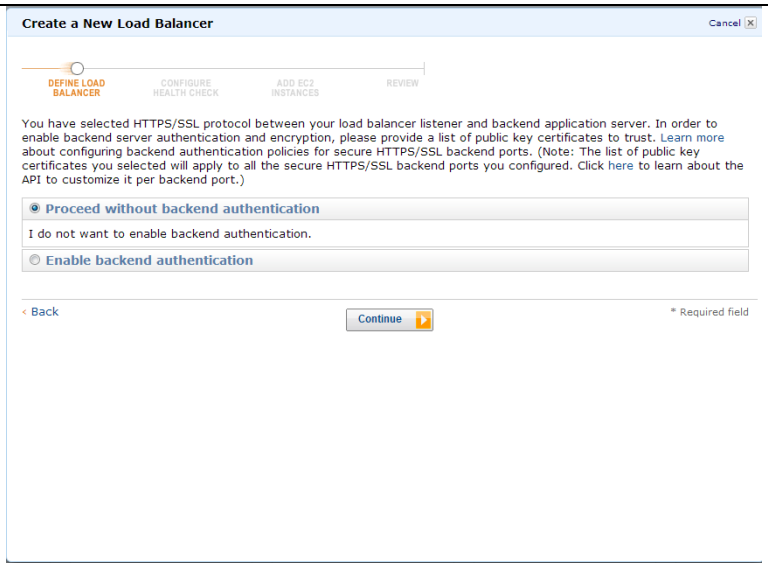
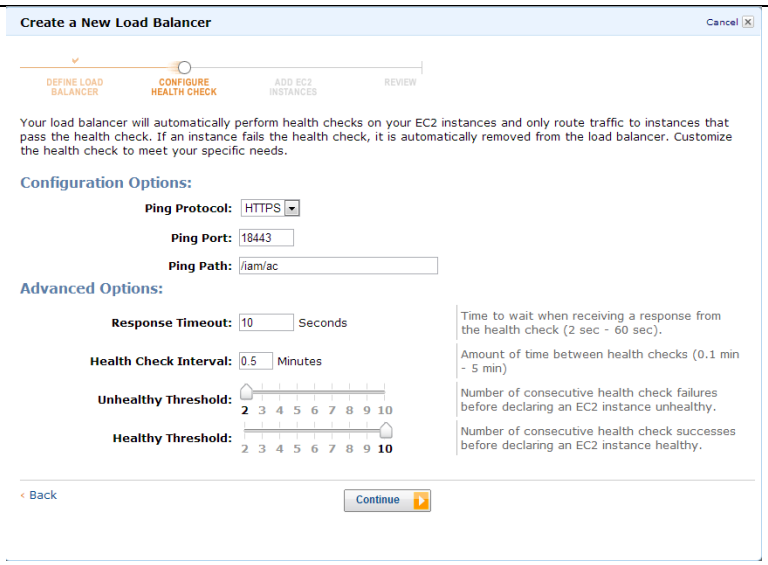
The ENTM Server is not accessible from the internet because it is deployed in the VPC private subnet, but browser access to Enterprise Management may be required. Amazon Elastic Load Balancer can be employed to provide such access.

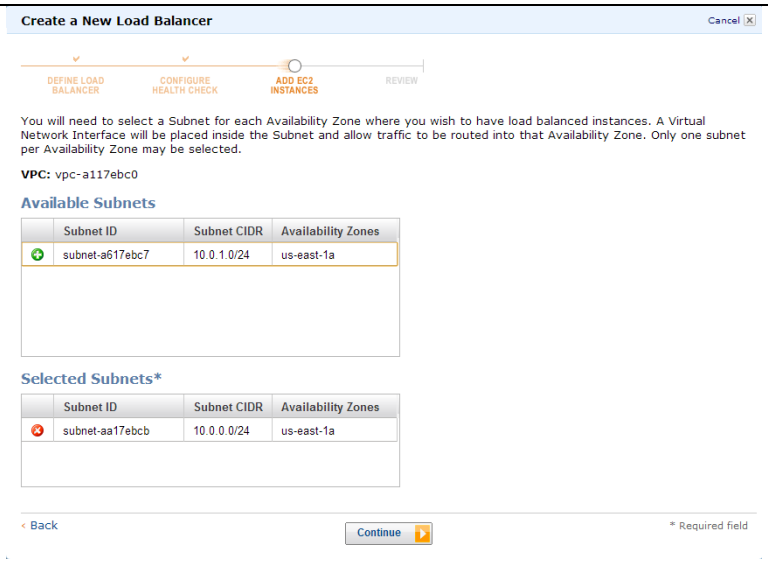
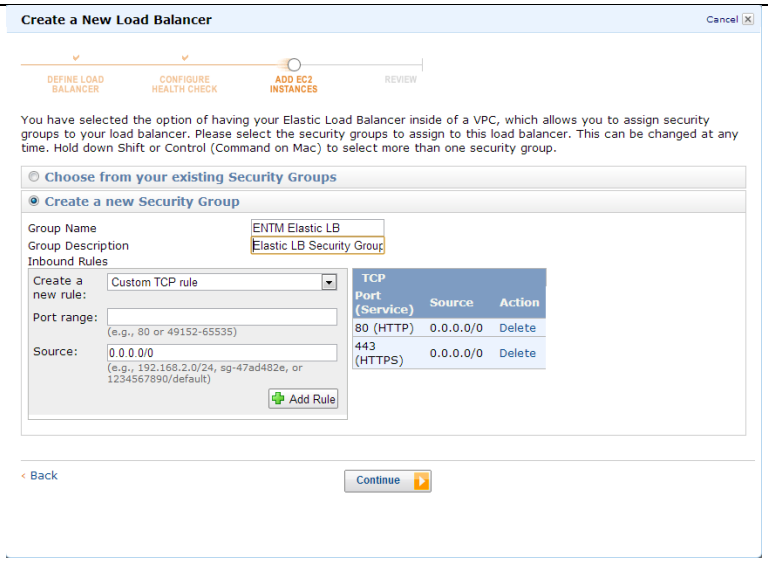
In case it is necessary to implement Load Balancing Enterprise Management servers for scalability, the Amazon Elastic Load Balancer can also balance the load across all Enterprise Management servers.

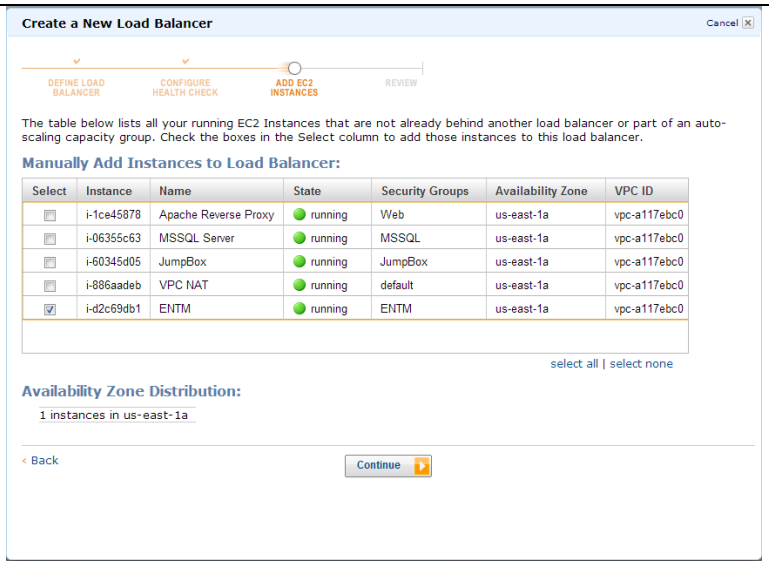
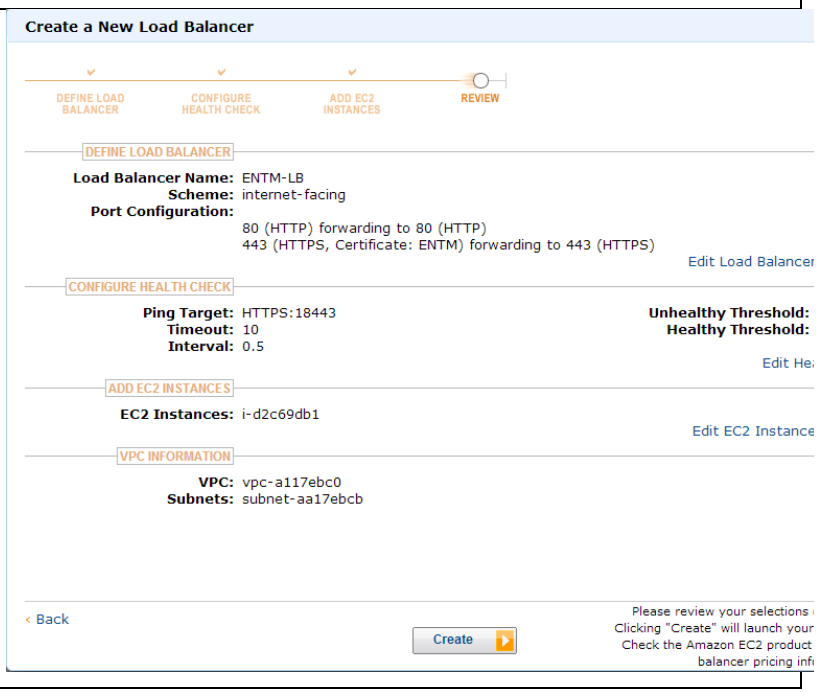
As an alternative, Appendix C describes how to configure an Apache proxy server instead of using Amazon Elastic Load Balancer.

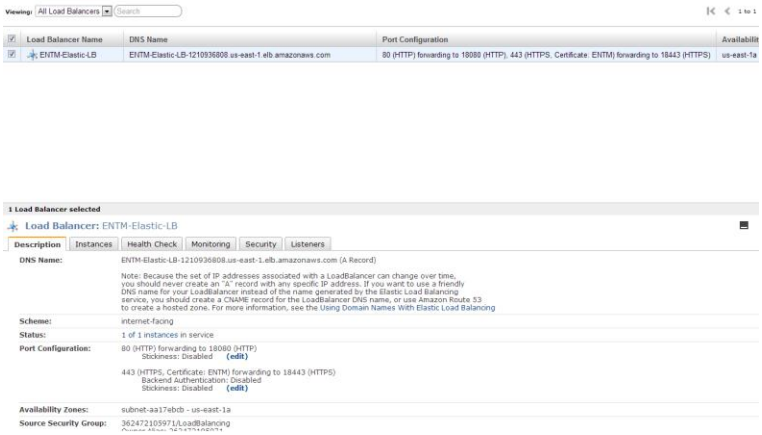
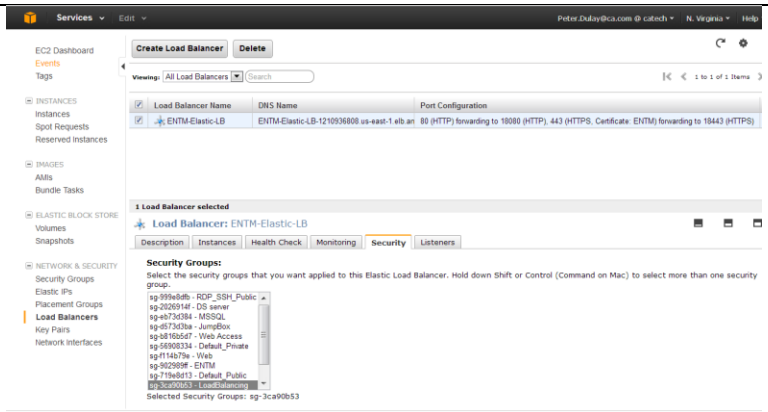
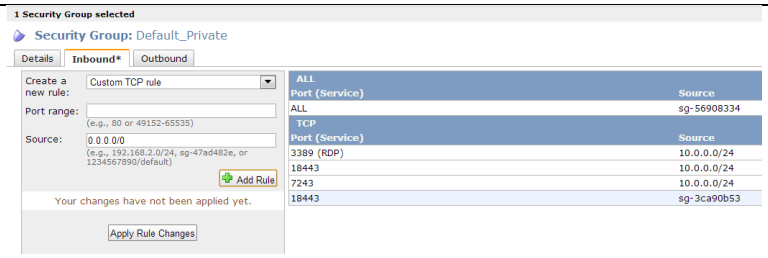
Choose "Load Balancers" option on the Amazon EC2 left side menu. Click on the "Create Load Balancer" button.	
Create the load balancer on the public subnet. Configure two listeners: • One to route port 443 to port 18443 • The other to route port 80 to port 18080	

You should supply certificate information which will be used for SSL connectivity. Use the following guides for help. How to create a server certificate: http://docs.aws.amazon.com/IAM/latest/UserGuide/InstallCert.html How to create a self-signed certificate: http://www.akadia.com/services/ssh_test_certificate.html	
Select ELBSample-ELBDefaultNegotionPolicy that includes SSLv3 and TLSv1.	

Select “Proceed without backend authentication” and click Continue.	
Configure the URL that will be used by the Load Balancer for health monitoring. Specify port 18433 and path “/iam/ac”.	

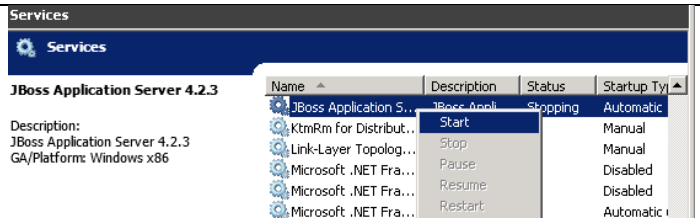
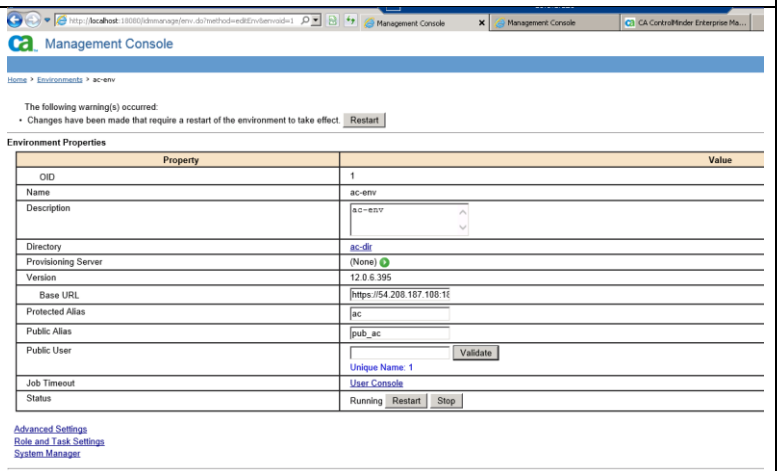
Select the private subnet as the subnet where load balanced instances are located. As already noted, this scenario is interested in providing browser access to the ENTM Server.	
Assign the Web Access Security Group to the Amazon Elastic Load Balancer.	

Add the ENTM Server instance to the load balancer.	
Click the Create button to create the new load balancer.	

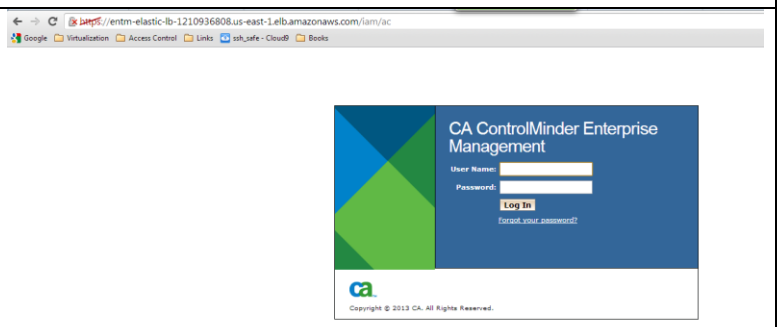
The newly created load balancer will be displayed in the list.	
Allow access to ENTM from the load balancer. You need to use the security group ID of the load balancer. You can obtain the group name from the load balancer properties – Security tab.	
Update the Default_Private Security Group adding a rule to allow communication from the Amazon Elastic Load Balancer to instances on the private subnet over port 18443. Remember that the ENTM Server is located on the private subnet.	

Configure ENTM to Use Amazon Elastic Load Balancer

Enable the idmmange URL on the ENTM server:
 	
Edit the following file:
 	
C:\jboss4.2.3.GA\server\default\deploy\IdentityMinder.ear\management_console.war\WEB-INF\Web.XML
 	
Change the "AccessFilter" token value to "true"
	`<filter>`
	`  <filter-name>AccessFilter</filter-name>`
	`  <filter-class>com.netegrity.ims.manage.filter.AccessFilter</filter-class>`
	`  <init-param>`
	`  <param-name>Enable</param-name>`
	`  <param-value>true</param-value>`
	`  </init-param>`
	`</filter>`

Restart JBoss to effect the change.	
From your Remote Desktop session to the ENTM Server, browse to the idmmanage URL: http://localhost:18080/idmmanage Choose "Environments" -> "ac-env". Change the "Base URL" property to point to the public address of the Amazon Elastic Load Balancer (e.g. https://<ip address>) Click the Save button.	

Disable the idmmanage URL
 	
Edit the following file:
 	
C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\management_console.war\WEB-INF\Web.XML
 	
Reset the AccessFilter token value to false.
 	
Restart JBoss to effect the change.
	`<filter>`
	`  <filter-name>AccessFilter</filter-name>`
	`  <filter-class>com.netegrity.ims.manage.filter.AccessFilter</filter-class>`
	`  <init-param>`
	`  <param-name>Enable</param-name>`
	`  <param-value>false</param-value>`
	`  </init-param>`
	`</filter>`

You can now access Enterprise Management via the Amazon Elastic Load Balancer.	

Deploying Distribution Server

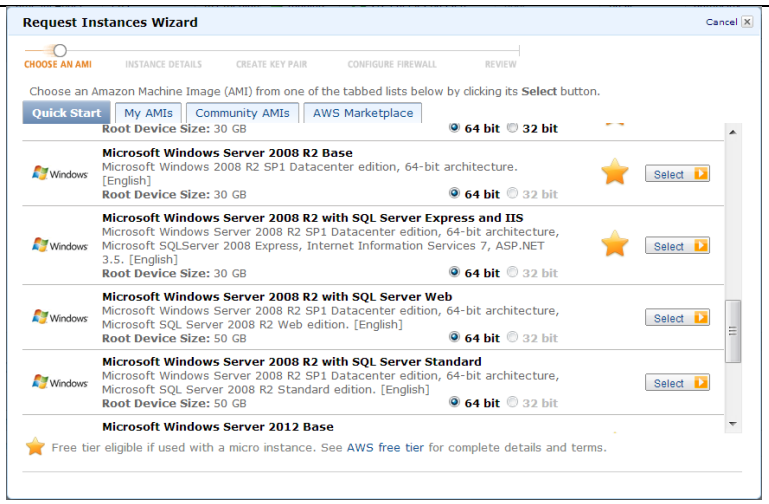
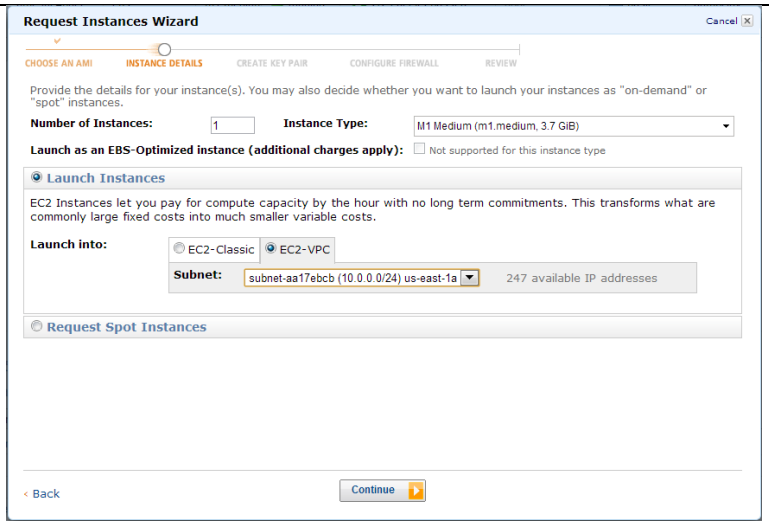
Deploy a Distribution Server on each subnet where there are ControlMinder endpoints.

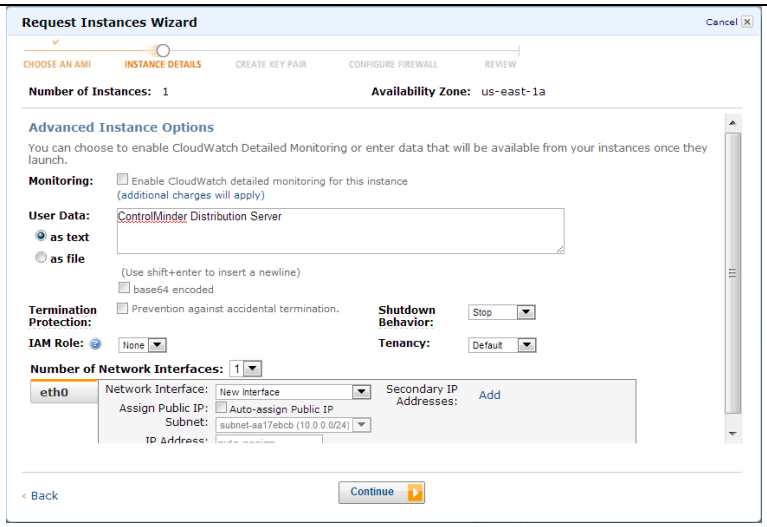
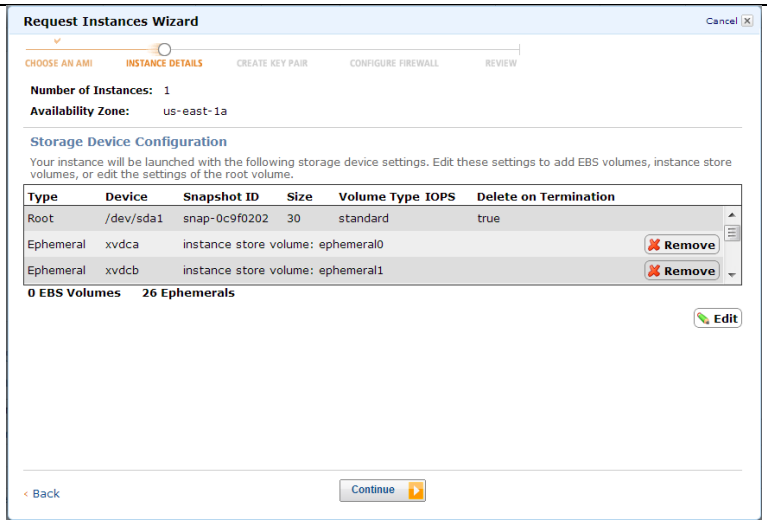
The Distribution Server provides communication services and scalability between the endpoints and the ENTM Server while limiting direct access to the ENTM Server.

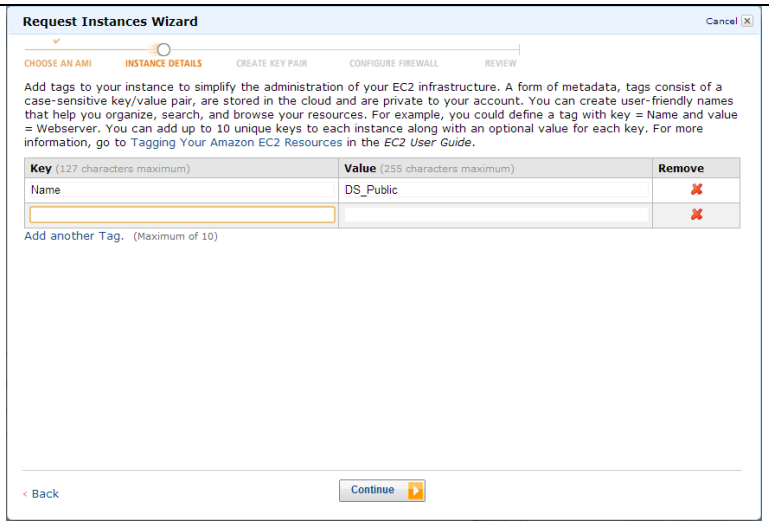
We will implement a distribution server that will be used to manage endpoint sin the public subnet.

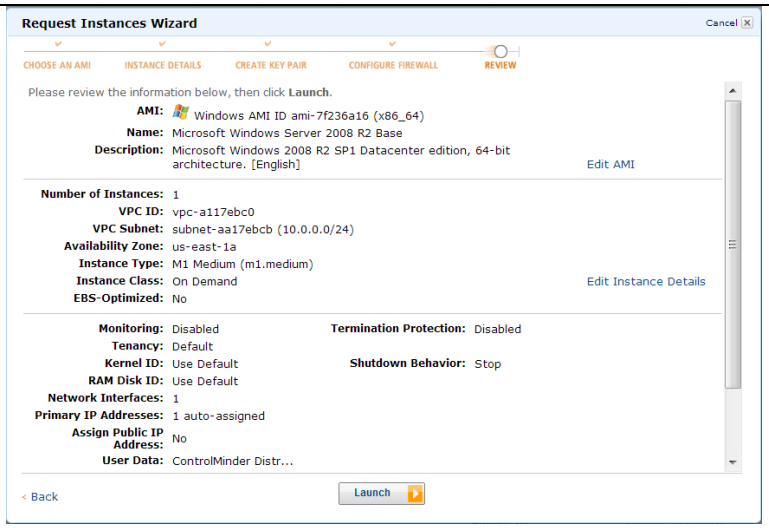
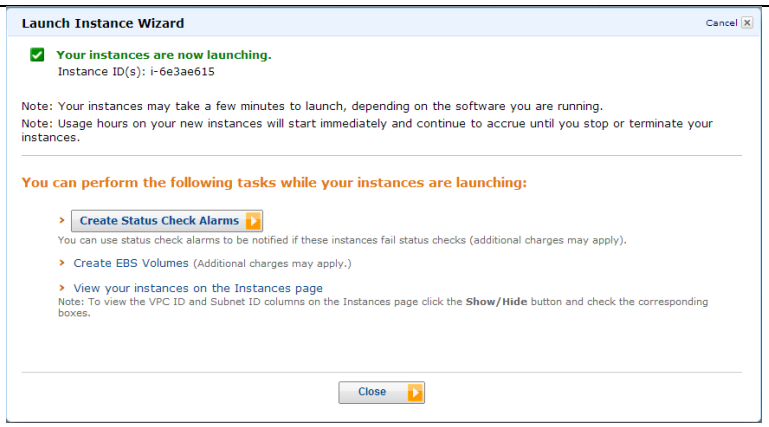
The endpoint located in the private segment can be directly managed by the embedded distribution server on the ENTM.

Create the Distribution Server Instance

Use the Classic Wizard to launch a new "Microsoft Windows Server R2 Base" instance	
Set Instance Type to M1 Large. For the Launch into information, select the radial button for EC2-VPC and set the subnet to the public subnet (10.0.0.0/24). Click the Continue button.	

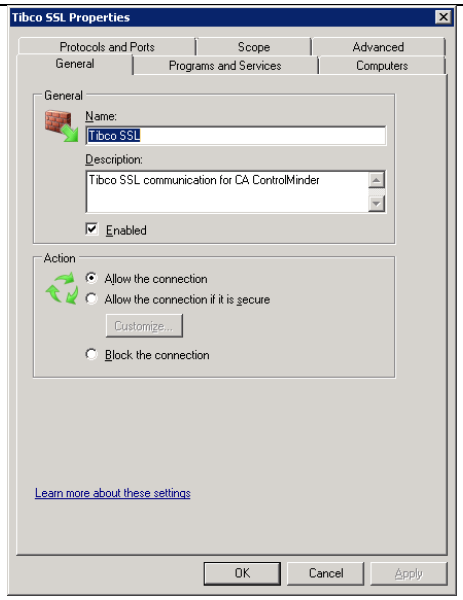
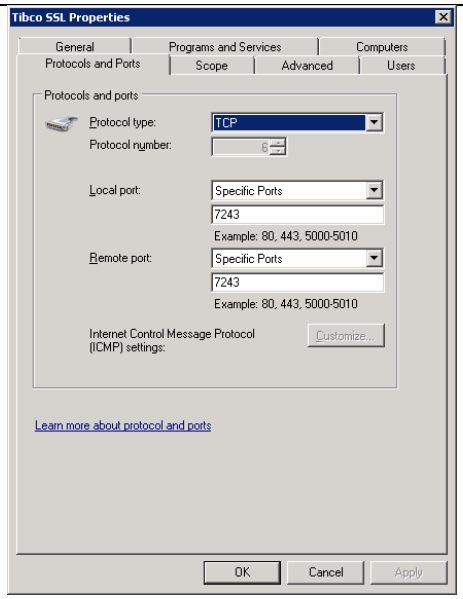
Provide User Data to identify your instance. Click the Continue button.	
Keep the default storage configuration. 30 gigabytes of disk storage is sufficient for the Distribution server.	

Name your instance and provide any additional tags as required.	
Use the key pair associated you're your AWS ECS Account.	
Add the Default_Public Security Group to the Distribution Server instance	

Click the Launch button.	
Click the Close button.	

Prepare to Install the Distribution Server

Tibco Communication Configuration

Ensure there are Microsoft Windows Firewall rules on both the ENTM Server and the Distribution Server to allow incoming and outgoing communication on the Tibco SSL Port (7243).	
	

Configure Name Resolution

The ENTM Server and the Distribution Server need to resolve each other's hostname.

This is not provided by default for an Amazon EC2 environment.

The hostname of the ENTM server throughout this example is WIN-LKLJMLRD44O; however, nslookup resolves the hostname as ip-10-0-1-128.ec2.internal.

Following the example, add an entry for the ENTM Server to the Distribution Server's hosts file:

10.0.1.128 WIN-LKLJMLRD44O WIN-LKLJMLRD44O.ec2.internal

Copy the ControlMinder software to the Distribution Server. Copy the same software that was copied to the ENTM Server:

- DVD Drive Emulator
- CA ControlMinder Third-Party Components for Windows
- CA ControlMinder Server Components for Windows

Remember that you can obtain the Distribution Server's IP address from its instance properties.

Steps to install Distribution Server include:

- Install the DVD Drive emulator.
- Install the third party prerequisite components.
- Install the Distribution Server software.
- Reboot the server.

The installation process typically requires from as little as 15 minutes up to 60 minutes.

After you install the DVD drive emulator, mount the CA ControlMinder Third-Party Components ISO image.

Always run the installation utilities as administrator. On Windows 2008 R2 servers, this implies right-clicking the installation binary and selecting Run as administrator from the menu. An example is noted in a screenshot below.

The following installation example loads the product ISO images in the D: drive. Adjust the drive letter as required for your environment.

The drive letter of the target disk drive is not important, but it is important to pick a disk drive with sufficient disk storage. The **minimum space** required is :

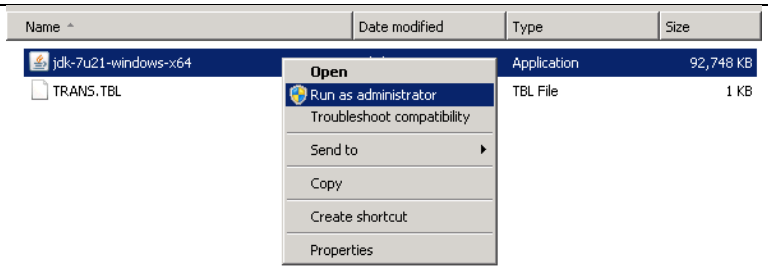
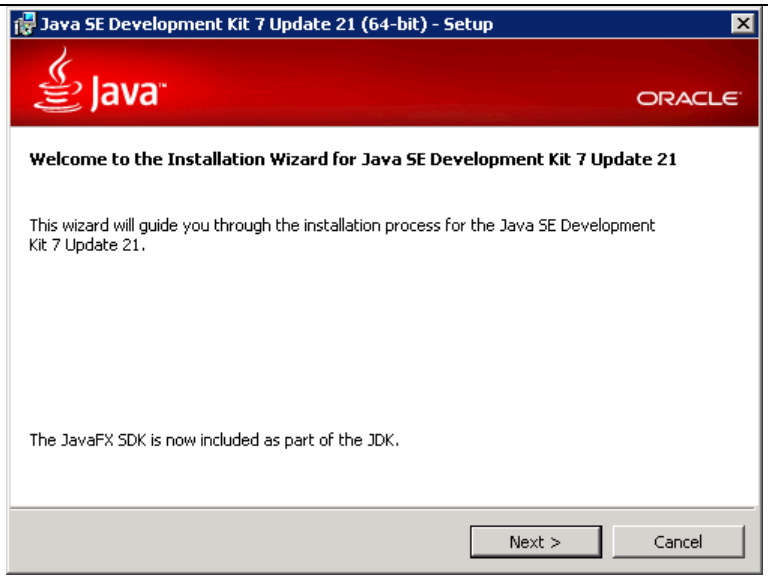
- JDK (from the Third-Party Components) 200 MB
- JBoss (from the Third-Party Components) 850 MB
- Enterprise Management ??? GB

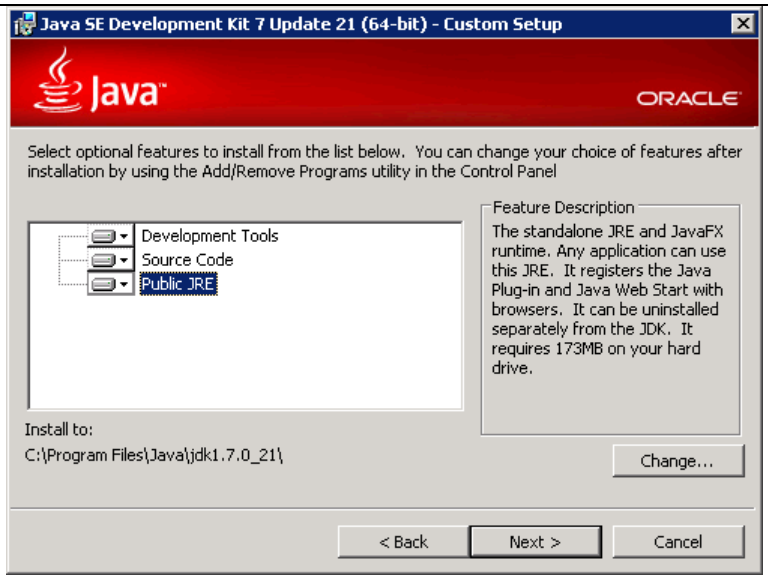
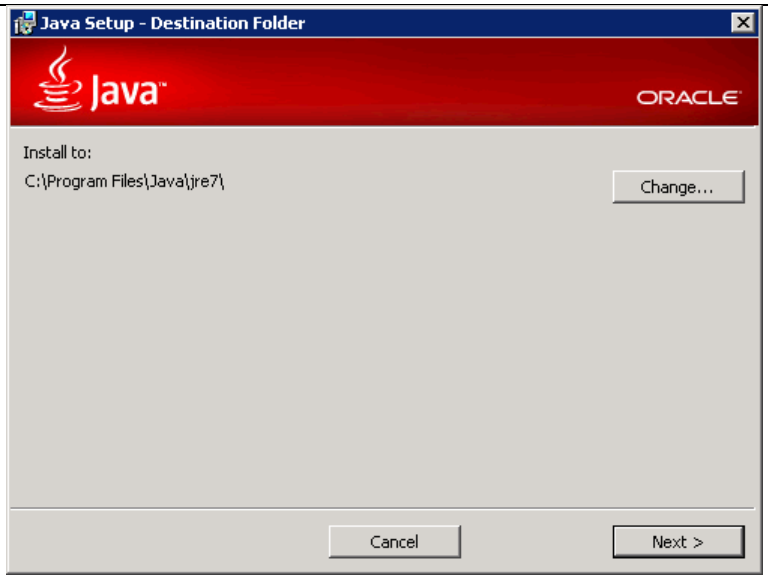
Install Third-Party Components

Login to the Distribution Server as a member of the local Administrators group.

Mount the ISO image containing CA ControlMinder Third-Party Components for Windows in the virtual DVD drive.

Important: Do not use a UNC path or remote share to specify the software location

Locate the Java SDK installer, **jdk-7u21-windows-x64.exe,** from the JDK-1.7.21_x64 directory on the DVD drive. Right click **jdk-7u21-windows-x64.exe** and choose Run as administrator.	
Click the Next button to start the Java SDK installation.	

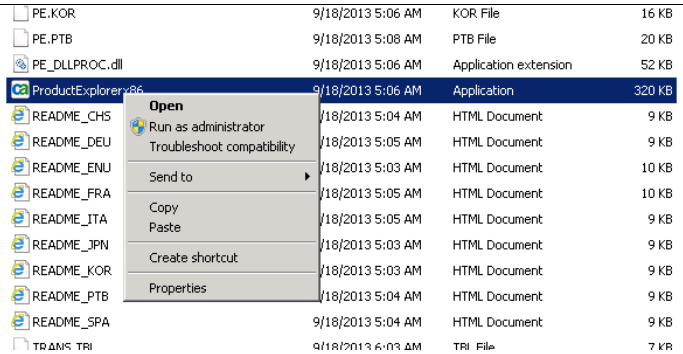
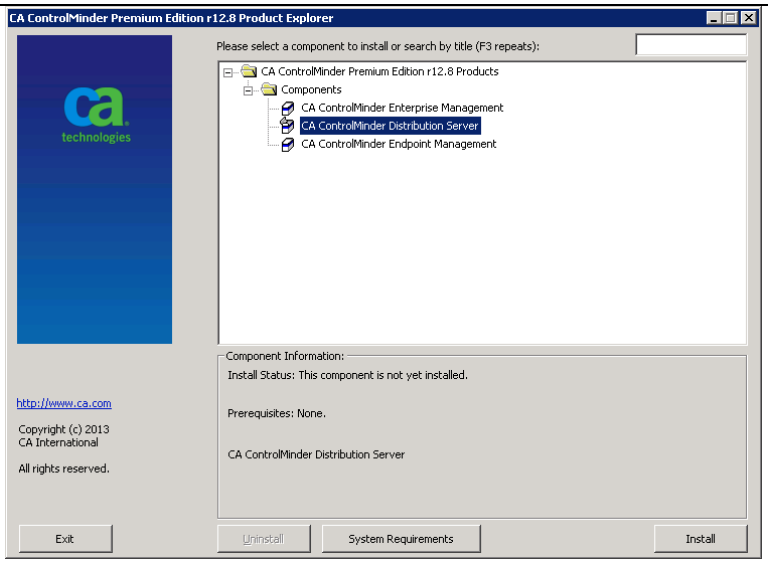
Click the Next button.	
Click the Next button.	

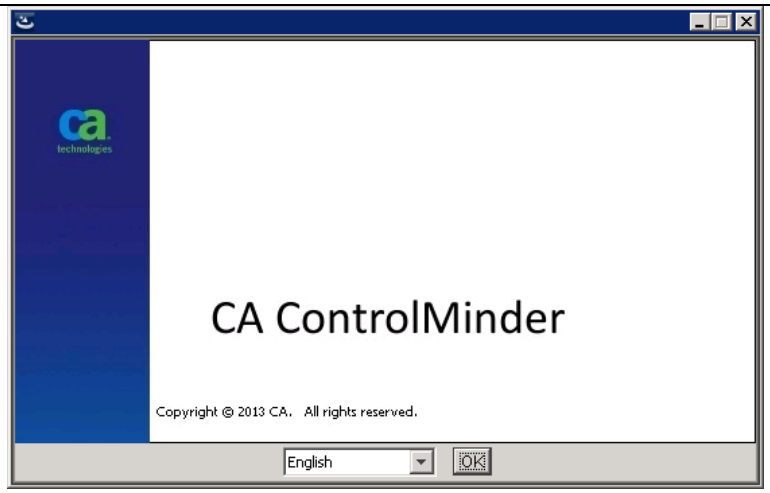
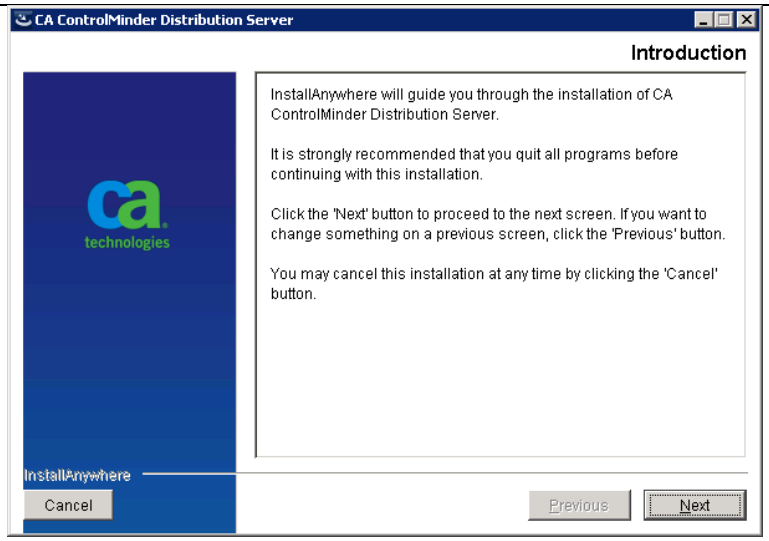
Click the Close button to finish the installation.	

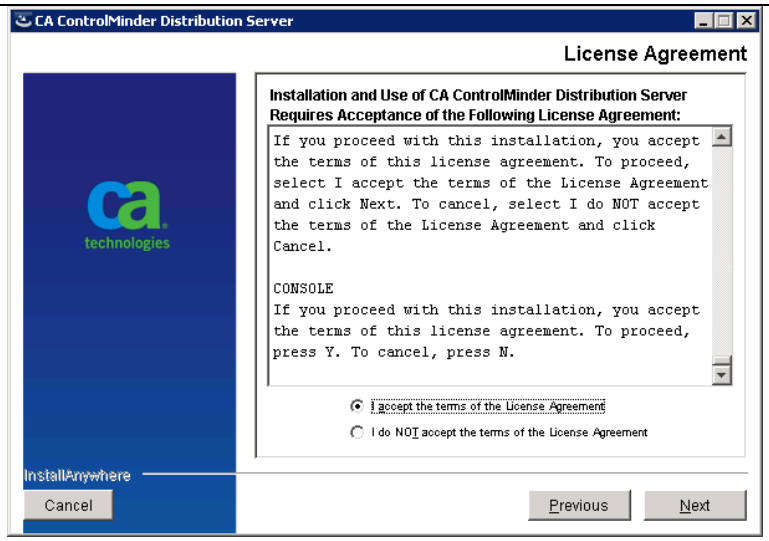
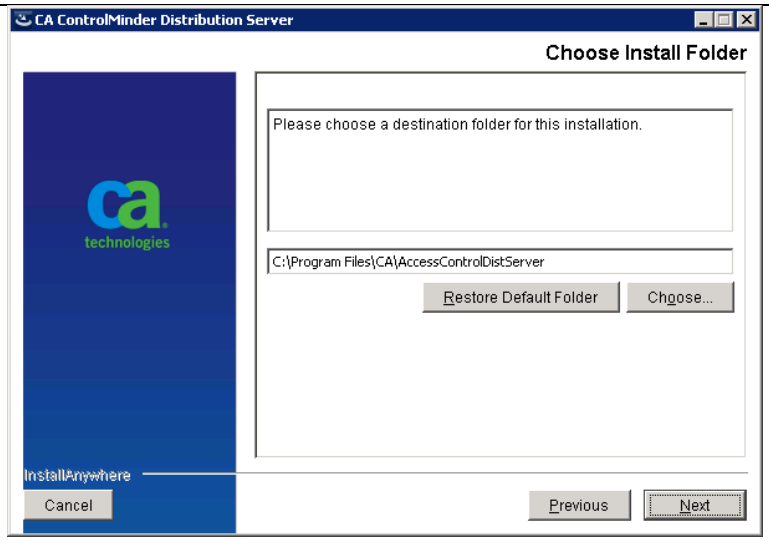
Install the Distribution Server

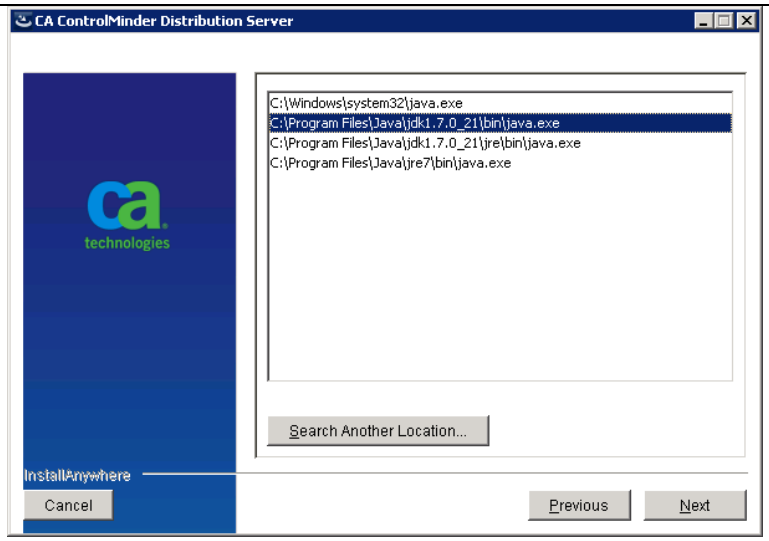
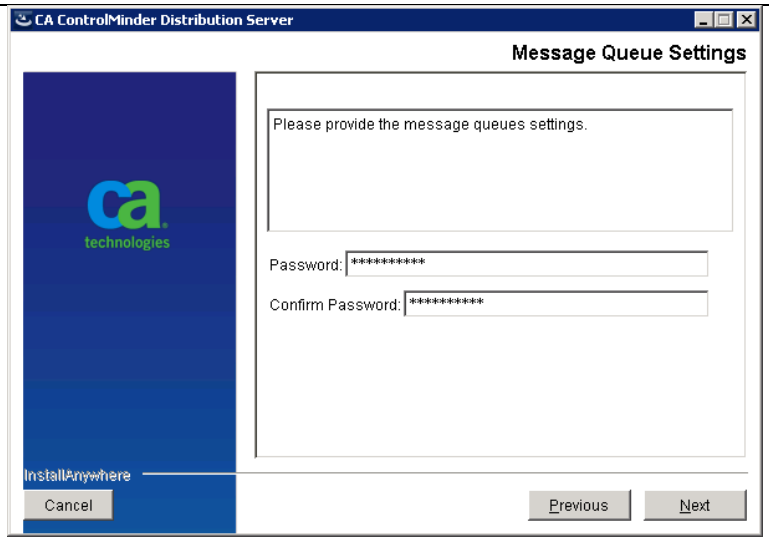
Mount the CA ControlMinder Server Components ISO image in the virtual DVD drive.

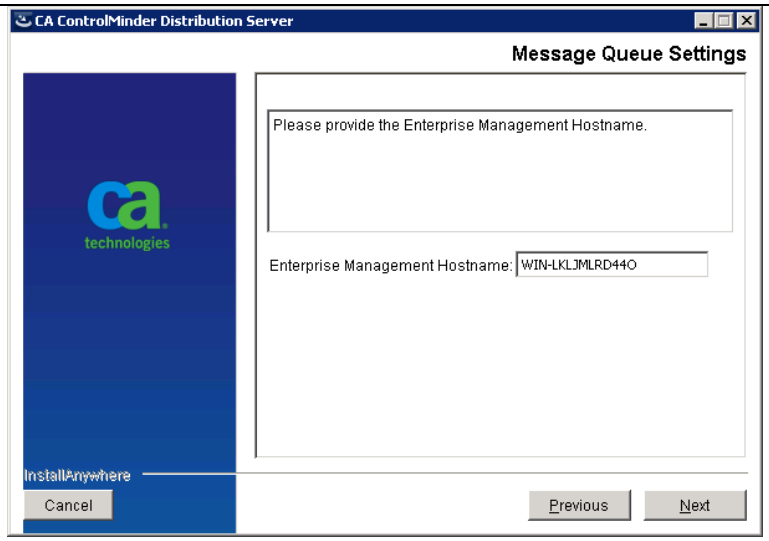
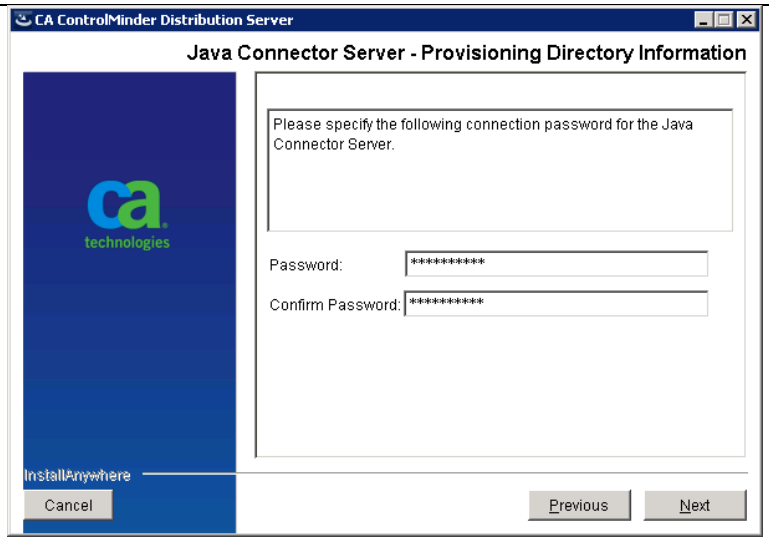
Important: Do not use a UNC path or remote share to specify the software location.

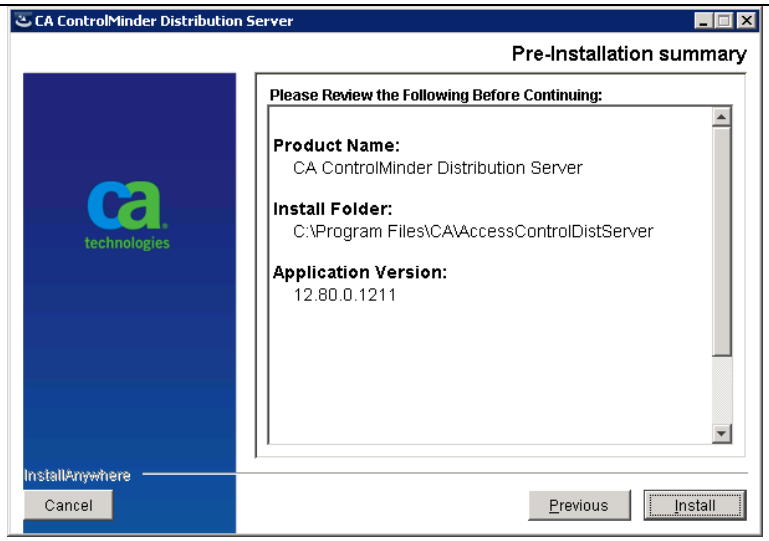
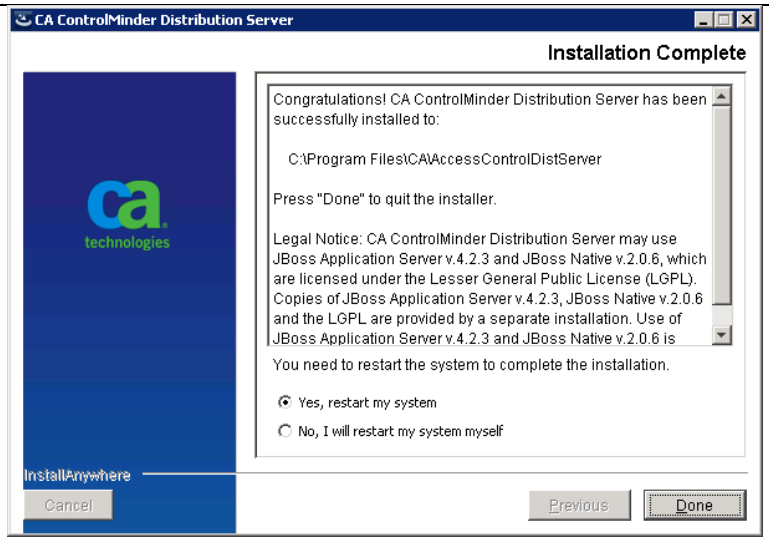
Start the Distribution Server installation by launching **ProductExplorer** from the virtual DVD drive. Remember to start **ProductExplorer** by right-clicking the executable and choosing Run as administrator.	
From the Components folder of **ProductExplorer**, select CA ControlMinder Distribution Server. Click the Install button.	

Click the OK button to accept English as the language for the installation.	
Click the Next button.	

Read the License Agreement as you use the scrollbar to advance through the document. Click the radial button noting I accept the terms of the License Agreement. Click the Next button.	
Select the installation directory. Click the Next button.	

Select the location where you previously installed the Java JDK from the Third-Party Components ISO image. Click the Next button.	
Provide the message queue password. This is the communication password you specified during the ENTM Server installation. Click the Next button.	

Provide the ENTM Server hostname. Ensure this hostname can be resolved. Click the Next button.	
Provide a password for the Java Connector Server. Click the Next button.	

Click the Install button.	
After the installation successfully completes, click the Done button to reboot the server and finalize the installation.	

Install ControlMinder Endpoints

Each endpoint on which ControlMinder is installed must resolve the hostname of the Distribution Server, and vice versa, the Distribution Server must resolve the hostname of each endpoint it services.

Update host files as appropriate, or if you implemented a DNS server, update DNS as appropriate.

Open Required Communication Ports

Either create of update a Security Group that allows communication on ports 8891 5249, and 7243 for communication between endpoints and the Distribution Server. Earlier, the Distribution Server was configured to allow communication on port 7243.For any active firewall, also ensure bidirectional communication on these ports.

Connect to the endpoint where you want to install the endpoint software.

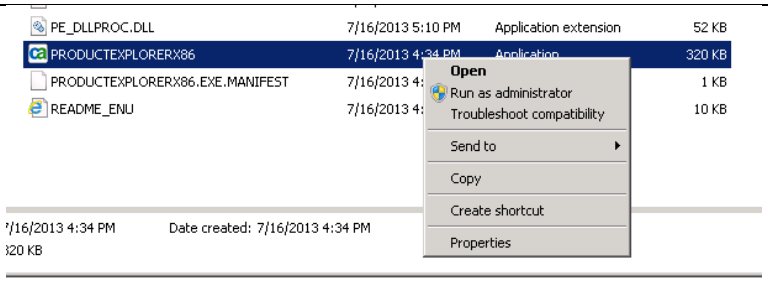
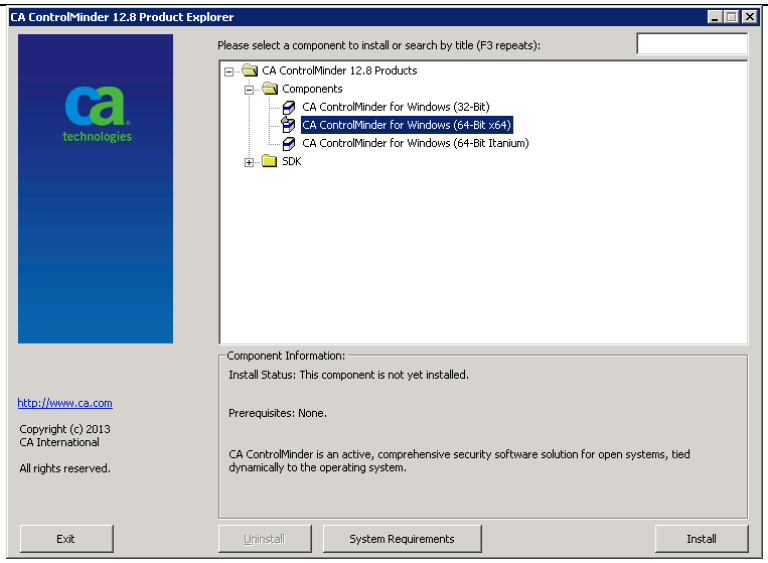
Microsoft Windows Installation

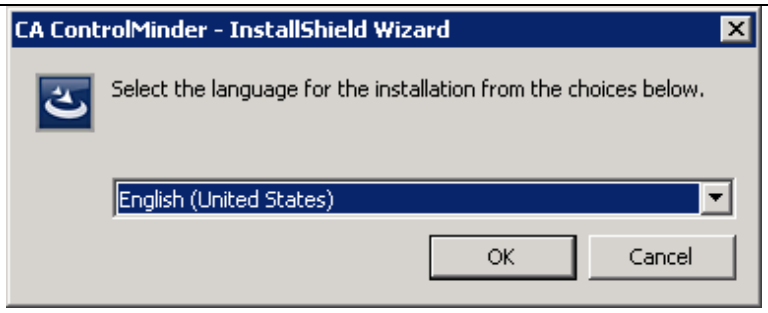
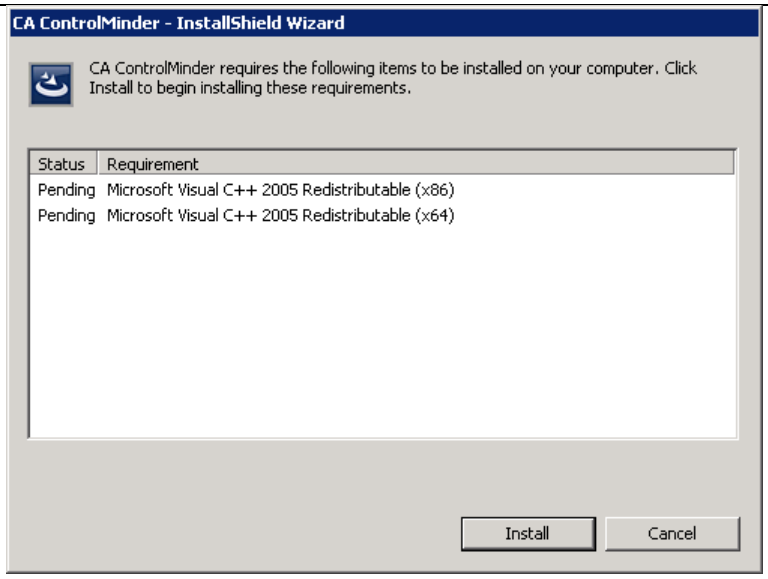
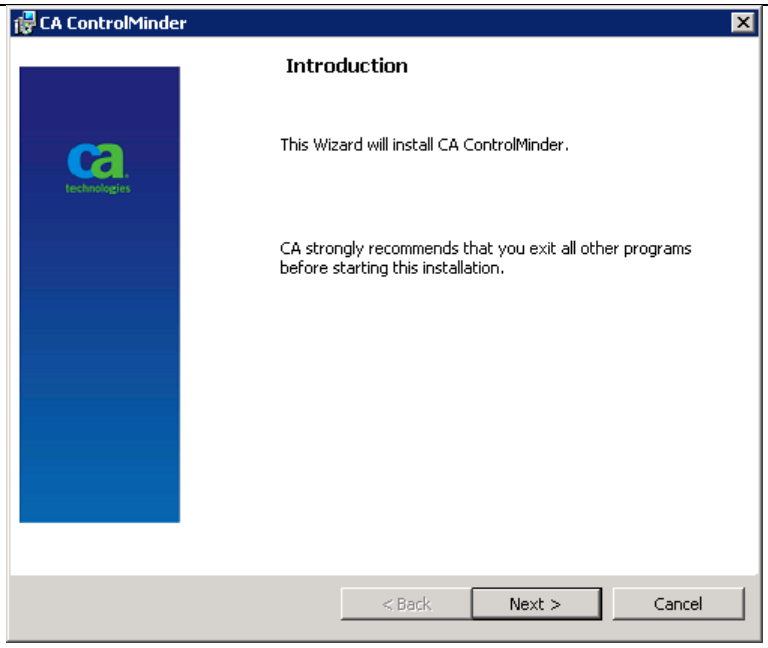
Transfer the CA ControlMinder Endpoint software to the instance.

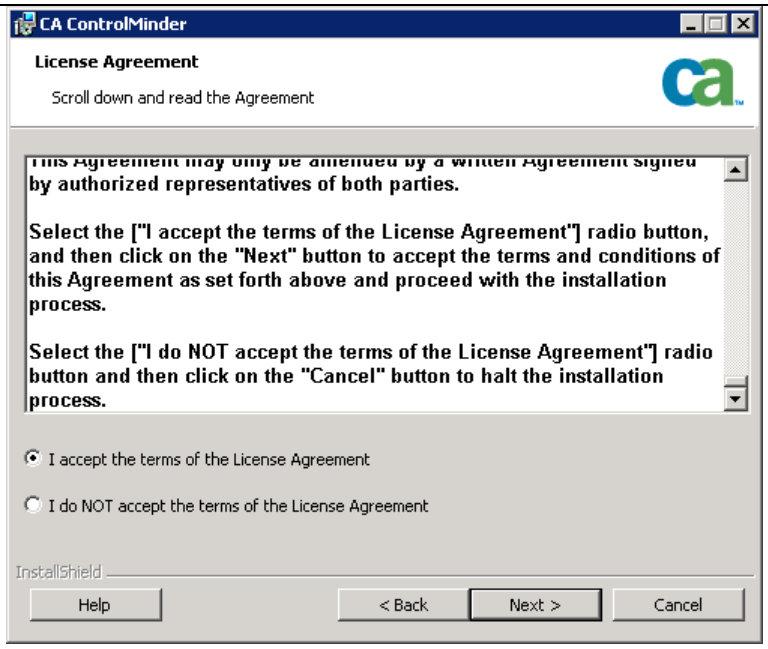
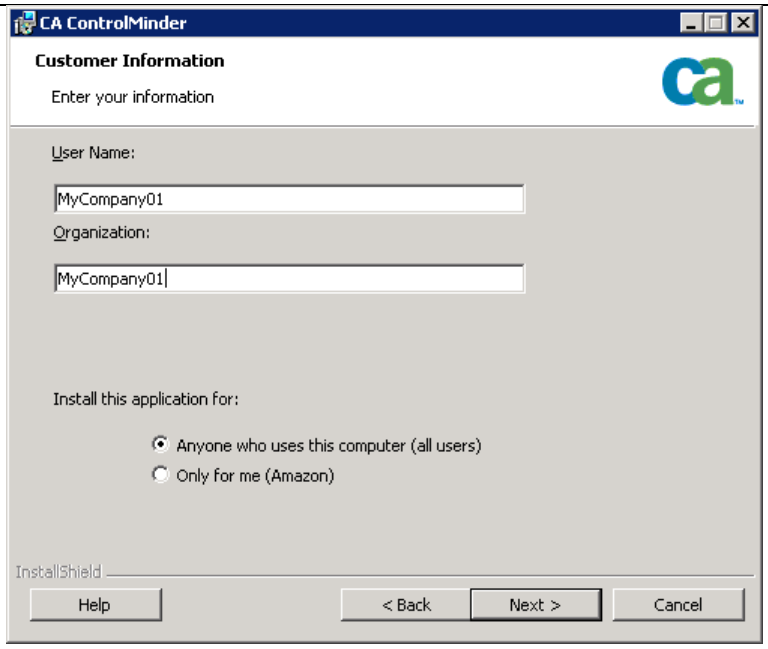
You can either mount the ISO image or extract all of the files from the ISO image.

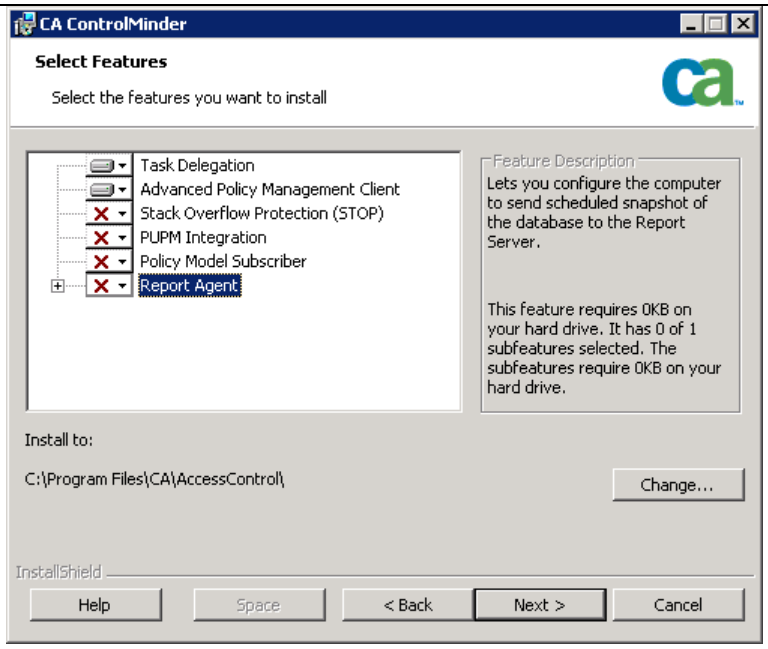
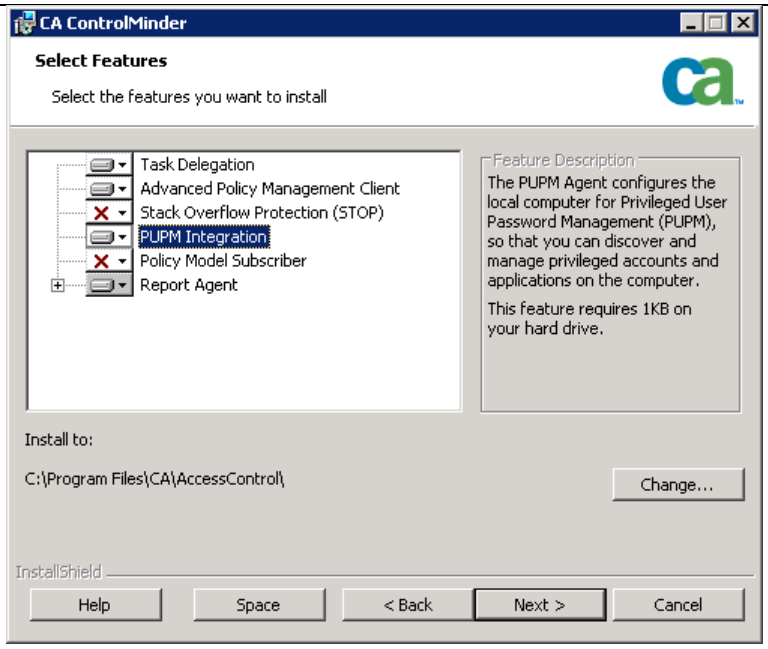
You must be a member of the local Administrators group to perform the installation.

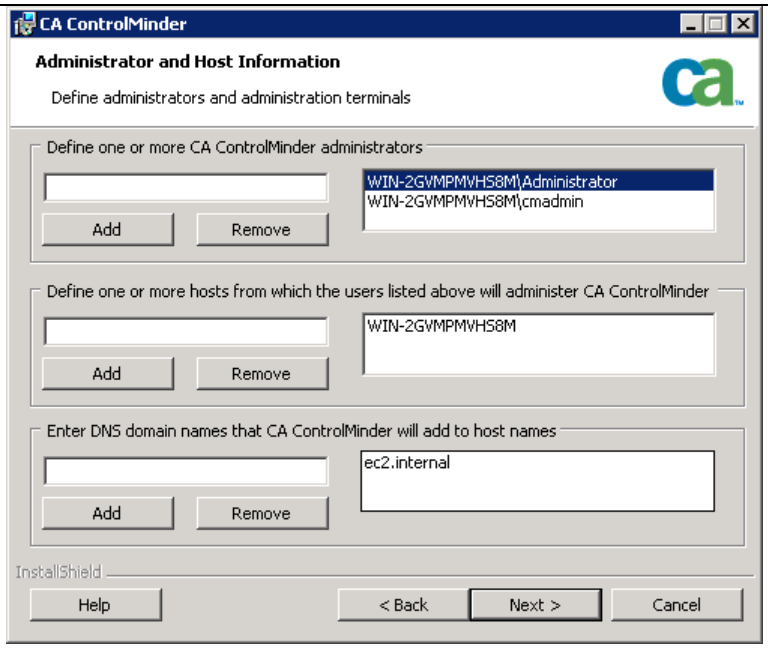
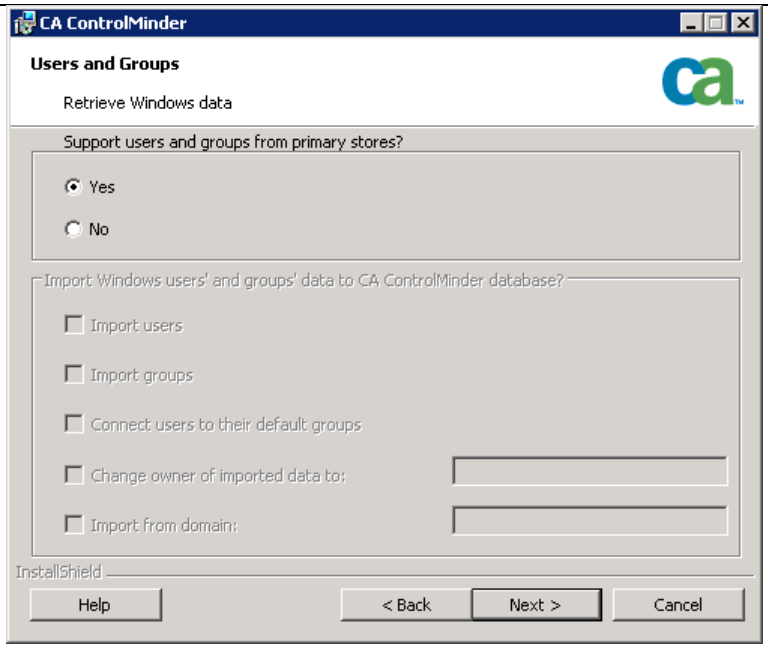
The following example leverages a graphical user interface (GUI) to install the endpoint software. Silent installation is available to facilitate unattended installation. Refer to the Implementation Guide for additional information.

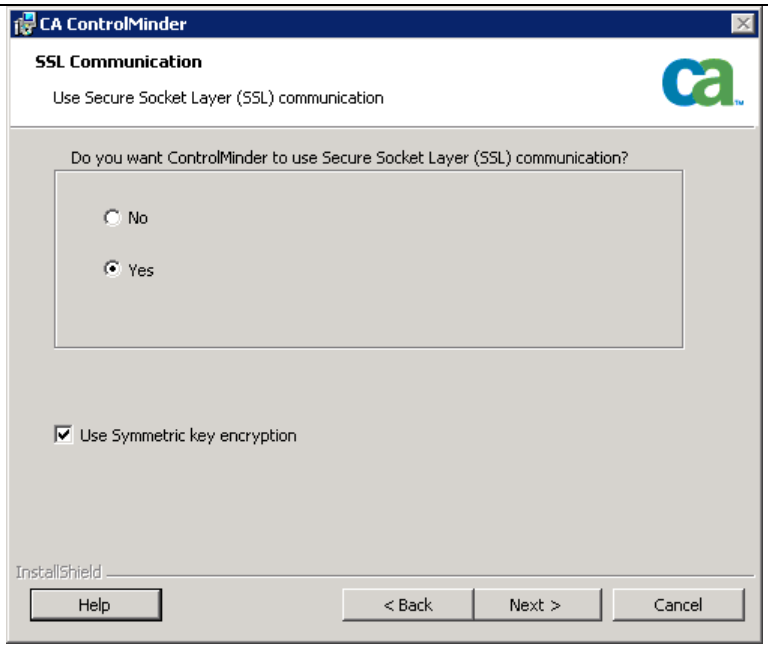
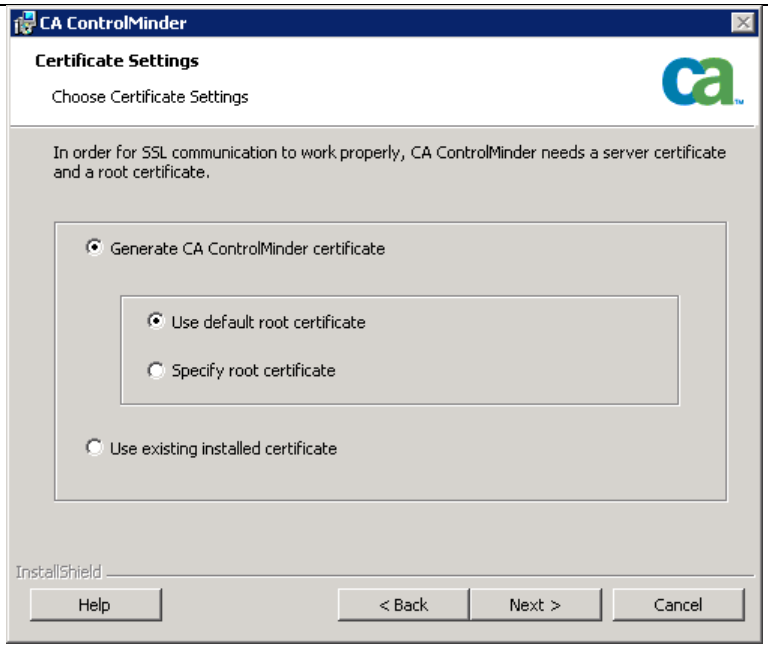
Locate the PRODUCTEXPLORERX86.EXE executable. Right-click the executable and choose Run as administrator to start the installation.	
This example assumes that the endpoint is a 64-bit Intel/AMD architecture. From the Components folder of the Product Explorer, select CA ControlMinder for Windows (64-Bit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

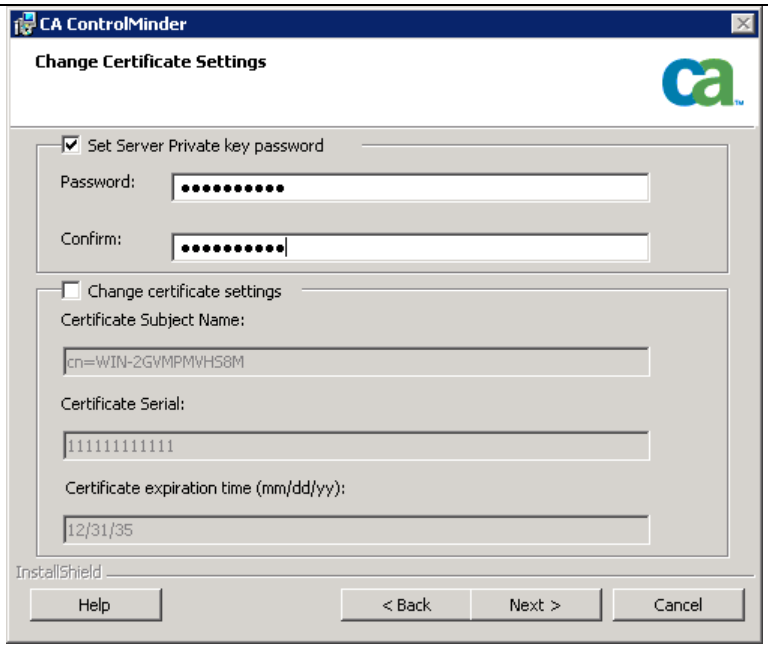
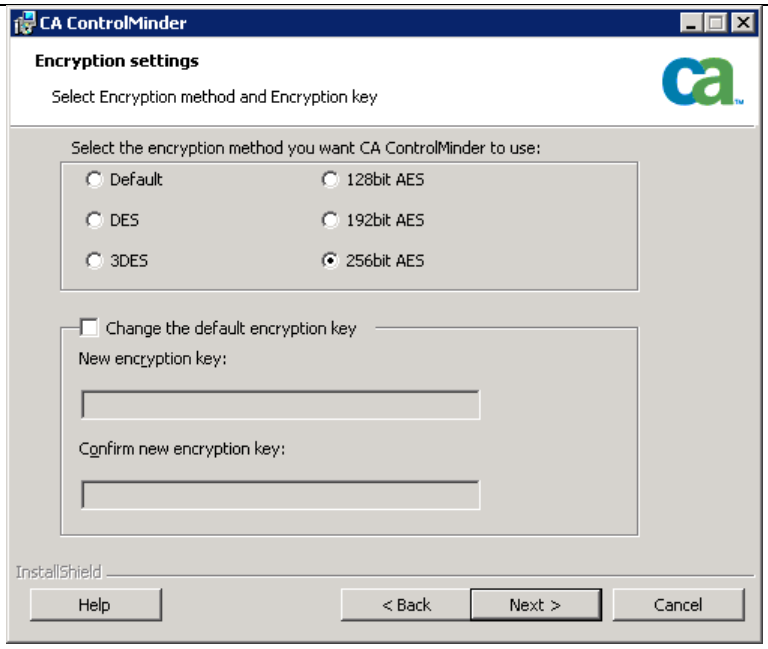
Select the language for the installation and click the OK button.	
If prompted to install Microsoft Visual C++ Redistributable libraries, click the Install button.	
Click the Next button to proceed with the ControlMinder endpoint software installation.	

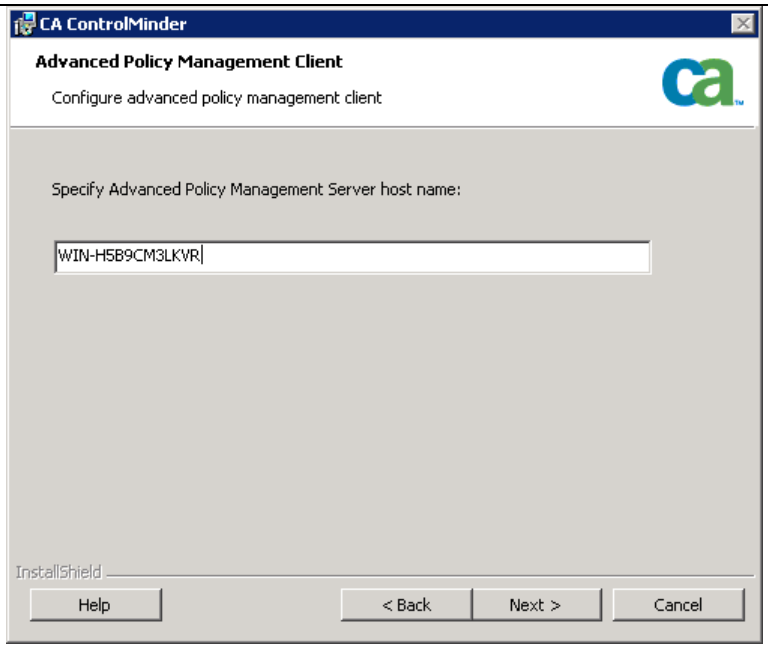
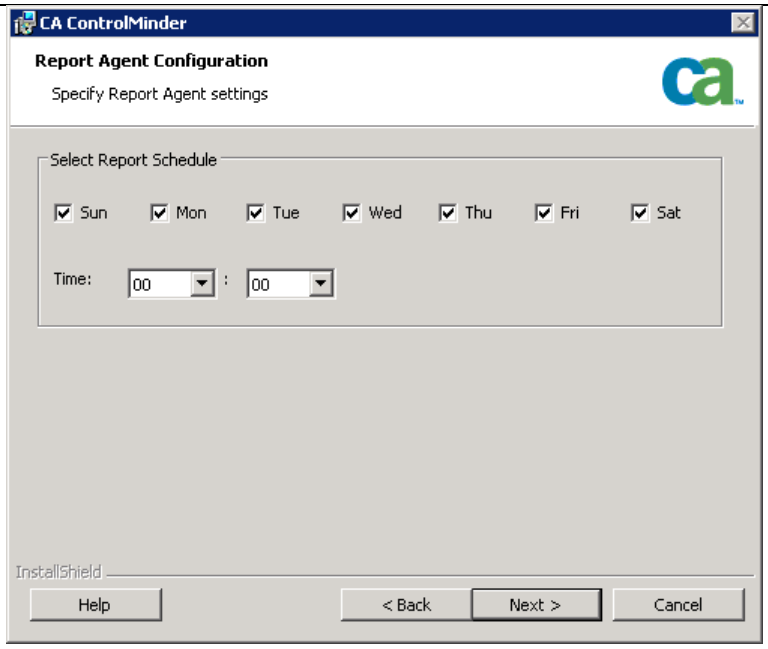
Read the License Agreement as you use the scrollbar to advance through the document. Click the radial button noting I accept the terms of the License Agreement. Click the Next button.	
Provide customer information. Click the Next button.	

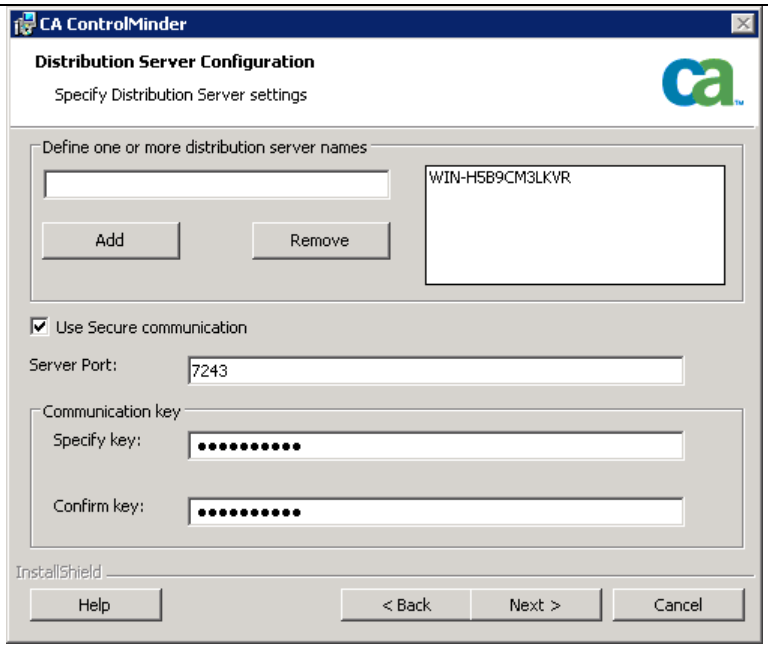
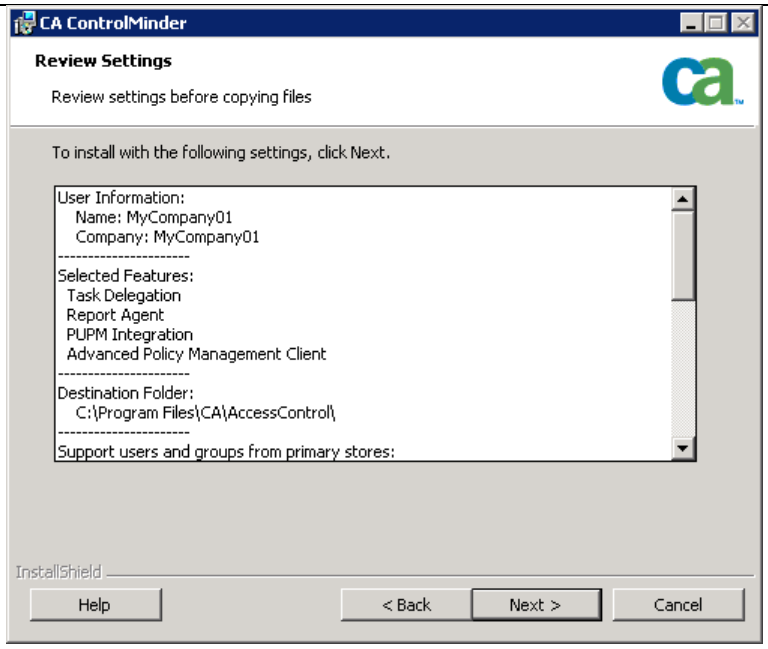
Select the installation directory and the components to be installed. Add “PUPM Integration” and “Report Agent” out of those no selected by default. Click the Next button.	
If you do not plan to use ControlMinder reporting functionality and audit event collection, do not install the Report Agent component. Click the Next button.	

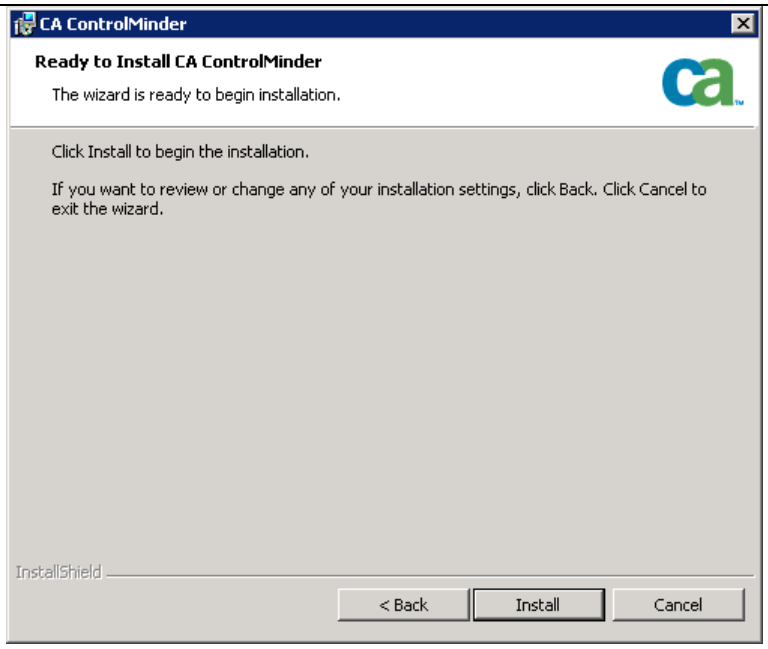
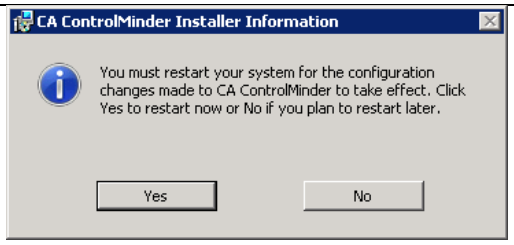
Provide the names of the ControlMinder administrators. Identify the servers from which the ControlMinder administrators are allowed to manage the endpoint. Typically, this is the endpoint itself and possibly the Distribution Server and/or the ENTM Server. For the latter Security Group and/or firewall rules may be required. The user installing ControlMinder is added by default as a ControlMinder administrator. **DO NOT REMOVE THIS USER; otherwise the installation will fail! This user can be removed after the installation has completed.** In the example screenshot, Administrator was added by default as the installer, and cmadmin was manually added. Provide DNS domain names to add to the hostname when identifying the endpoint. Click the Next button.	
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. Click the Next button.	

Click the radial button for Yes to use Secure Socket Layer (SSL) communication. Leave the Use Symmetric key encryption checkbox checked. Click the Next button.	
Specify the certificate to use for SSL communication. The example in the screenshot uses a default root certificate to create a self-signed certificate. A consideration is whether or not to use a certificate generated by the Certificate Authority employed by your organization. Click the Next button.	

Provide the password of the certificate's private key. Click the Next button.	
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. 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.	

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

Specify the Distribution Server that the endpoint will use for Message Queue (Tibco) communication. Use the same hostname as specified for Advanced Policy Management. Provide the communication password that was specified during the installation of Enterprise Management. Click the Next button.	
Review the installation parameters and click the Next button.	

Click the Install button.	
After the installation has completed, click the Finish button.	
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.	

Ubuntu Installation

We will be installing on an Ubuntu machine in the public subnet. Follow the details in the appendix if you need step by step for connection to the Ubuntu machine.

Transfer the installation packages to a read/write directory on you Ubuntu instance.

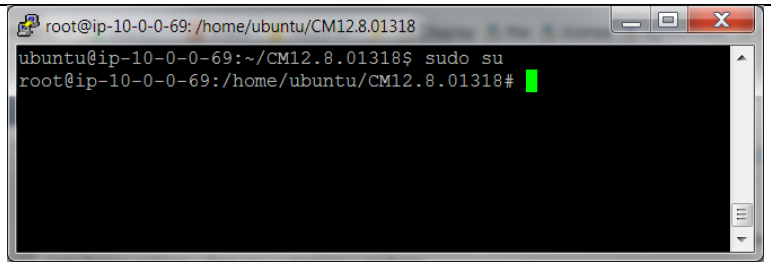
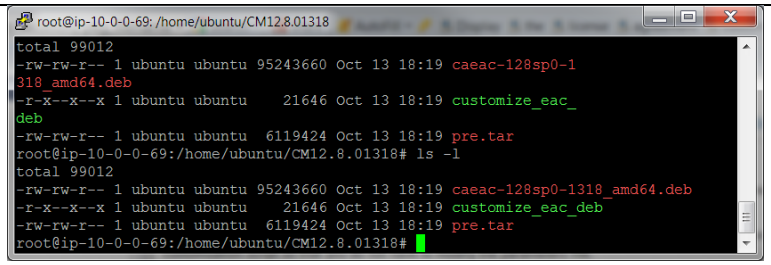
You need the following files from the CA ControlMinder UNIX Endpoint installation DVD:

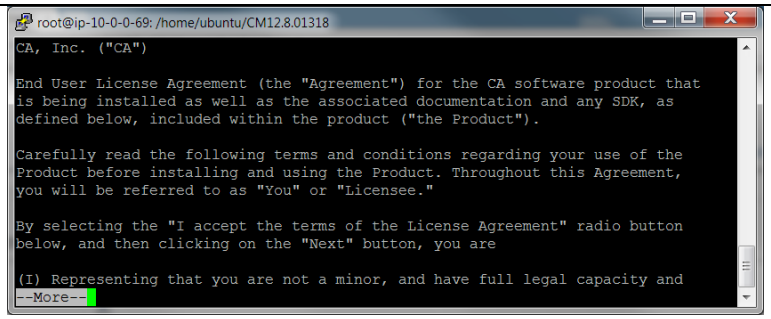
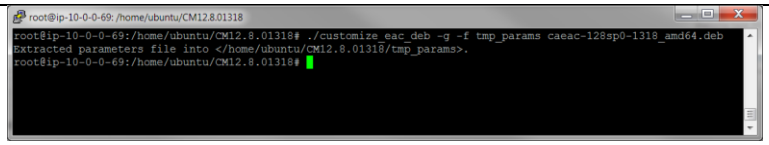
- caeac-xxxspx-xxx_amd64.deb
- customize_eac_deb
- pre.tar

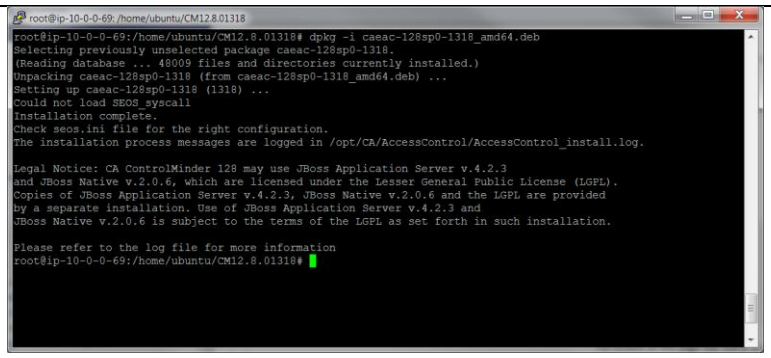
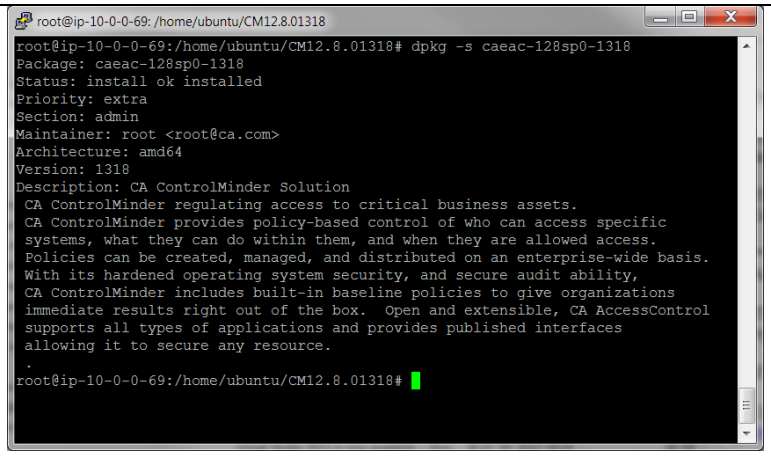
These are usually located under NativePackages\RPMPackages\DEBIAN directory.

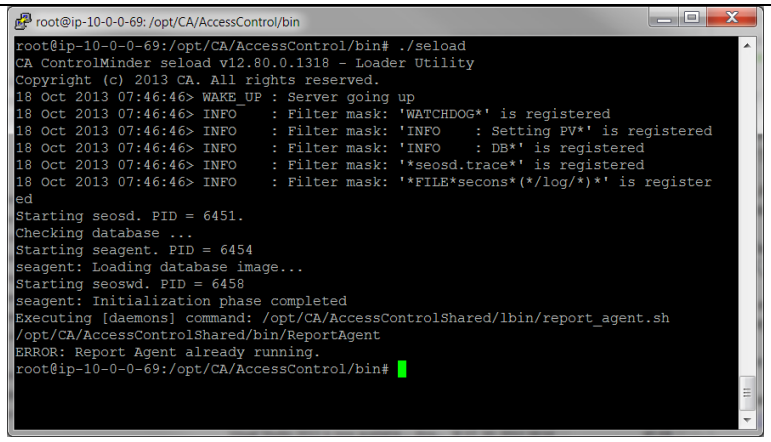
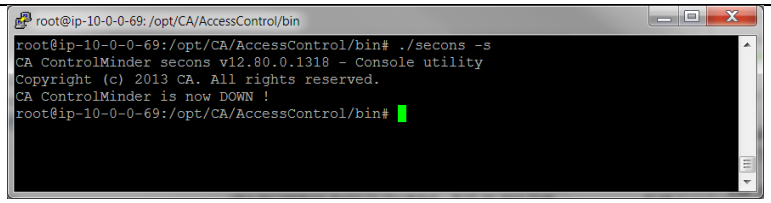
Before you can install CA ControlMinder using a native package, you must customize the CA ControlMinder package to specify that you accept the license agreement. You can also specify custom installation settings when you customize the package.

You customize a package by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

Change your identity to root by running: sudo su	
Change to the directory where the installation package is located. Make sure that customize_eac_deb is executable.	

Run: customize_eac_deb -a pkg_filename to display the license agreement. Take note of the keyword that appears at the end of the license agreement inside square brackets. You specify this keyword in the next step.		
Get the installation parameters file and save it as tmp_params by running: customize_eac_deb -g -f tmp_params pkg_filename		
Open the tmp_params file for editing and customize the parameters.	LIC_CMD=	Provide the keyword you extracted earlier noting that you accept the license agreement.
	ADMIN_USERS=”root,ubuntu”	Specifies the the root and ubuntu users are ControlMinder administrators of the endpoint.
	ENCRYPTION_METHOD_SET=3	Specifies that both SSL encryption and Symmectric key encryption are enabled.
	DH_NAME=”Distribution_Server_Hostname”	Hostname of the Distribution Server that manages the endpoint. NOTE: the endpoint must be able to resolve this hostname.
	DIST_SRV_HOST=”Distribution_Server_Hostname”	Use the same value as assigned to DH_NAME.
	INSTALL_RA=”yes”	Install the Report Agent for collecting endpoint snapshots and optionally to collect audit events.
	REPORT_SHARED_SECRET=My Secret	This is the communication password specified when Enterprise Management was installed. Report Agent uses it to communicate to the Message Queue.
	ENABLE_ELM=”no”	Determines whether or not audit events are collected. Set to “no”

		unless a UAR server is implemented.
	INSTALL_PUPM="yes"	Installs the PUPM Agent.
Save your customized settings in installation package. customize_eac_deb -s -f tmp_params pkg_filename The package will be updated with the customized settings.		
Install the CA ControlMinder package: dpkg -i caeac-xxxspx-xxx_amd64.deb The package is installed into the /opt/CA/ directory by default. The installation directory can be modified in the parameter file.		
Verify that the package status is "OK installed". dpkg -s caeac-xxxspx-xxx		

Start the endpoint software. Navigate to the bin directory under ControlMinder home. It is /opt/CA/AccessControl/bin in our case. Run the following command to start the endpoint SW: ./seload	
You can use: ./secons –s to stop the endpoint software.	

To configure the endpoint software for automatic startup

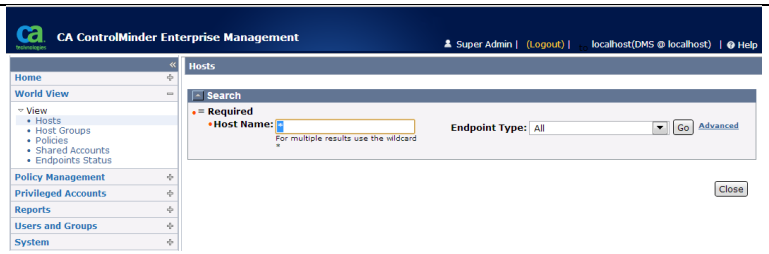
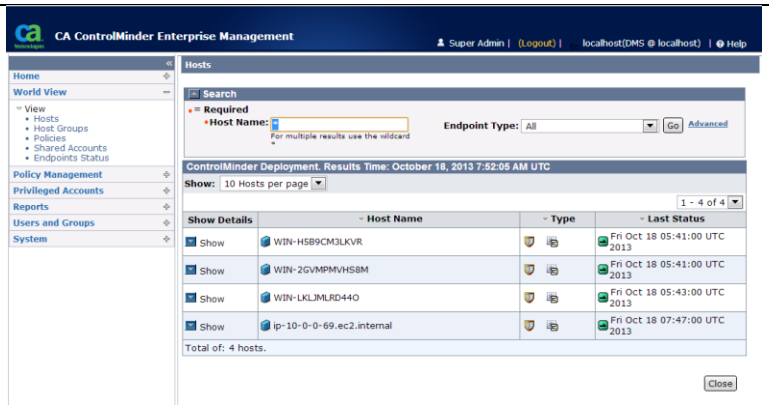
Navigate to:

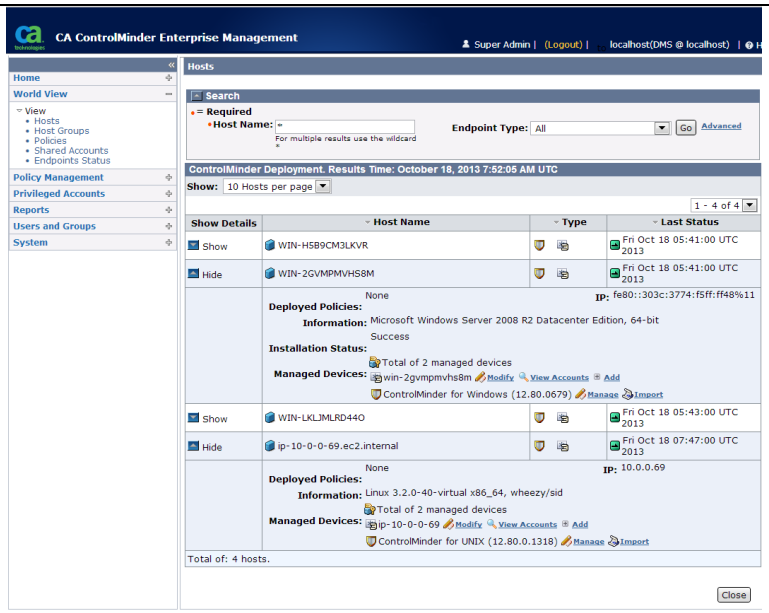
opt/CA/AccessControl/samples/system.init/LINUX

This directory contains a sample script that can be used to start CA ControlMinder at system startup time.

Follow the instructions in the README file found in the same directory.

Validate Endpoint Installation

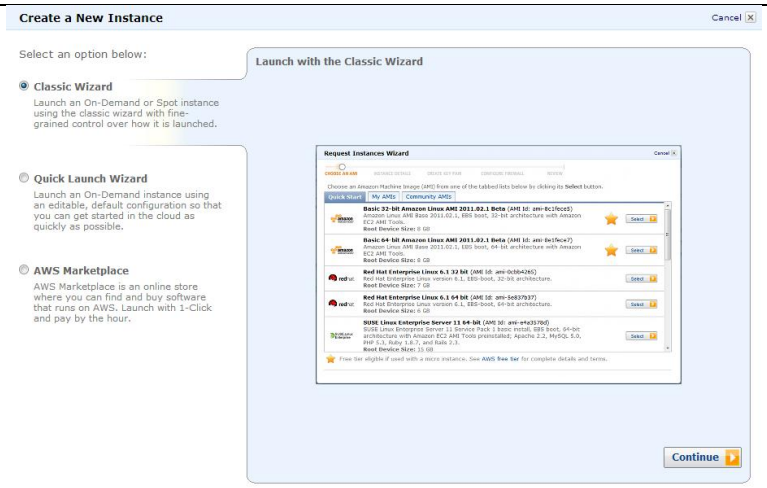
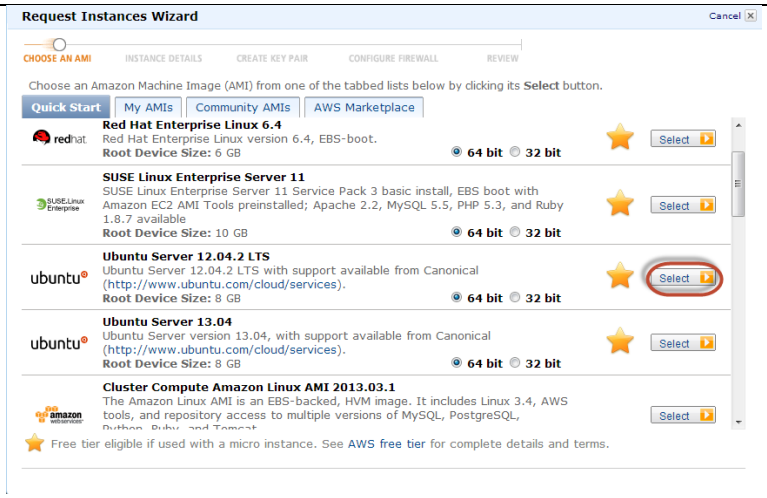
Login to Enterprise Management using the superadmin account. NOTE: The superadmin account's password was specified when Enterprise Management was installed.	
Navigate to World View -> View -> Hosts	
Click Go to display the list of registered endpoints Observe that the ENTM Server, Distribution Server, and Windows and Ubuntu endpoints (on which ControlMinder endpoint software was installed) are listed.	

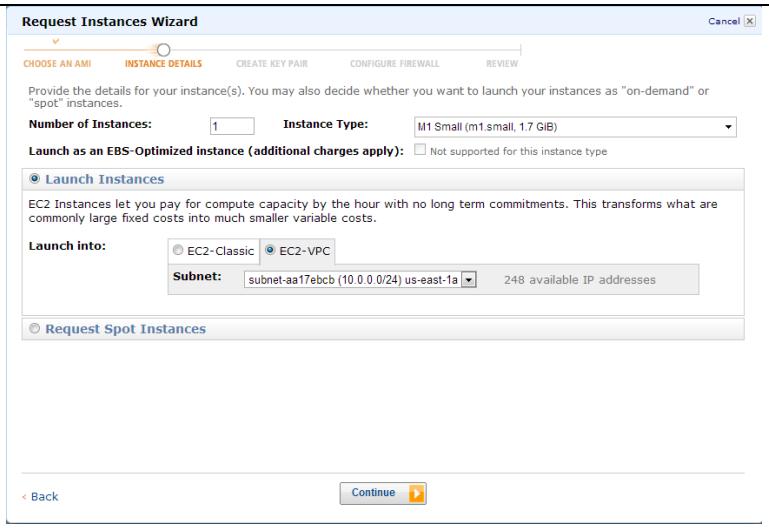
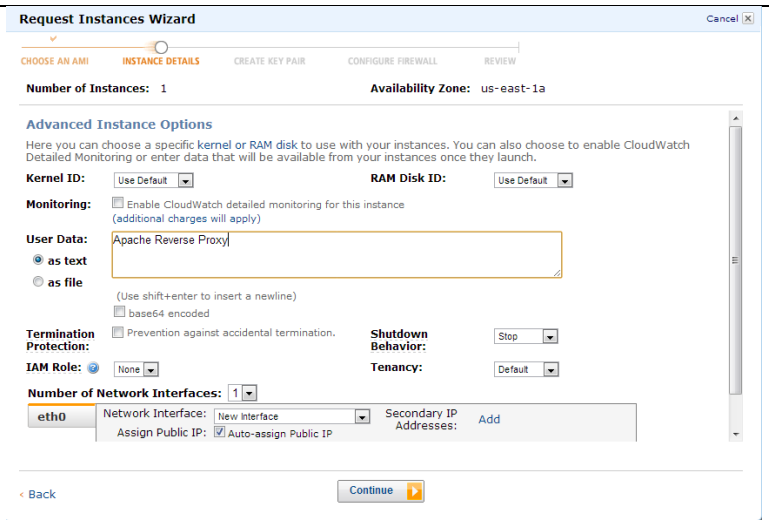
Expand the Windows and Ubuntu endpoints. You should see 2 managed devices per endpoint: • Shared Account Management • ControlMinder for Windows/UNIX This indicates that your endpoints were registered successfully.	

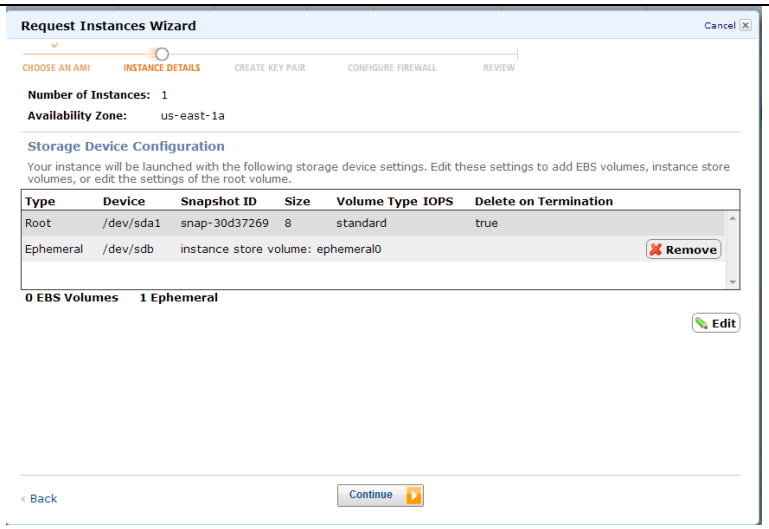
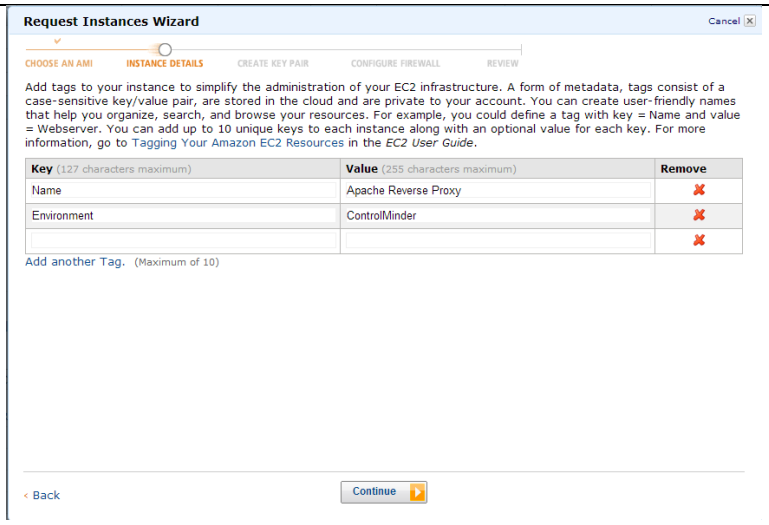
Appendix A – Configure Apache Reverse Proxy Server

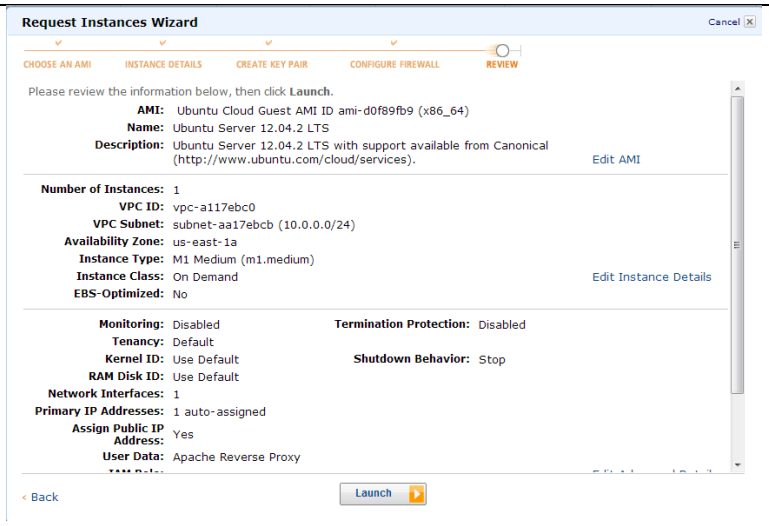
Apache Reverse Proxy is only needed in case Amazon Elastic Load Balancing is not used!
The reverse proxy will allow HTTP/HTTPS traffic from the internet to the ENTM Server running in the private zone.

Deploy Ubuntu Instance

Use the Classic Wizard to launch an Ubuntu instance.	
Scroll through the Quick Start list of Amazon Machine Images (AMIs) and select a 64-bit Ubuntu Server.	

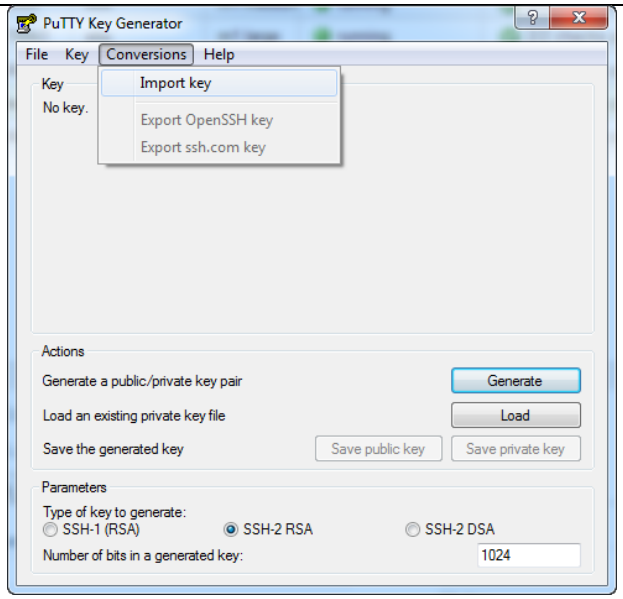
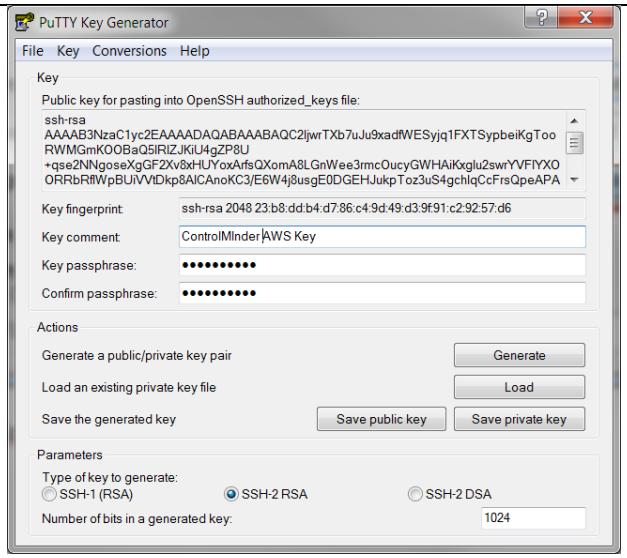
Set Instance Type to M1 Small. For the Launch into information, select the radial button for EC2-VPC and set the subnet to the public subnet (10.0.0.0/24). Click the Continue button.	
Provide User Data to identify your instance. Ensure the Auto-assign Public IP checkbox is checked. Click the Continue button.	

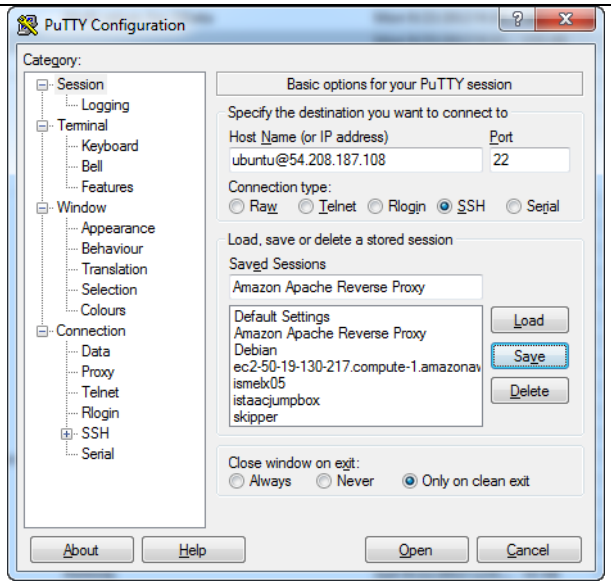
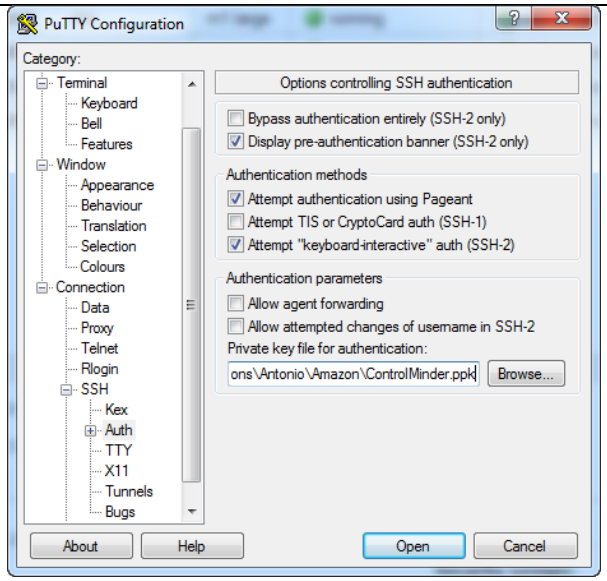
Keep the default storage configuration. 8 gigabytes of disk storage is sufficient for the Apache Reverse Proxy Server. Click the Continue button.	
Name your instance and provide any additional tags as required. Click the Continue button.	

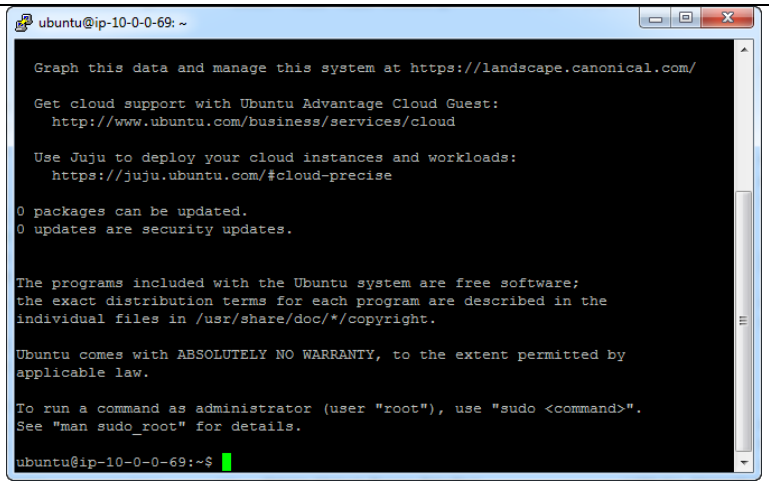
Use the key pair associated you're your AWS ECS Account. Click the Continue button.	
Add Default_Public and RDP_SSH and Web_Access security group to this instance	
Click the Launch button.	

Click the Close button.	

Connect to the Apache Reverse Proxy Server

Start a Remote Desktop session to the JumpBox Server logging in as Administrator.	Follow instructions already described.
Download PuTTy the JumpBox Server	
Install PuTTy on the JumpBox Server	Specific instructions are not provided since this is a straight forward installation.
The following steps describe how to convert your AWS ECS account certificate to a certificate that can be used by PuTTy to login to your Ubuntu instances. You will convert the ControlMinder.PEM Key Pair into the PPK format used by PuTTy. Run PuTTYKeyGen. From the Conversions menu item, choose Import Key.	
Make your AWS ECS account certificate available. In the examples throughout this document, the key pair file is named ControlMinder.pem. Choose the ControlMinder.pem key pair file to import. Create and confirm a key passphrase. Remember this passphrase because you must provide it each time you login to the Apache Reverse Proxy Server. Click the Save private key button and the file as ControlMinder.ppk.	

Run PuTTY. Set Host Name to: ubuntu@<apache host name> where <apache host name> is either the hostname or the IP address of the Apache Reverse Proxy Server. The JumpBox must be able to resolve the hostname if hostname is used. Under Saved Sessions, name the session Amazon Apache Reverse Proxy. Click the Save button to save the session.	
Under Category, select Connection → SSH → Auth Specify the path to ControlMinder.ppk in <u>Private key file for authentication</u> <u>Under Category, select Session and save the session again.</u> <u>Click the Open button.</u>	

When prompted, provide the passphrase associated with the private key. A PuTTy session will be started with the Apache Reverse Proxy Server as the ubuntu user.	

Install Apache 2.0

Install Apache Reverse Proxy Server.

Execute the following commands:

- sudo apt-get update
- sudo apt-get install apache2

ubuntu@ip-10-0-0-69: /

```
Setting up apache2.2-common (2.2.22-1ubuntu1.4) ...
Enabling site default.
Enabling module alias.
Enabling module autoindex.
Enabling module dir.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module status.
Enabling module auth_basic.
Enabling module deflate.
Enabling module authz_default.
Enabling module authz_user.
Enabling module authz_groupfile.
Enabling module authn_file.
Enabling module authz_host.
Enabling module reqtimeout.
Setting up apache2-mpm-worker (2.2.22-1ubuntu1.4) ...
 * Starting web server apache2                                          [ OK ]
Setting up apache2 (2.2.22-1ubuntu1.4) ...
Setting up ssl-cert (1.0.28ubuntu0.1) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
```

Enable SSL by running:

- sudo a2enmod ssl
- sudo a2ensite default-ssl

root@ip-10-0-0-69: /etc/apache2/sites-available

```
root@ip-10-0-0-69:/etc/apache2/sites-available# sudo a2enmod ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and
 create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
root@ip-10-0-0-69:/etc/apache2/sites-available# service apache2 restart
 * Restarting web server apache2
 ... waiting                                                           [ OK ]
root@ip-10-0-0-69:/etc/apache2/sites-available# sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
root@ip-10-0-0-69:/etc/apache2/sites-available#
```

Run the following commands to enable Reverse Proxy:

- sudo ln –s /etc/apache2/mods-available/proxy.load /etc/apache2/mods-enabled
- sudo ln –s /etc/apache2/mods-available/proxy_http.load /etc/apache2/mods-enabled

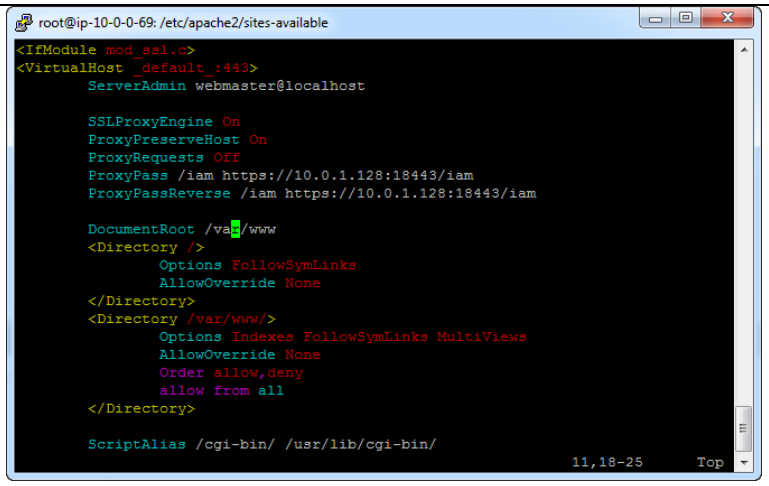
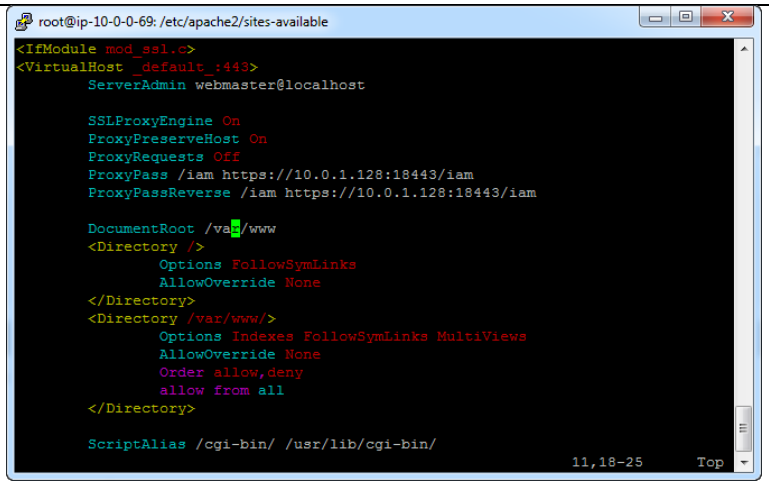
ubuntu@ip-10-0-0-69: /etc/apache2/sites-available

```
<VirtualHost *:80>
        ServerAdmin webmaster@localhost

        ProxyPreserveHost On
        ProxyRequests     Off
        ProxyPass /iam http://10.0.1.128:18080/iam
        ProxyPassReverse /iam http://10.0.1.128:18080/iam


        DocumentRoot /var/www
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
                                                        8,0-1         Top
```

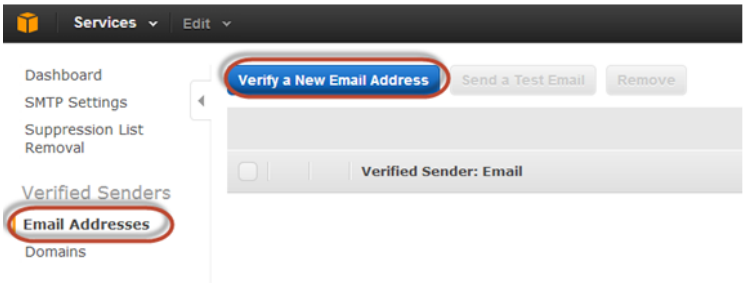
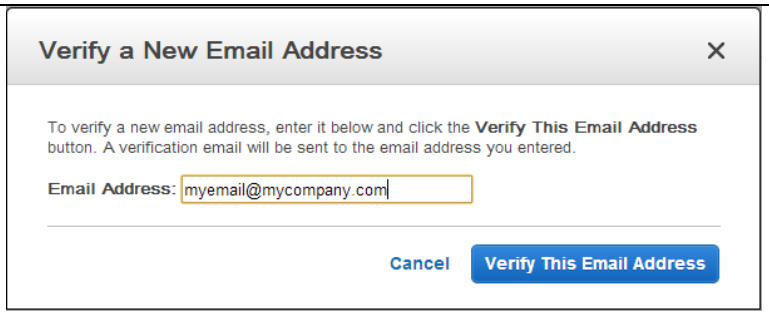
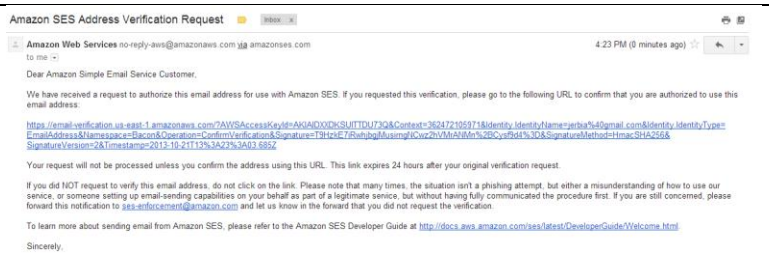
Modify the reverse proxy settings: sudo vi /etc/apache2/sites-available/default Add the following lines: ProxyPreserveHost On ProxyRequests Off ProxyPass / http://<ENTM private IP>:18080/iam ProxyPassReverse / http://<ENTM Private IP>:18080/iam	
sudo vi /etc/apache2/sites-available/default-ssl Add the following lines: SSLProxyEngine On ProxyPreserveHost On ProxyRequests Off ProxyPass / https://<ENTM private IP>:18443/iam ProxyPassReverse / https://<ENTM Private IP>:18443/iam	
Execute the following command to restart Apache: • service apache2 restart	

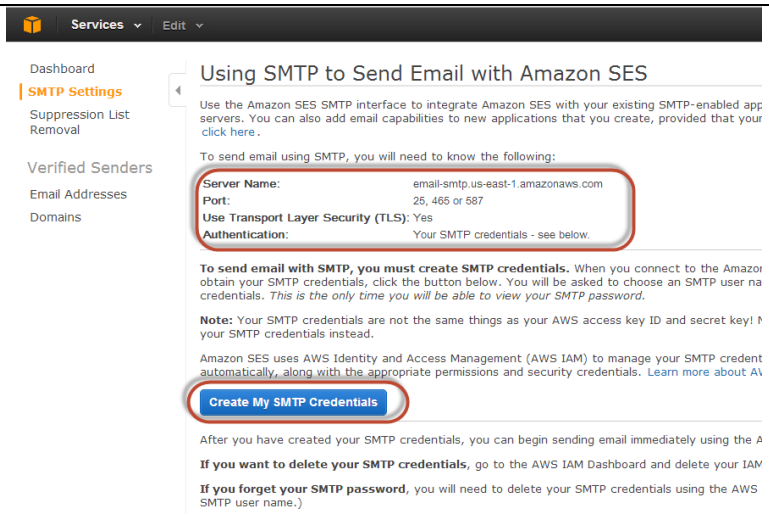
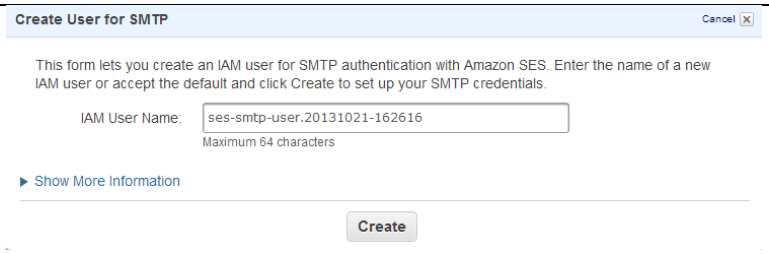
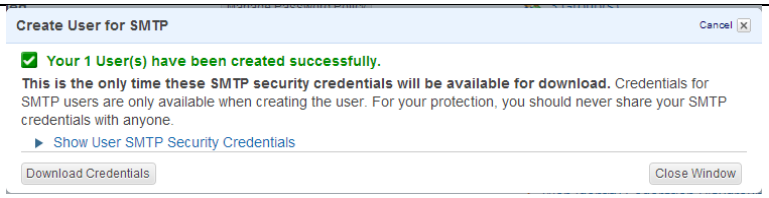
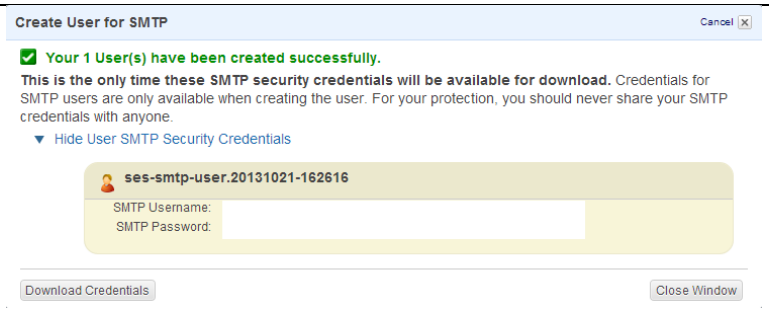
Appendix B - Setup email notification using Amazon SES

You can use Amazon SES (Simple Email Service) for CA ControlMinder workflow notification.

You can either use the default “sandbox” access or request a production access from Amazon.

Create E-Mail Sandbox

Go to Amazon AWS console. Choose the SES Service to enable Amazon Email Service.	
You must register the email address of each sender and each recipient when using “sandbox” access. Click the Email Addresses button. Click the Verify a New Email Address button.	
Specify the email address you will be using.	
A verification email is sent to the email address. The recipient must click on the link within this email.	

Capture the SMTP settings from the SMTP Settings menu. Click the Create My SMTP Credentials button.	
Specify a user name or accept the default. Click the Create button.	
Click on the Show Security Credentials.	
Copy the SMTP user name and password	

Configure Email Workflow Notification

CA ControlMinder Enterprise Management can send email notifications when a specific event occurs.

Email notifications inform CA ControlMinder Enterprise Management users of events in the system, and are generated from email templates. If you enable email notifications, CA ControlMinder Enterprise Management can generate email notifications when one of the following occurs:

- An event that requires approval or rejection is pending.
- An approver approves an event.
- An approver rejects an event.
- An event starts, fails, or completes.
- A CA ControlMinder Enterprise Management user is created or modified.

It is a best practice to enable email notifications for events related to approval workflows.

The two most common events of interest include:

BreakGlassCheckOutAccountEvent

- A notification will be sent to the approver when a Break Glass action is performed on a privileged account.

CreatePrivilegedAccountExceptionNotStartedEvent

- A notification will be send to the approver that a request is pending in his worklist for and access to a privileged account.
- Notifications will be sent to the requestor when the request is approved, rejected or completed.

It is also possible to have a notification for “CheckOutAccountPasswordEvent” if you require a notification to be received every time a password is checked out.

There is also CreatePrivilegedAccountExceptionEvent that represents the availability of the requested account for usage. Once this event is completed the account is available for the user to be checked out and checked in. If you want to enable notification for this event you must edit the corresponding template in the “completed” folder.

To configure email notification settings follow these steps:

Start a Remote Desktop session with the ENTM server and login as Administrator.

Stop the JBoss service from the Services panel.

Open the mail-service.xml file. By default, the file is located in the following directory:

<JBoss_HOME>/server/default/deploy

Locate the User and Password attributes and change to the values you obtained from Amazon SES.

```
<attribute name="User">MySMTPUser</attribute>
<attribute name="Password">MySMTPPassword</attribute>
```

Add the following properties to the file to enable SMTP authentication and TLS security.

```
<property name="mail.smtp.auth" value="true"/>
<property name="mail.smtp.starttls.enable" value="true"/>
```

If you are using some other SMTP service that does not require authentication you can skip the above steps.

Locate the following entry in the file:

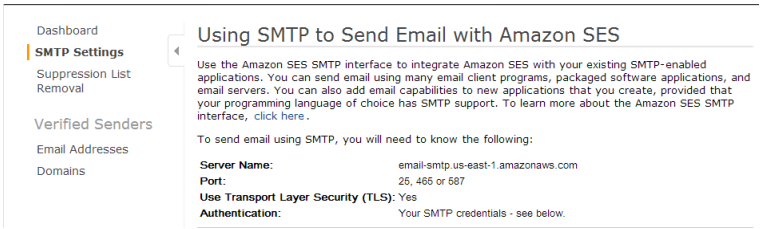
```
<property name="mail.smtp.host" value="smtp.nosuchhost.nosuchdomain.com"/>
```

Change the smtp.nosuchhost.nosuchdomain.com value to the full DNS domain name of the outgoing email server host. For example:

```
<property name="mail.smtp.host" value="email-smtp.us-east-1.amazonaws.com"/>
```

Note: The Enterprise Management Server must resolve the IP address of the SMTP server to the full DNS domain name that you specify for this property.

You can find the smtp server settings for Amazon SES if you navigate to SES and then SMTP Settings om Amazon EWS console.



Update the smtp port if required.

```
<property name="mail.smtp.port" value="25"/>
```

Save the changes.

Open the corresponding email templates for the privileged account password request CreatePrivilegedAccountExceptionNotStartedEvent.tmpl file in the following directories:

JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/approved

JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/cancelled

JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/pending

JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/rejected

Change the URL from “http://localhost:8080/iam/ac” to the URL for Enterprise Management running on the ENTM_Server. Since we are using the elastic load balancer, use that URL, for example,

https://entm-elastic-lb-1210936808.us-east-1.elb.amazonaws.com/iam/ac

Repeat the above process for the following template:

BreakGlassCheckOutAccountEvent.tmpl found in the directory:

<JBoss_HOME>/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/pending

Ensure that the files are saved.

Open the email.properties file. This file is located in the following directory:

<JBoss_HOME>/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/

Edit the following entry:

```
admin.email.address=IMS
```

Specify the sender email address then save and close the file. For example:

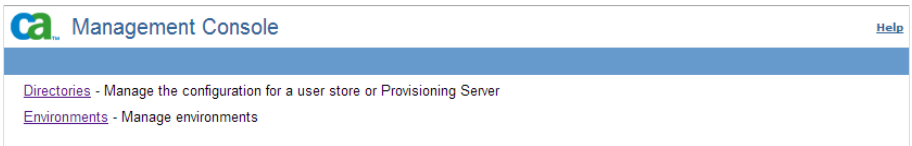
```
admin.email.address= cmadmin@mydomain.com
```

Start JBoss.

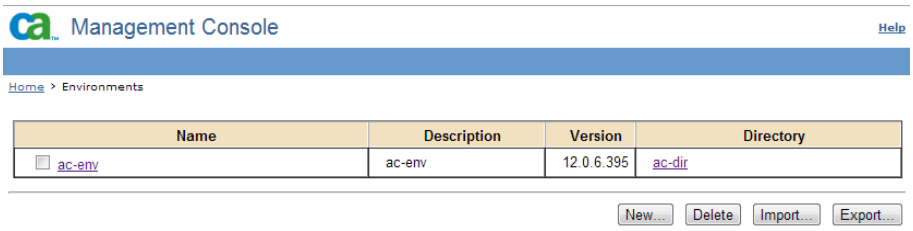
If the CA IdentityMinder Management Console is not enabled, you must enable it before proceeding.

Open the IdentityMinder Management Console by browsing to the following link: https://localhost:18443/idmmanage

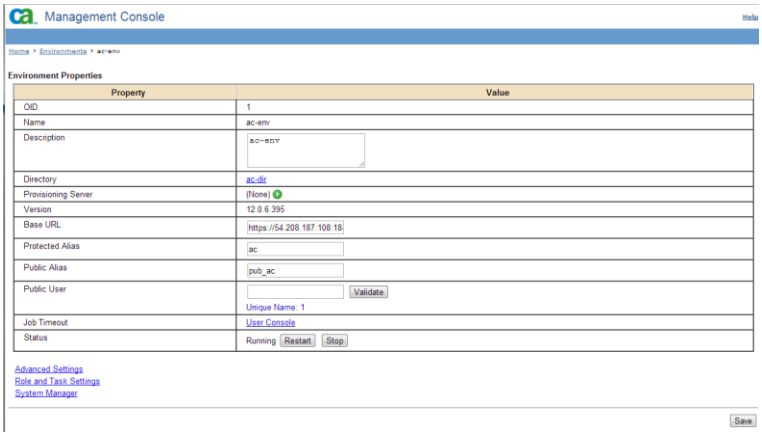
In the CA IdentityMinder™ Management Console, click Environments.



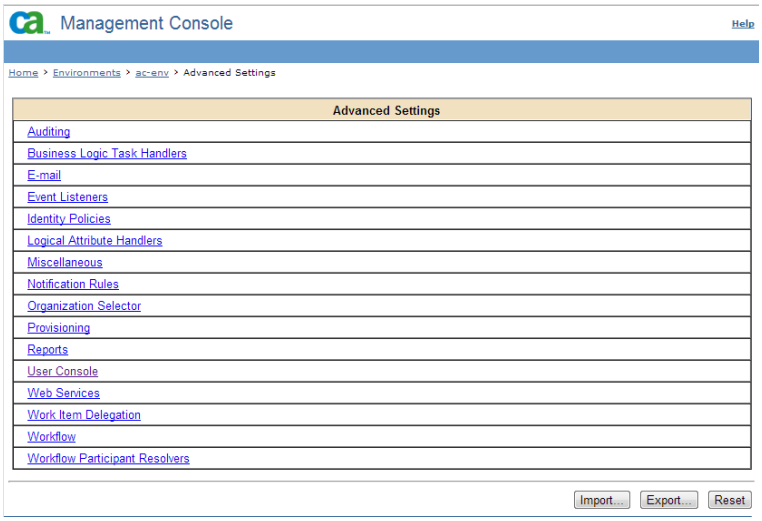
Select ac-env.



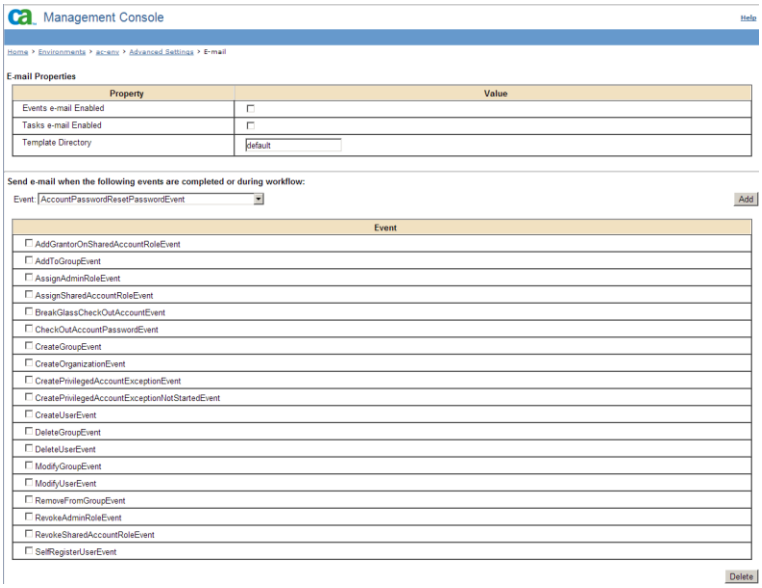
Select Advanced Settings.



Select E-mail.



The E-mail Properties window appears.



Select the check box next to “Events e-mail Enabled”

This enables email notifications for CA ControlMinder Enterprise Management events, including SAM events.

The Template Directory is set to default. Do NOT change this setting.

Note: The email templates are located in the following directory:

<JBoss_Home>/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default

Specify the events for which to send email notifications.

We recommend that you only specify SAM events for email templates that have been provided.

Select the check box next to every event, except the following SAM events:

- BreakGlassCheckOutAccountEvent
- CreatePrivilegedAccountExceptionNotStartedEvent

Click Delete.

Note: You can also keep “CheckOutAccountPasswordEvent” if you want to receive a notification every time a password is checked out.

All other notifications are deleted.

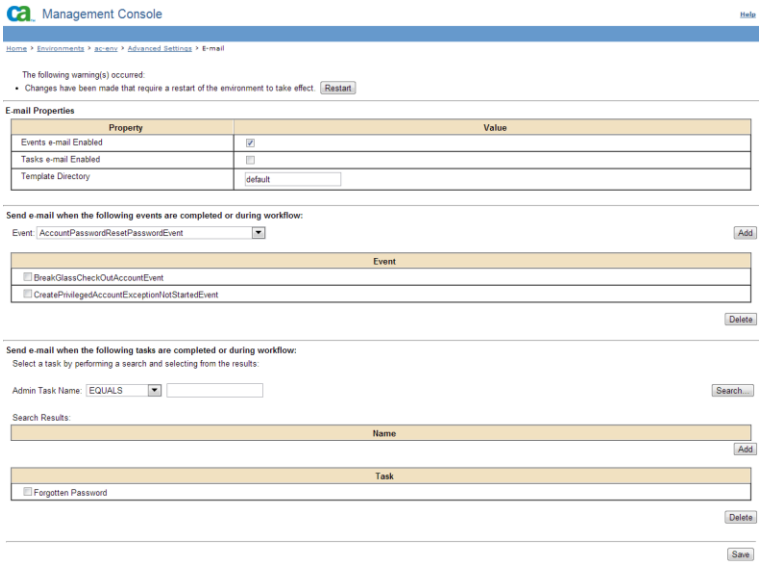
You have configured CA ControlMinder Enterprise Management to send email notifications for the selected SAM events.

Click Save.

The email notification properties are saved.

You are warned that there are changes that require a restart.

Click the Restart button.



The CA IdentityMinder Management Console restarts the environment and applies your changes.

Note: For more information about email notifications, see the Enterprise Administration Guide.