



CA Technologies

# CA ControlMinder™ Rapid Implementation Guide

## Amazon EC2 Deployment

## Contents

References .....	4
CA ControlMinder References .....	4
Tibco References.....	4
Glossary.....	6
Prerequisites .....	8
Introduction .....	8
Solution Highlights .....	9
Instances Summary.....	10
Prerequisites and Getting Started .....	12
Generating a Key Pair.....	12
Creating a Virtual Private Cloud.....	13
Defining Security Groups .....	16
Setting Up a Jump Box .....	20
Connecting to the JumpBox.....	26
Deploying the RDBMS Using Microsoft SQL Server .....	29
Create the Microsoft SQL Server Instance on the private subnet.....	29
Preparing the Database .....	33
Deploying Enterprise Management.....	35
Create ENTM Instance .....	35
Transferring the Software.....	39
From the JumpBox server, copy the software to the ENTM Server. ....	39
ENTM Installation.....	41
Install Third-Party Components .....	42
Install Enterprise Management .....	46
Create Amazon Elastic Load Balancer.....	54
Configure ENTM to Use Amazon Elastic Load Balancer.....	60
Deploying Distribution Server.....	62
Create the Distribution Server Instance .....	62
Prepare to Install the Distribution Server .....	66
Tibco Communication Configuration .....	66
Configure Name Resolution .....	67

Install Third-Party Components .....	69
Install the Distribution Server .....	72
Install ControlMinder Endpoints .....	78
Open Required Communication Ports .....	78
Microsoft Windows Installation .....	79
Ubuntu Installation .....	89
Validate Endpoint Installation .....	93
Appendix A – Configure Apache Reverse Proxy Server .....	95
Deploy Ubuntu Instance .....	95
Connect to the Apache Reverse Proxy Server .....	100
Install Apache 2.0 .....	103
Appendix B - Setup email notification using Amazon SES .....	104
Create E-Mail Sandbox .....	105
Configure Email Workflow Notification .....	107

## References

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

<https://support.ca.com>

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

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

### CA ControlMinder References

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

### Tibco References

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

Copyright ©2013, CA, Inc. All rights reserved. Microsoft, Windows, Windows Server, Active Directory, SQL Server, and Internet Explorer are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. RACF is a registered trademark of International Business Machines Corporation in the United States, other countries, or both. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. UNIX is a registered trademark of The Open Group. EC2 and VPC are registered trademarks of Amazon Services LLC. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

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

## Glossary

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:

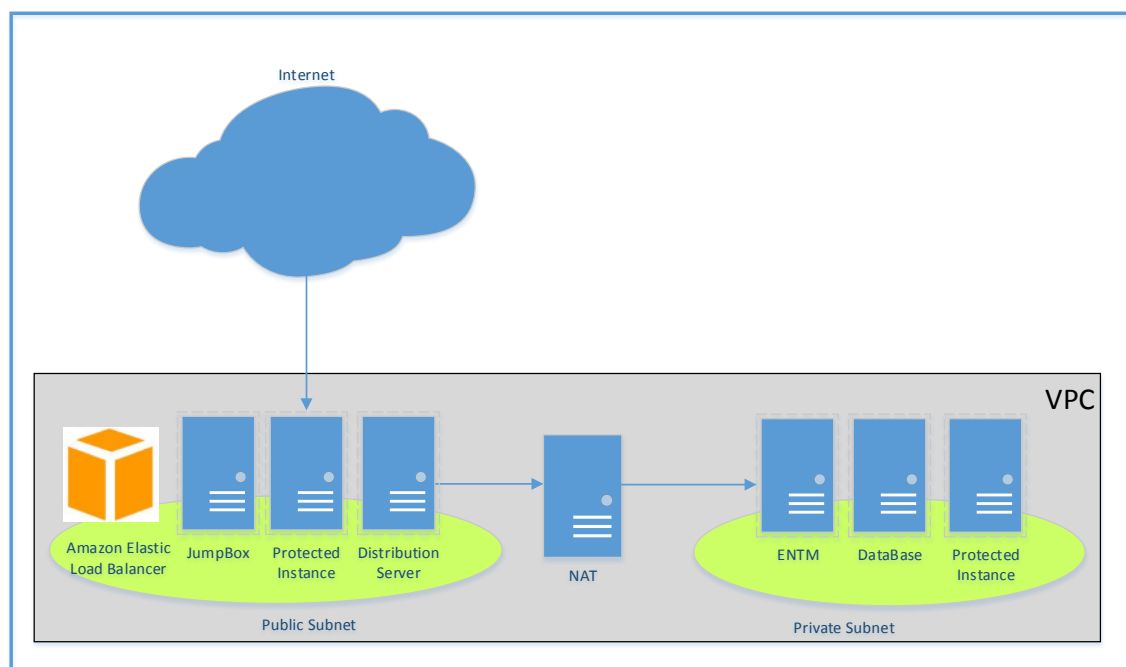
- A web browser to view the documentation in HTML format.
- Adobe® Reader® or any other compatible PDF viewer

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



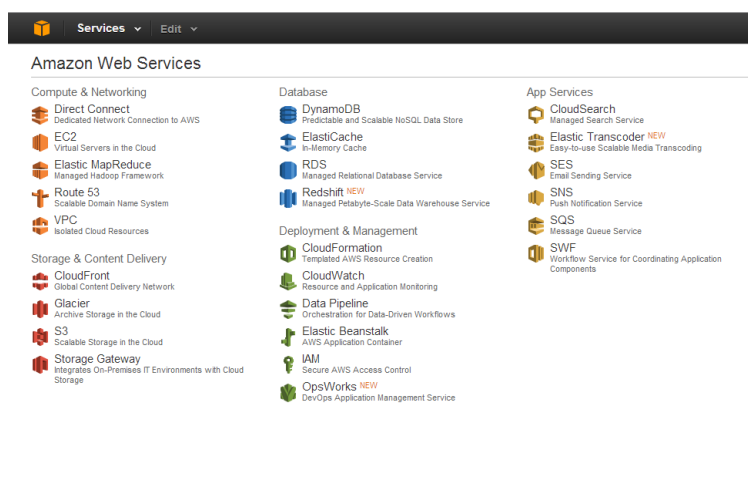
## Prerequisites and Getting Started

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

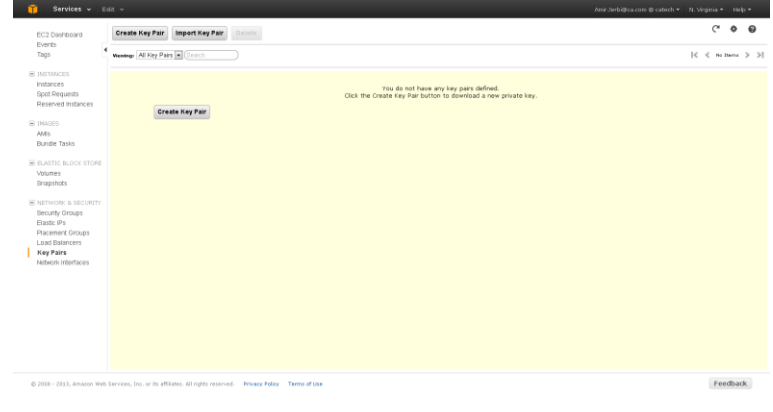

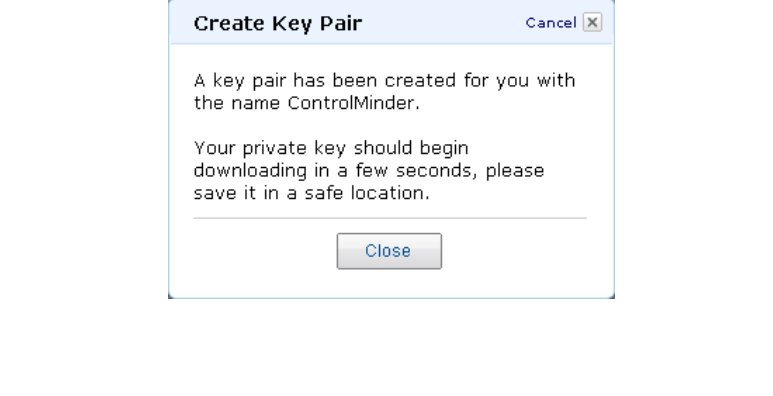
To log in to your instances you must first create a key pair. Specify the name of the key pair when you launch the instance and provide the private key when you connect to the instance.

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.

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Select AWS Services to create a Key Pair.</p>	
<p>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.</p>	
<p>Select Close once the Key Pair has been created.</p> <p>Save the private key file to your local machine and remember the location.</p> <p>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.</p>	

## 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.

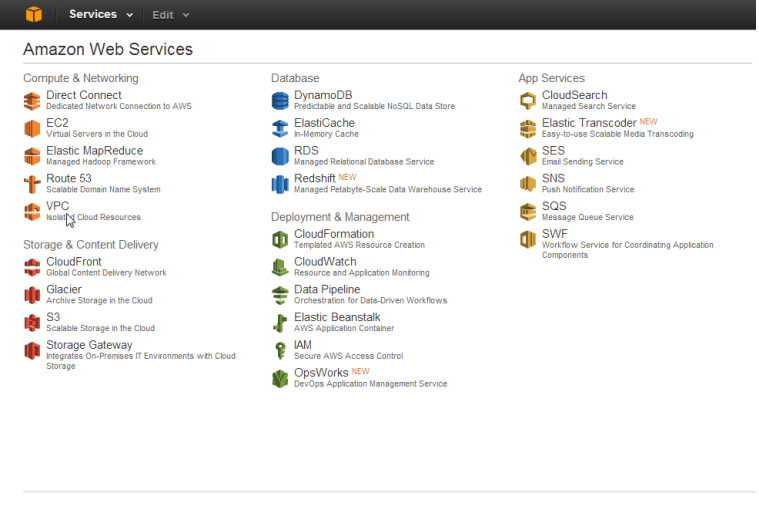
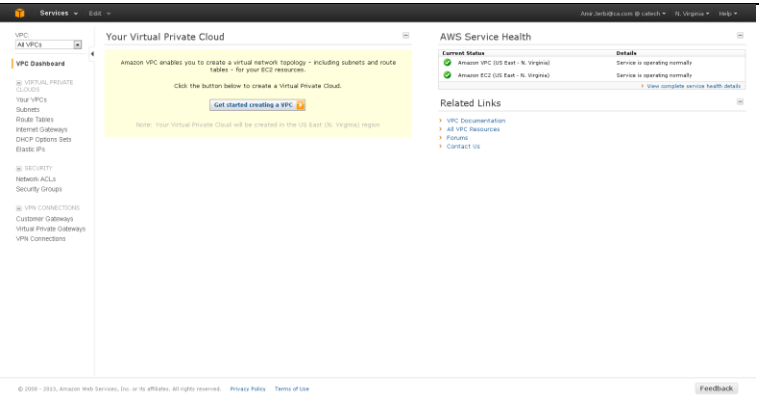
We will create 2 subnets:

- Public subnet
- Private subnet

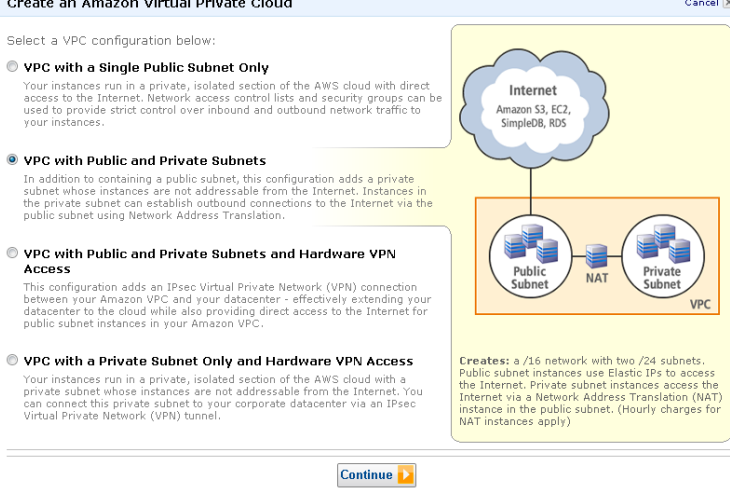
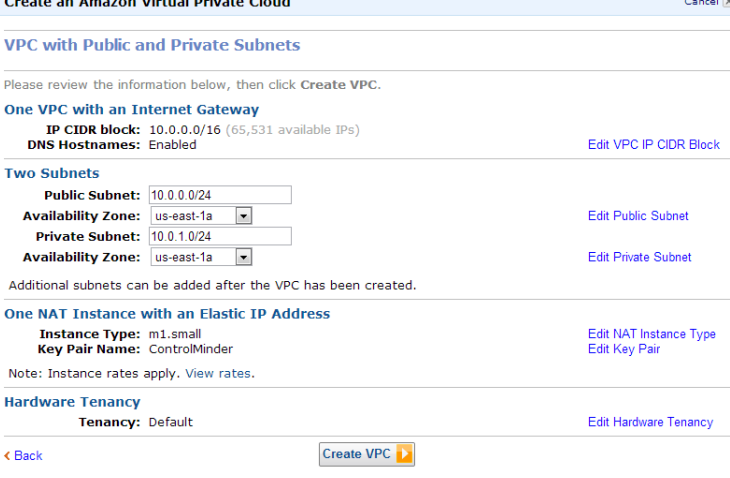
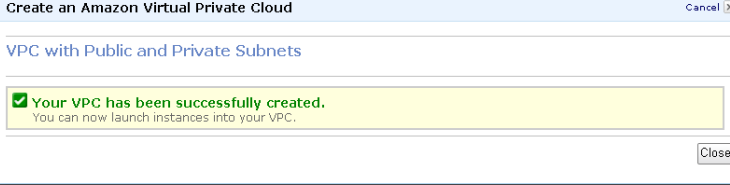
Internet access can be allowed to instances in the public subnet.

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

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

# CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>For this example, “VPC with Public and Private Subnets” was chosen.</p> <p>The ENTM server and the Microsoft SQL server will be isolated on the private subnet.</p> <p>Other instances will be public facing.</p> <p>Choose the type of VPC that meets your needs.</p> <p>Click the Continue button to proceed.</p>	
<p>This VPC has two subnets:</p> <ul style="list-style-type: none"> <li>• a public subnet (10.0.0.0/24)</li> <li>• a private subnet (10.0.1.0/24)</li> </ul> <p>Verify that both subnets are deployed on the same availability zone.</p> <p>Click the <u>Create VPC</u> button.</p>	
<p>You will see confirmation that the VPC was successfully created.</p>	

## 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.

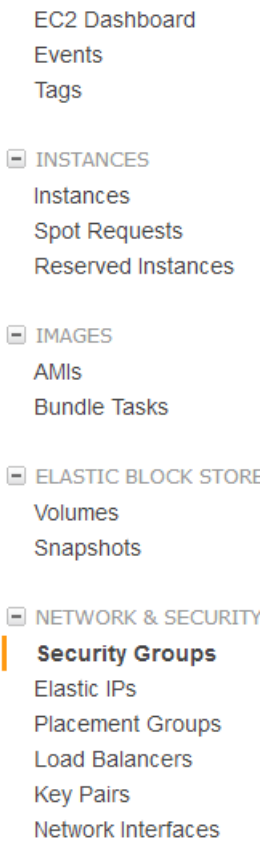
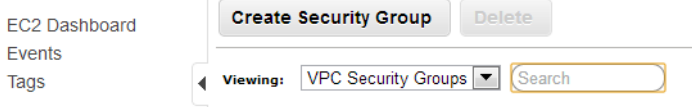
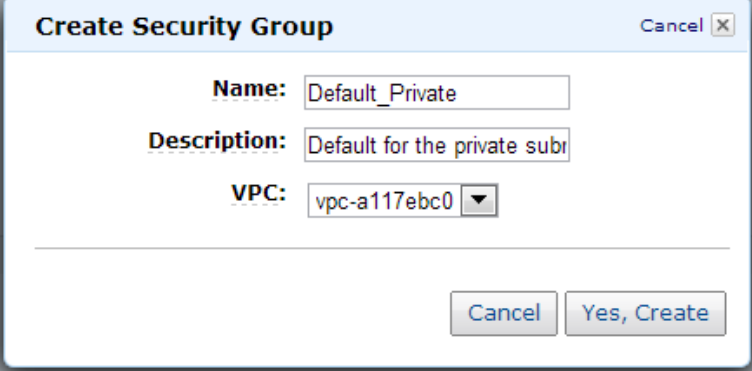
You need to create security groups to open all the necessary ports for implementing and running CA ControlMinder.

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.



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

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..

### 1 Security Group selected

#### Security Group: Default\_Private

Details

Inbound\*

Outbound

Create a new rule:

All Traffic

Source:

sg-56908334

(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

+ Add Rule

Your changes have not been applied yet.

Apply Rule Changes

### 1 Security Group selected

#### Security Group: Default\_Private

Details

Inbound

Outbound

Group Name: Default\_Private

Group ID: sg-56908334

Group Description: Default for the private subnet

VPC ID: vpc-a117ebc0

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”

### 1 Security Group selected

#### Security Group: Default\_Private

Details

Inbound

Outbound

Create a new rule: Custom TCP rule

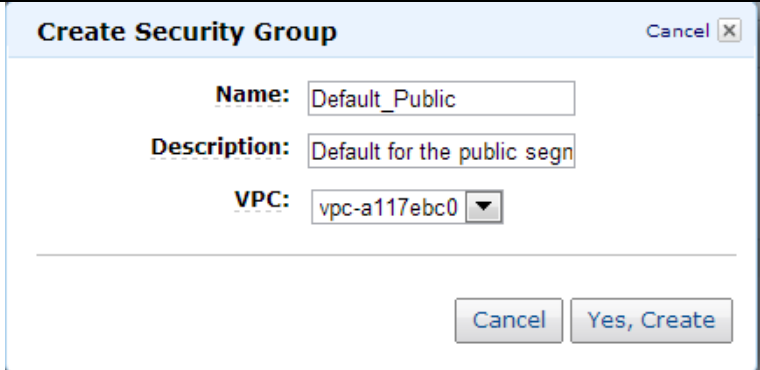
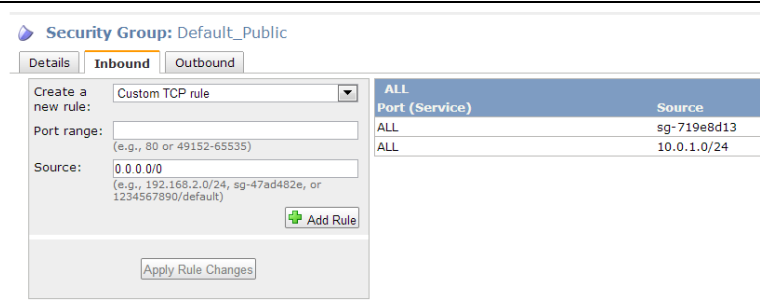
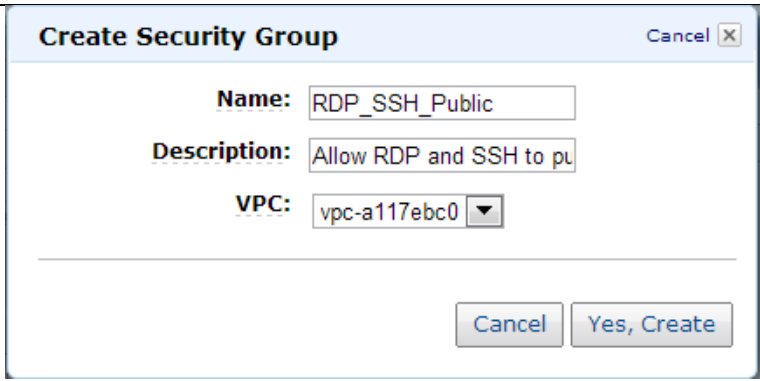
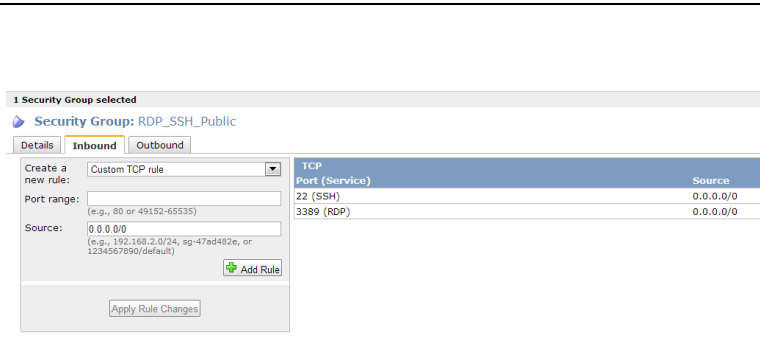
Port range: (e.g., 80 or 49152-65535)

Source: 0.0.0.0 (e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

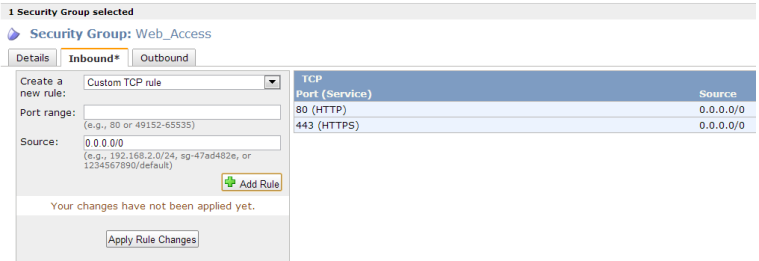
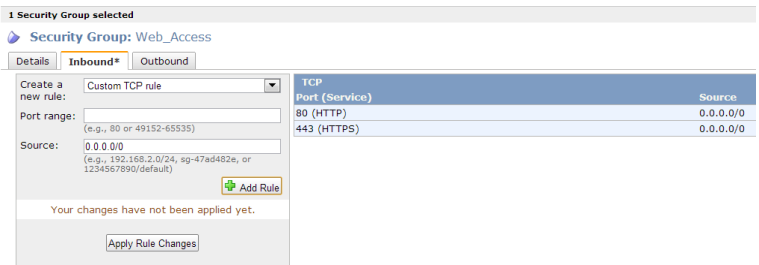
+ Add Rule

Apply Rule Changes

All Port (Service)	Source
ALL	sg-56908334
TCP Port (Service)	Source
3389 (RDP)	10.0.0.0/24
18443	10.0.0.0/24
7243	10.0.0.0/24

<p>Create group Default_Public”</p>	
<p>Add rules that permit access from all members of the public subnet and all members of the private subnet.</p> <p>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).</p>	
<p>Create a Security Group to allow Remote Desktop (RDP) and Secure Shell (SSH) access to group members.</p>	
<p>Add rules to allow members of the public subnet access to members of the private subnet over the following ports:</p> <ul style="list-style-type: none"> <li>Remote Desktop (3389)</li> <li>Secure Shell (22)</li> </ul> <p>This example allows access to group members from the public subnet, the private subnet, and the internet.</p> <p>Limit access further to meet your specific requirements.</p> <p>Click “Apply Rule Changes”</p>	

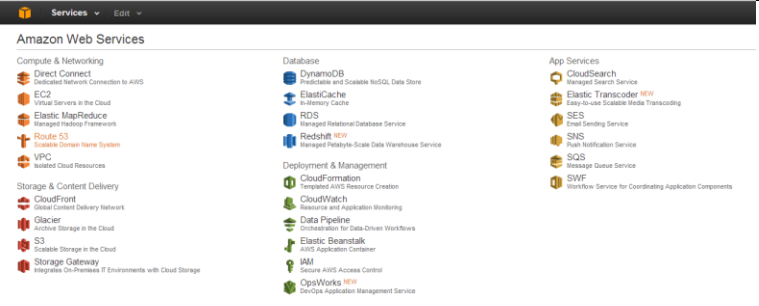
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Create the Web_Access group to allow browser access.</p>	
<p>Allow browser access to the:</p> <ul style="list-style-type: none"> <li>• Default HTTP port (80)</li> <li>• Default HTTPS port (443)</li> </ul> <p>This example allows access to group members from the public subnet, the private subnet, and the internet.</p> <p>Limit access further to meet your specific requirements.</p>	

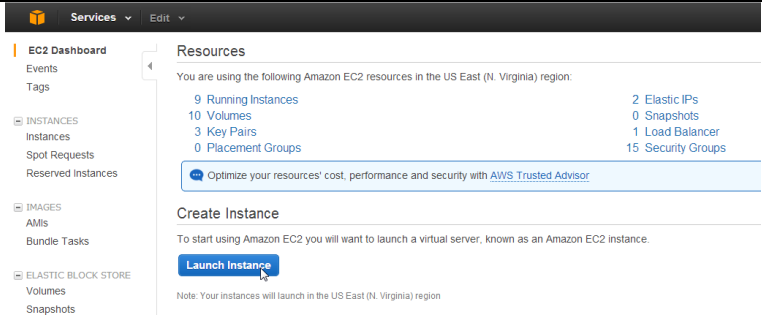
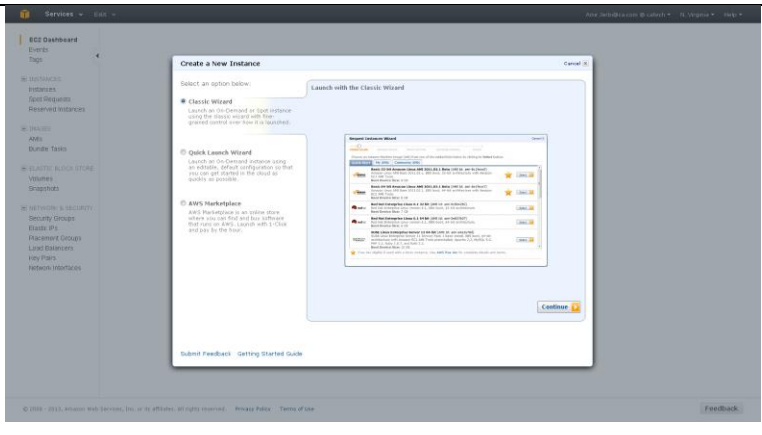
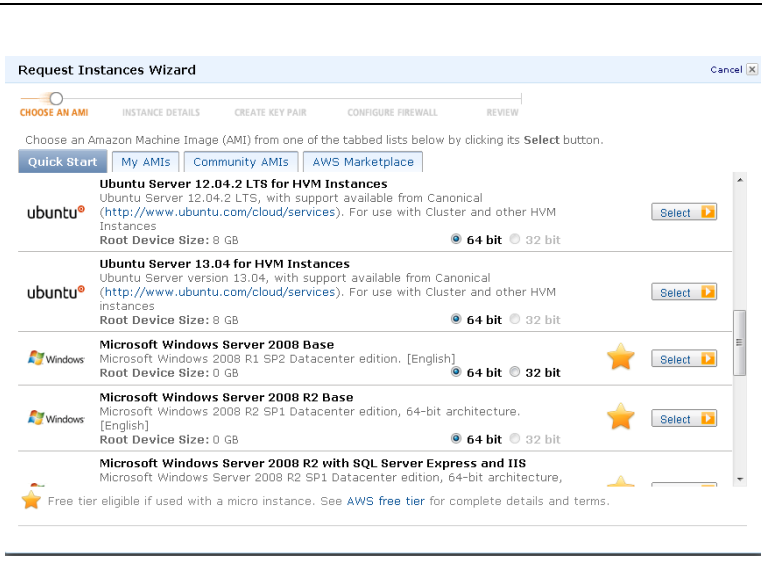
## Setting Up a Jump Box

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.

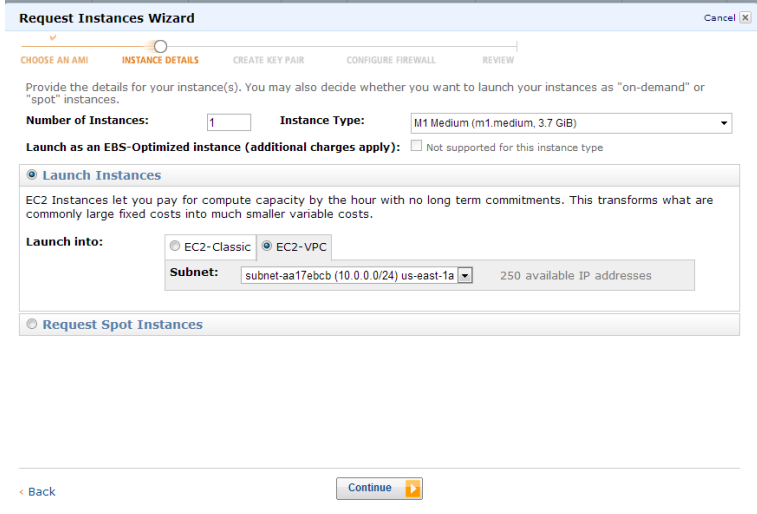
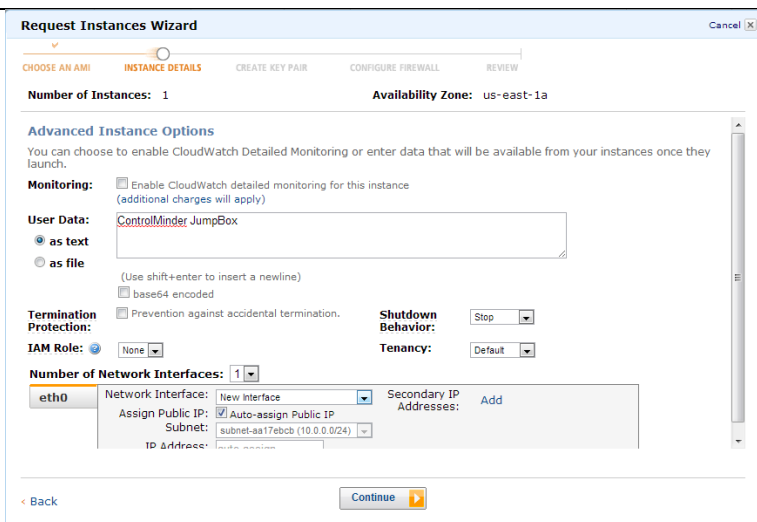
We will deploy a medium-sized Windows 2008 R2 instance on the public subnet as the JumpBox.

<p>Click the EC2 tab on the Amazon Web Services (AWS) Console.</p>	
--	--

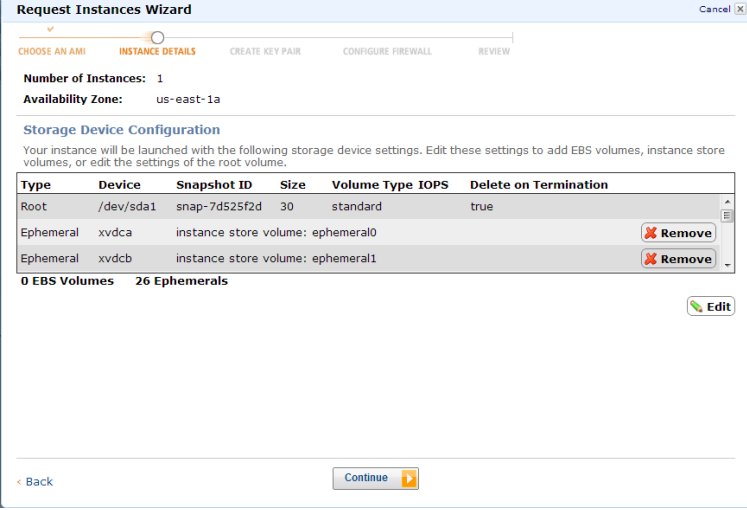
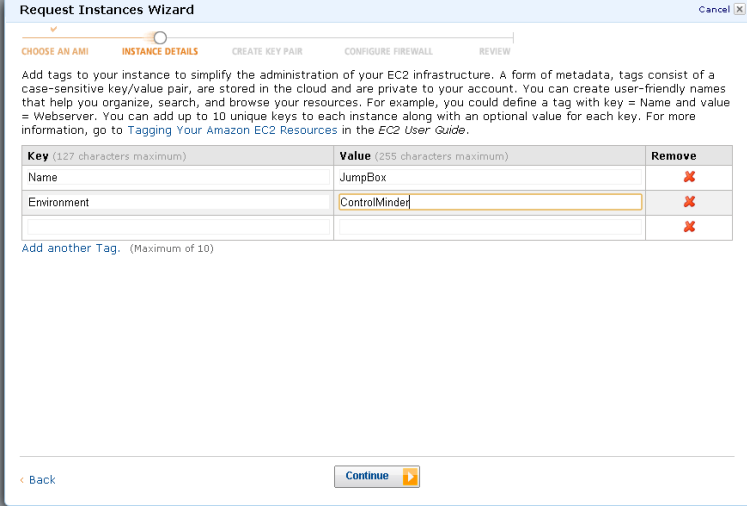

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

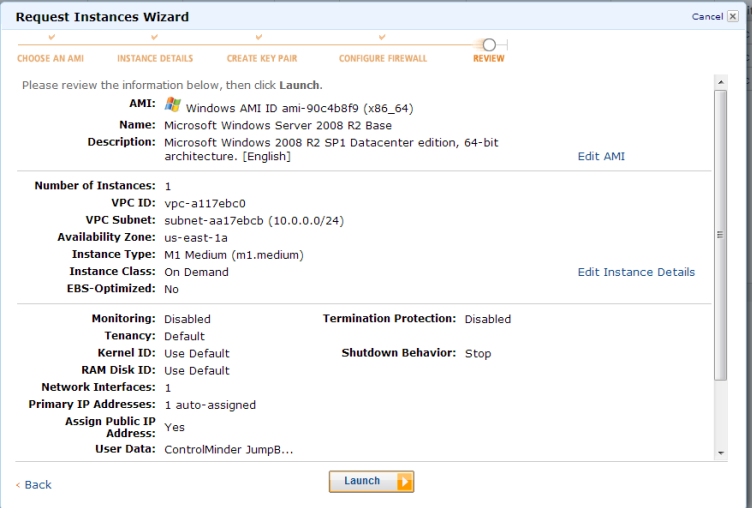
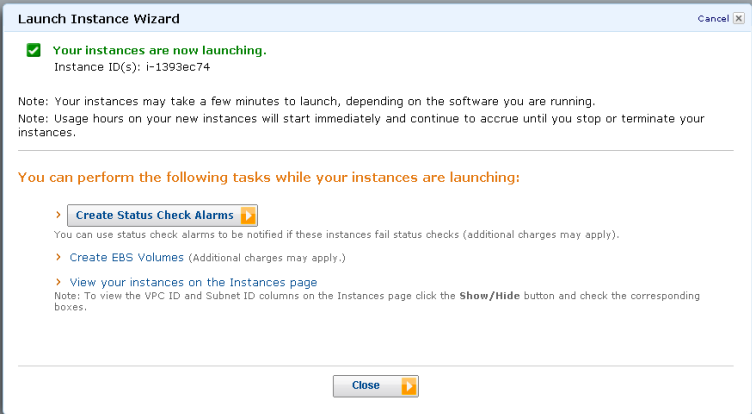
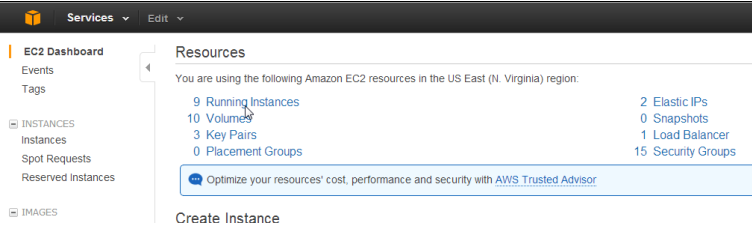
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

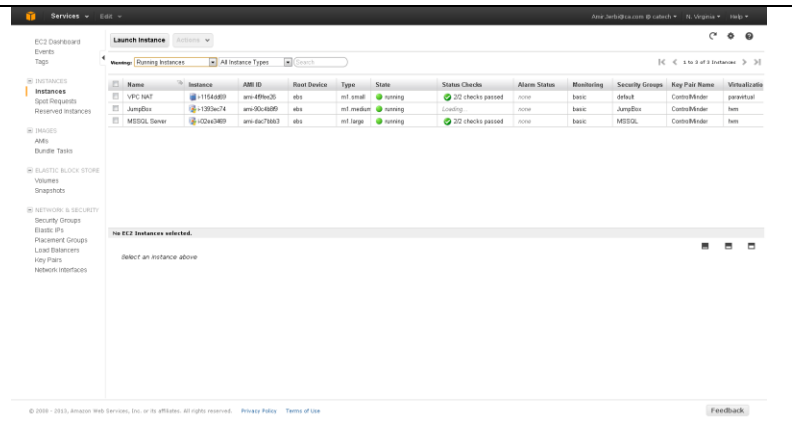
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Assign the following Security Groups to the JumpBox:</p> <ul style="list-style-type: none"> <li>• Default_Public</li> <li>• RDP_SSH_Public</li> </ul>	
<p>Click the “Launch” button.</p>	
	
<p>Click on “Running Instances” on the EC2 Dashboard to verify that your instance is up and running.</p>	



## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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



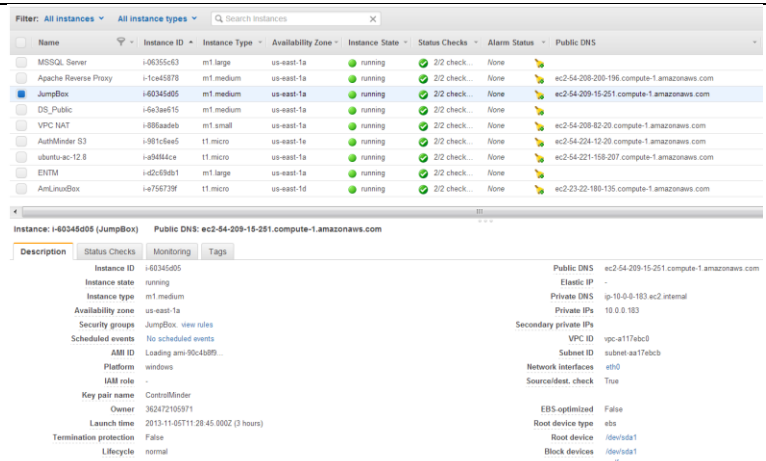
Name	Instance	AMI ID	Root Device	Type	State	Status Checks	Alarm Status	Monitoring	Security Groups	Key Pair Name	Virtualization
VPC NAT	i-115d4889	ami-4f9a20	efs	m1.xlarge	running	2/2 checks passed	none	basic	default	ControlMinder	paravirtual
MySQL Server	i-115d4889	ami-4f9a20	efs	m1.xlarge	running	2/2 checks passed	none	basic	default	ControlMinder	paravirtual

## 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.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
MSSQL Server	i-06355c63	m1.large	us-east-1a	running	2/2 check	None	ec2-54-209-200-196.compute-1.amazonaws.com
Apache Reverse Proxy	i-1ce45878	m1.medium	us-east-1a	running	2/2 check	None	ec2-54-209-15-251.compute-1.amazonaws.com
<b>JumpBox</b>	<b>i-60345d05</b>	<b>m1.medium</b>	<b>us-east-1a</b>	<b>running</b>	<b>2/2 check</b>	<b>None</b>	<b>ec2-54-209-15-251.compute-1.amazonaws.com</b>
DS_Public	i-6e3ae615	m1.medium	us-east-1a	running	2/2 check	None	ec2-54-209-83-20.compute-1.amazonaws.com
VPC NAT	i-886aadeb	m1.small	us-east-1a	running	2/2 check	None	ec2-54-204-10-20.compute-1.amazonaws.com
AuthMinder S3	i-981c6ee5	t1.micro	us-east-1a	running	2/2 check	None	ec2-54-221-158-207.compute-1.amazonaws.com
ubuntu-ac-12.8	i-a94f44ce	t1.micro	us-east-1a	running	2/2 check	None	ec2-54-221-158-207.compute-1.amazonaws.com
ENTM	i-d2c69db1	m1.large	us-east-1a	running	2/2 check	None	ec2-54-221-158-207.compute-1.amazonaws.com
AmLinuxBox	i-e756739f	t1.micro	us-east-1d	running	2/2 check	None	ec2-54-221-158-207.compute-1.amazonaws.com

Instance: i-60345d05 (JumpBox)		Public DNS: ec2-54-209-15-251.compute-1.amazonaws.com	
Description	Status Checks	Monitoring	Tags
Instance ID	i-60345d05	Public DNS	ec2-54-209-15-251.compute-1.amazonaws.com
Instance state	running	Elastic IP	-
Instance type	m1.medium	Private DNS	ip-10-0-0-183.ec2.internal
Availability zone	us-east-1a	Private IPs	10.0.0.183
Security groups	JumpBox, view rules	Secondary private IPs	-
Scheduled events	No scheduled events	VPC ID	vpc-a177abcb
AMI ID	Loading ami-90c4b895...	Subnet ID	subnet-a47f6cb3
Platform	windows	Network interfaces	eni0
IAM role	-	SourceDestCheck	True
Key pair name	ControlMinder	EBX optimized	False
Owner	362472105971	Root device type	ebs
Launch time	2013-11-05T11:20:45.000Z (3 hours)	Root device	/dev/sda1
Termination protection	False	Block devices	/dev/sda1
Lifecycle	normal		xvdf

Click "Connect".

Launch Instance

Connect

Actions ▾

Filter: All instances ▾ All instance types ▾

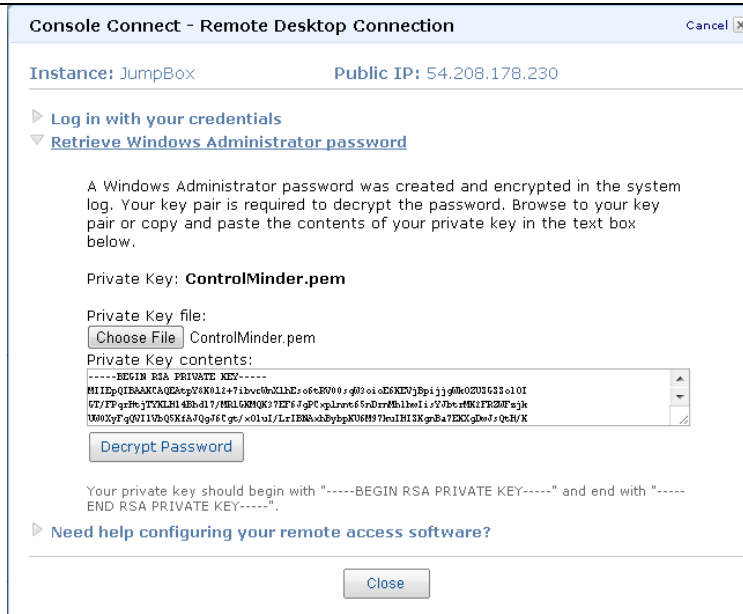
<input type="checkbox"/>	Name	Instance ID ▴
<input type="checkbox"/>	MSSQL Server	i-06355c63
<input type="checkbox"/>	Apache Reverse Proxy	i-1ce45878
<input checked="" type="checkbox"/>	JumpBox	i-60345d05
<input type="checkbox"/>	DS_Public	i-6e3ae615
<input type="checkbox"/>	VPC NAT	i-886aadeb
<input type="checkbox"/>	AuthMinder S3	i-981c6ee5
<input type="checkbox"/>	ubuntu-ac-12.8	i-a94f44ce
<input type="checkbox"/>	ENTM	i-d2c69db1
<input type="checkbox"/>	AmLinuxBox	i-e756739f

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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.



**Console Connect - Remote Desktop Connection** Cancel X

Instance: JumpBox Public IP: 54.208.178.230

► [Log in with your credentials](#)

▼ [Retrieve Windows Administrator password](#)

A Windows Administrator password was created and encrypted in the system log. Your key pair is required to decrypt the password. Browse to your key pair or copy and paste the contents of your private key in the text box below.

Private Key: **ControlMinder.pem**

Private Key file:  
 ControlMinder.pem

Private Key contents:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAzP7K0L1+7ibveW0L1Hs of eK00 0: q00 oi oD6KDPjBpijg0k0203633 o10I
C7/TPgrHejTYKLIH 4Bh-d17/MSLGMN0K37EF67gPc.pLret65ndrrMh1beLi:57beH9K1P82MF+jk
U00XyEg0011Vb05K4A70g76Cge/x01ul/Lr1ENa-shBybpK06M97ke1H1SKgr8a7E0Xgbe7+QcH/K
```

Your private key should begin with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----".

► [Need help configuring your remote access software?](#)

Click the [Log in with your credentials](#) link.

Click the [Download shortcut file](#) link.



**Console Connect - Remote Desktop Connection** Cancel X

Instance: JumpBox Public IP: 54.208.178.230

▼ [Log in with your credentials](#)

Log in to your instance with your credentials:

**Public IP:** 54.208.178.230  
**Username:** Administrator  
**Password:**

Note: If you are having problems with your decrypted password, try typing it instead of using copy and paste.

You can download an RDP file for this instance which will launch Remote Desktop Connection and connect to your instance. You will need to note down your password because the Remote Desktop Connection software will open in a new window.


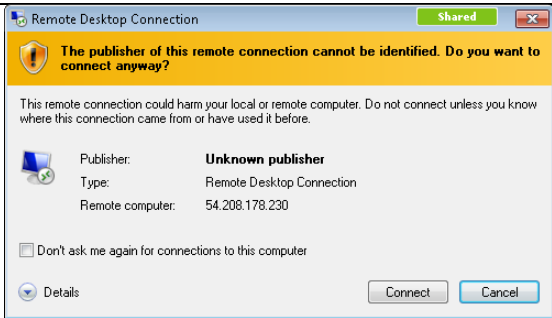
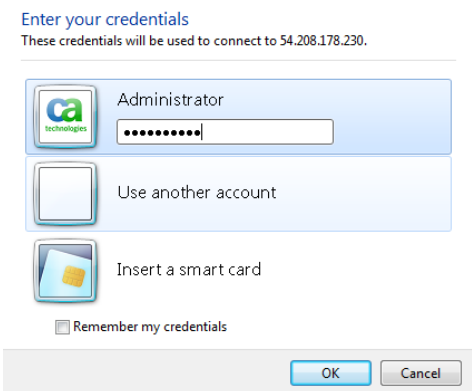
 [Download shortcut file](#)

If you need help configuring your remote desktop software, click [here](#).

► [Retrieve Windows Administrator password](#)

► [Need help configuring your remote access software?](#)

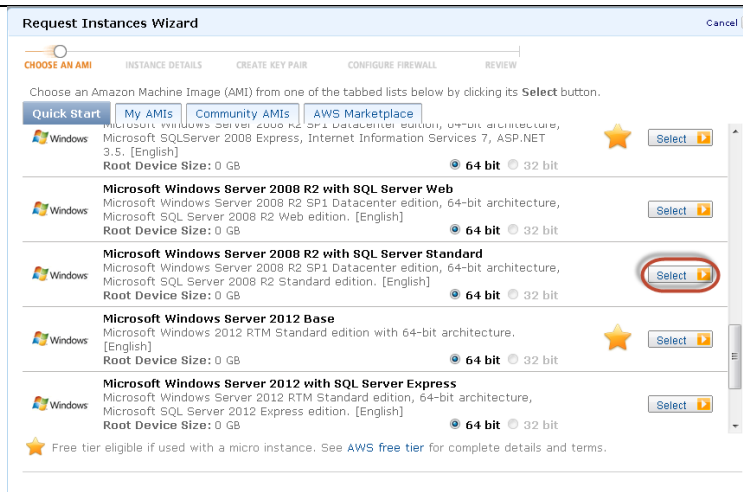
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

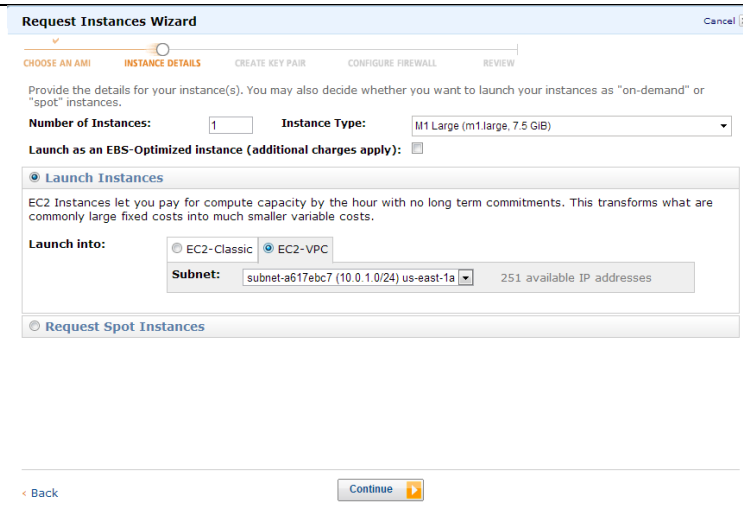
## Deploying the RDBMS Using Microsoft SQL Server

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”.



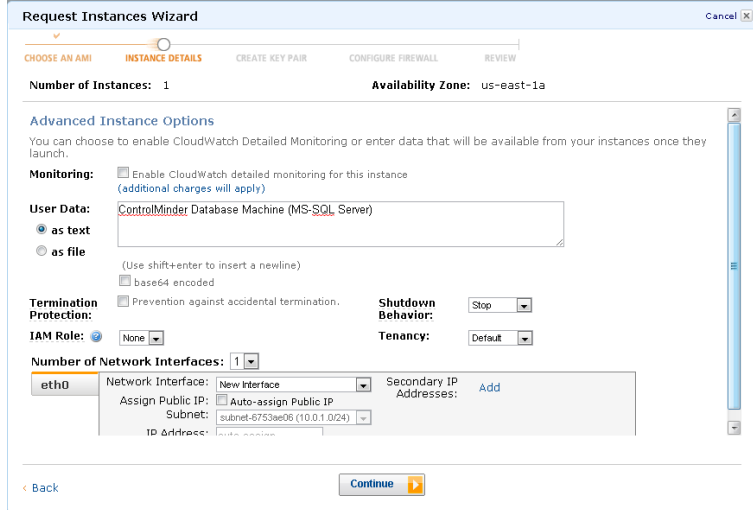
Deploy the instance on the private subnet.



## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

Provide “User data” to identify your instance.

Click the Continue button.



**Request Instances Wizard**

CHOOSE AN AMI | **INSTANCE DETAILS** | CREATE KEY PAIR | CONFIGURE FIREWALL | REVIEW

Number of Instances: 1 Availability Zone: us-east-1a

**Advanced Instance Options**

You can choose to enable CloudWatch Detailed Monitoring or enter data that will be available from your instances once they launch.

**Monitoring:** ☐ Enable CloudWatch detailed monitoring for this instance (additional charges will apply)

**User Data:** ControlMinder Database Machine (MS-SQL Server)

☒ as text ☐ as file

(Use shift+enter to insert a newline)

☐ base64 encoded

**Termination Protection:** ☐ Prevention against accidental termination.

**Shutdown Behavior:** Stop

**IAM Role:** None

**Tenancy:** Default

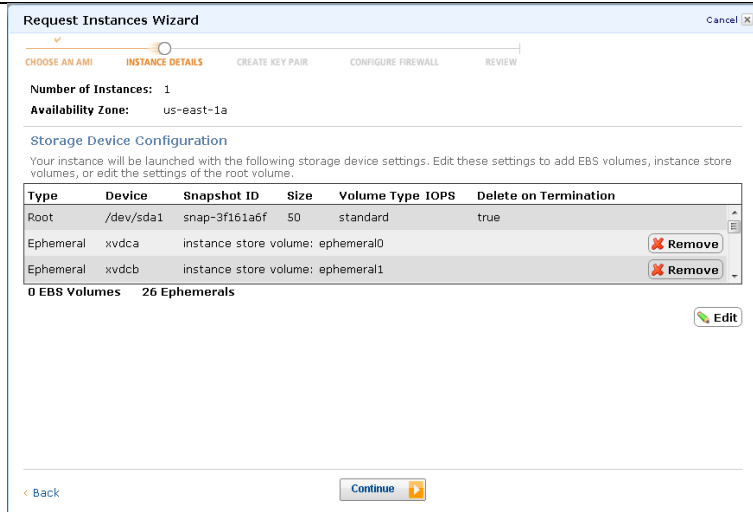
Number of Network Interfaces: 1

eth0 Network Interface: New Interface Assign Public IP: ☒ Auto-assign Public IP Subnet: subnet-6753ae06 (10.0.1.0/24) ID Address: Add

Secondary IP Addresses: Add

Back Continue

Click the Continue button to accept the default allocation of 50 gigabytes of disk storage.



**Request Instances Wizard**

CHOOSE AN AMI | **INSTANCE DETAILS** | CREATE KEY PAIR | CONFIGURE FIREWALL | REVIEW

Number of Instances: 1 Availability Zone: us-east-1a

**Storage Device Configuration**

Your instance will be launched with the following storage device settings. Edit these settings to add EBS volumes, instance store volumes, or edit the settings of the root volume.

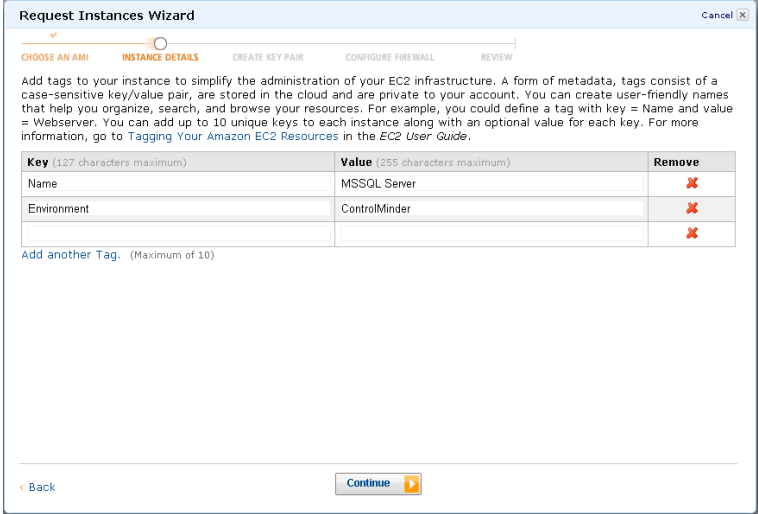
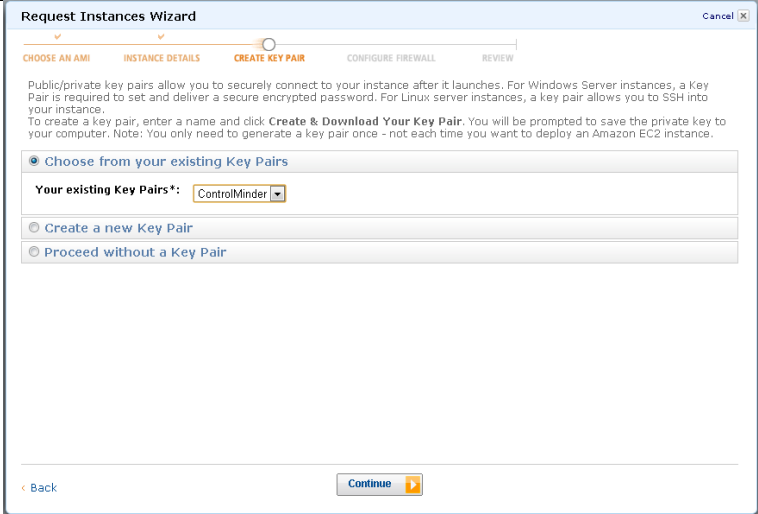
Type	Device	Snapshot ID	Size	Volume Type	IOPS	Delete on Termination
Root	/dev/sda1	snap-3f161a6f	50	standard		true
Ephemeral	xvda	instance store volume: ephemeral0				<a href="#">Remove</a>
Ephemeral	xvdc	instance store volume: ephemeral1				<a href="#">Remove</a>

0 EBS Volumes 26 Ephemerals

Edit

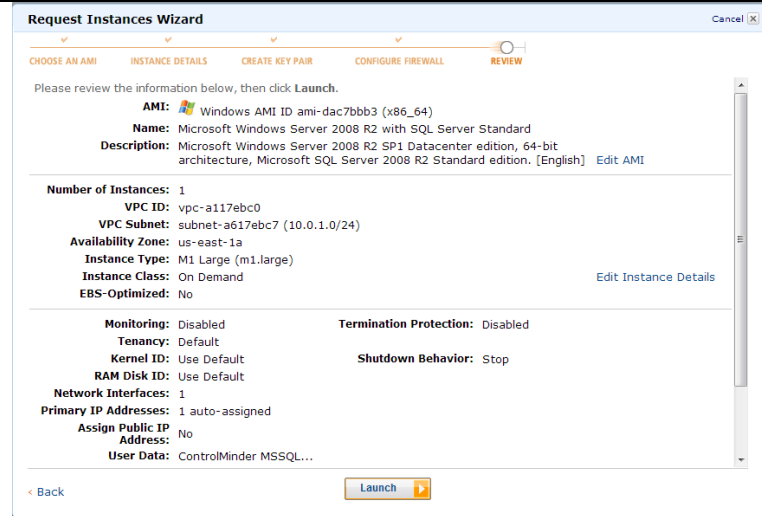
Back Continue

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment


Launch the instance by clicking the Launch button.



**Request Instances Wizard** Cancel X


CHOOSE AN AMI ✓ INSTANCE DETAILS ✓ CREATE KEY PAIR ✓ CONFIGURE FIREWALL ✓ **REVIEW** ○

Please review the information below, then click **Launch**.

**AMI:**  Windows AMI ID ami-dac7bbb3 (x86\_64)  
**Name:** Microsoft Windows Server 2008 R2 with SQL Server Standard  
**Description:** Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQL Server 2008 R2 Standard edition, [English] [Edit AMI](#)

**Number of Instances:** 1  
**VPC ID:** vpc-a117ebc0  
**VPC Subnet:** subnet-a617ebc7 (10.0.1.0/24)  
**Availability Zone:** us-east-1a  
**Instance Type:** M1 Large (m1.large) [Edit Instance Details](#)  
**Instance Class:** On Demand  
**EBS-Optimized:** No

**Monitoring:** Disabled **Termination Protection:** Disabled  
**Tenancy:** Default  
**Kernel ID:** Use Default **Shutdown Behavior:** Stop  
**RAM Disk ID:** Use Default  
**Network Interfaces:** 1  
**Primary IP Addresses:** 1 auto-assigned  
**Assign Public IP Address:** No  
**User Data:** ControlMinder MSSQL...

[Back](#) **Launch** 



## Preparing the Database

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

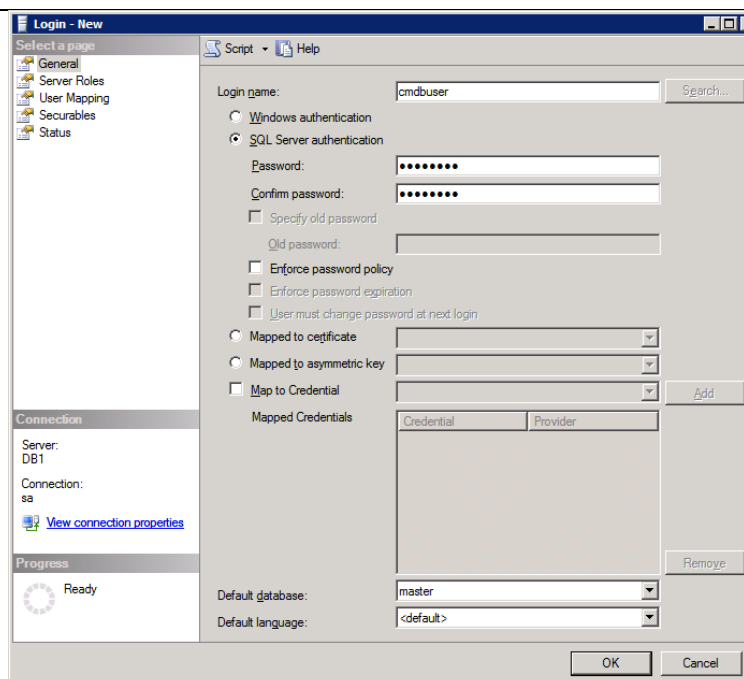
You can obtain the IP address of the Microsoft SQL Server from its instance properties.

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

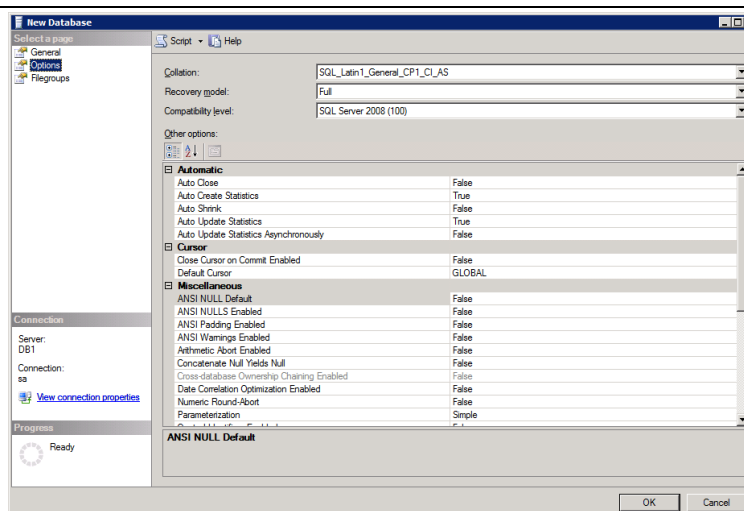
When creating the database, set Collation to:

**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.

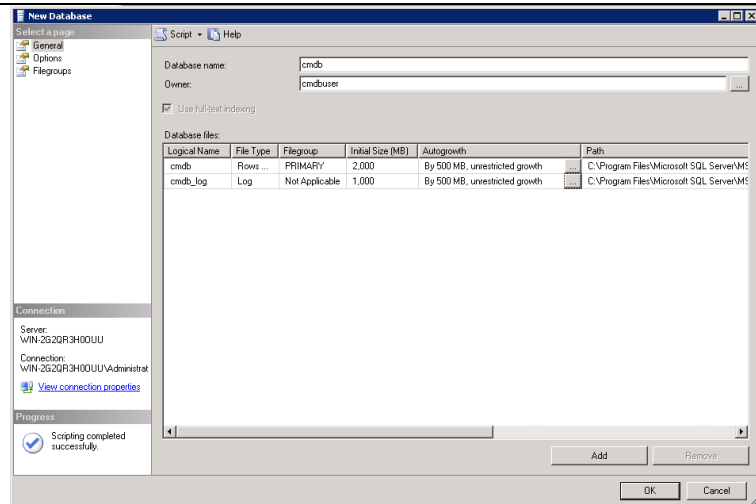


## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

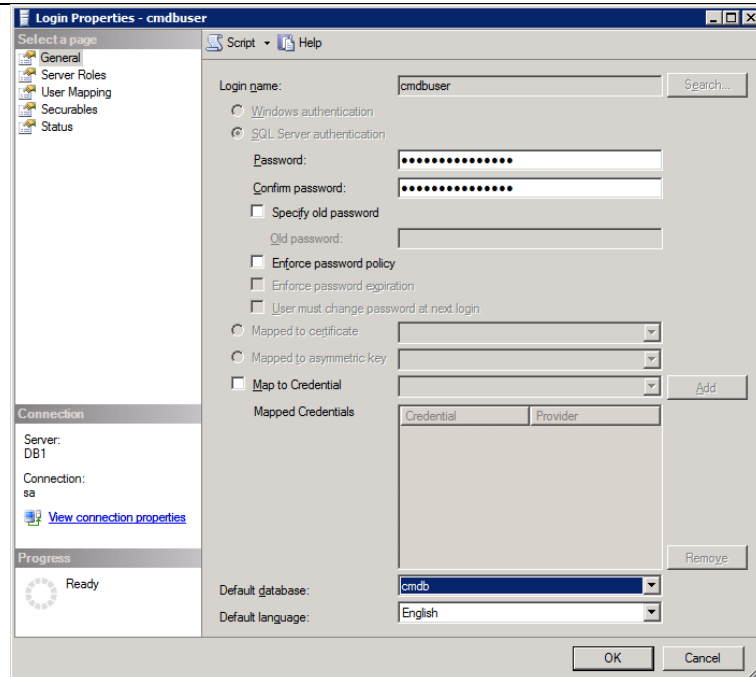
It is important to pre-allocate sufficient database space to hold configuration information and snapshot data.

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.

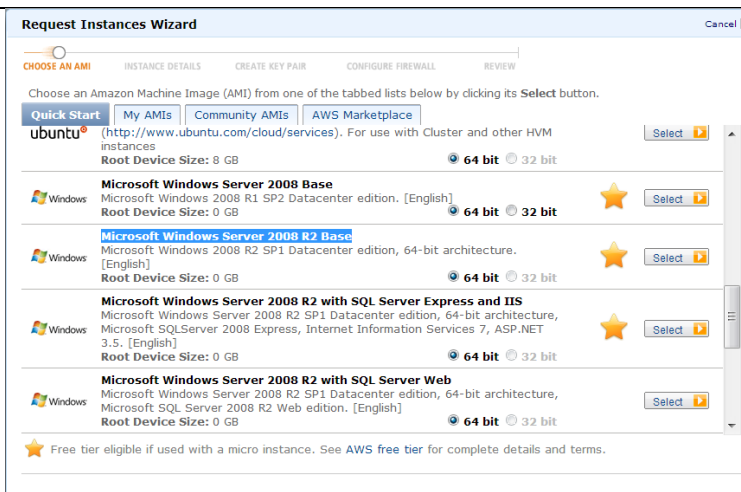


## Deploying Enterprise Management

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

### Create ENTM Instance

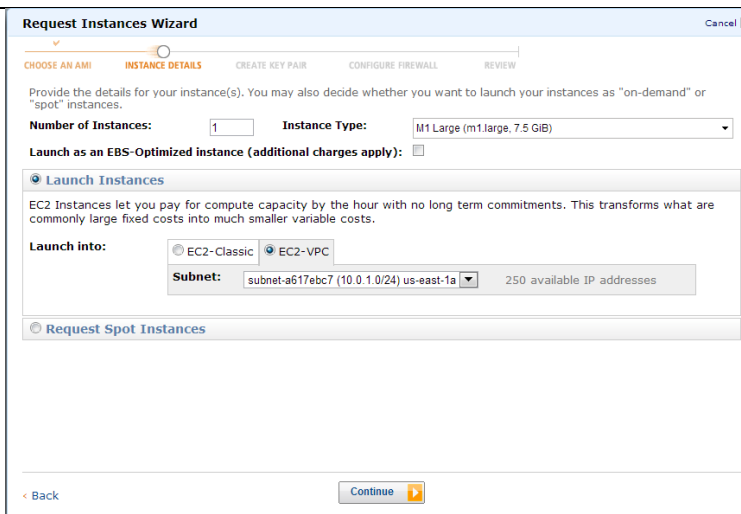
Create another instance using the Classic Wizard. Select “Microsoft Windows Server 2008 R2 Base” 64 bit.



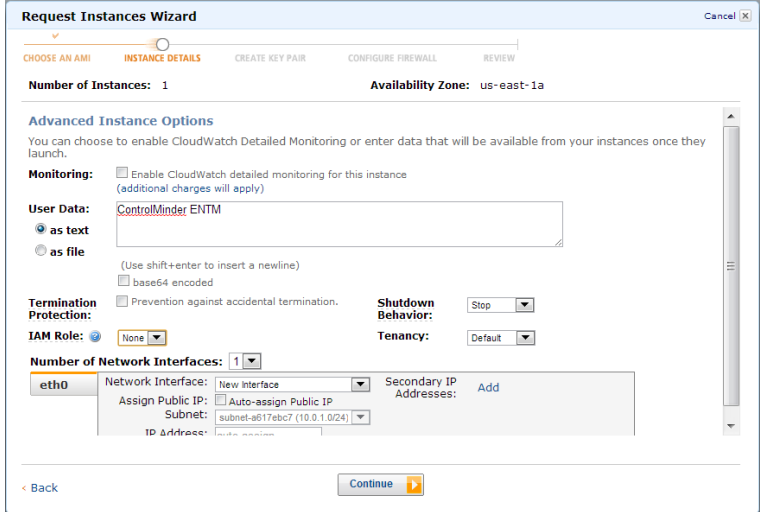
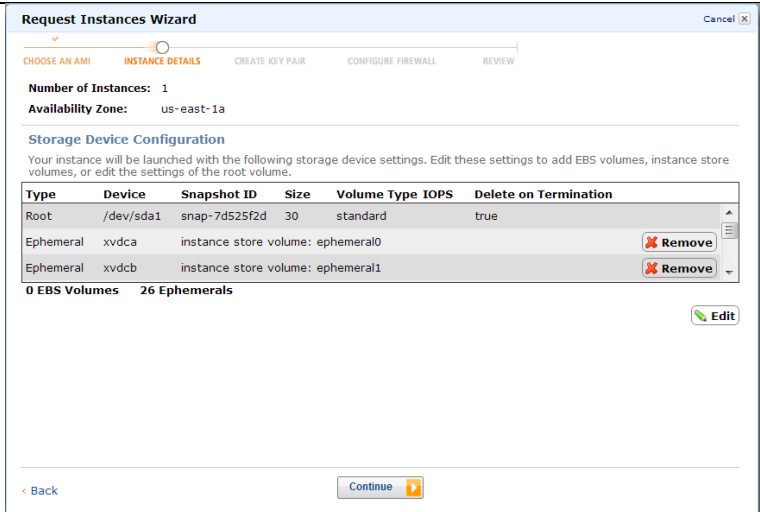
Set Instance Type to M1 Large.

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).

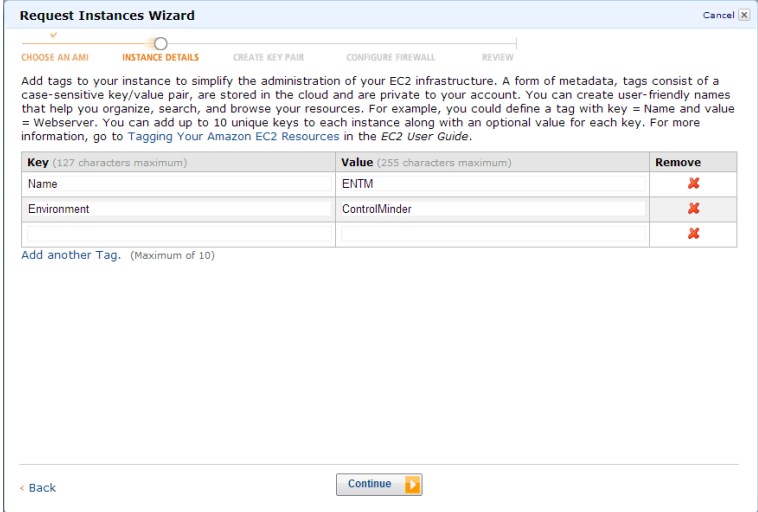

Click the Continue button.



## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Provide <u>User Data</u> to identify your instance.</p> <p>Keep default values for all other Settings.</p> <p>Click the Continue button.</p>																													
<p>Click the Continue button.</p> <p>30 gigabytes of disk storage is sufficient for the ENTM Server.</p>	 <table border="1" data-bbox="678 1003 1401 1108"> <thead> <tr> <th>Type</th> <th>Device</th> <th>Snapshot ID</th> <th>Size</th> <th>Volume Type</th> <th>IOPS</th> <th>Delete on Termination</th> </tr> </thead> <tbody> <tr> <td>Root</td> <td>/dev/sda1</td> <td>snap-7d525f2d</td> <td>30</td> <td>standard</td> <td></td> <td>true</td> </tr> <tr> <td>Ephemeral</td> <td>xvda</td> <td>instance store volume: ephemeral0</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Ephemeral</td> <td>xvdc</td> <td>instance store volume: ephemeral1</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Type	Device	Snapshot ID	Size	Volume Type	IOPS	Delete on Termination	Root	/dev/sda1	snap-7d525f2d	30	standard		true	Ephemeral	xvda	instance store volume: ephemeral0					Ephemeral	xvdc	instance store volume: ephemeral1				
Type	Device	Snapshot ID	Size	Volume Type	IOPS	Delete on Termination																							
Root	/dev/sda1	snap-7d525f2d	30	standard		true																							
Ephemeral	xvda	instance store volume: ephemeral0																											
Ephemeral	xvdc	instance store volume: ephemeral1																											

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

Launch the instance by clicking the Launch button.

Request Instances Wizard

Cancel

CHOOSE AN AMI


INSTANCE DETAILS

CREATE KEY PAIR

CONFIGURE FIREWALL

REVIEW

Please review the information below, then click **Launch**.

**AMI:**  Windows AMI ID ami-90c4b8f9 (x86\_64)  
**Name:** Microsoft Windows Server 2008 R2 Base  
**Description:** Microsoft Windows 2008 R2 SP1 Datacenter edition, 64-bit architecture. [English] [Edit AMI](#)

**Number of Instances:** 1  
**VPC ID:** vpc-a117ebc0  
**VPC Subnet:** subnet-a617ebc7 (10.0.1.0/24)  
**Availability Zone:** us-east-1a  
**Instance Type:** M1 Large (m1.large)  
**Instance Class:** On Demand [Edit Instance Details](#)  
**EBS-Optimized:** No

**Monitoring:** Disabled **Termination Protection:** Disabled  
**Tenancy:** Default  
**Kernel ID:** Use Default **Shutdown Behavior:** Stop  
**RAM Disk ID:** Use Default  
**Network Interfaces:** 1  
**Primary IP Addresses:** 1 auto-assigned  
**Assign Public IP Address:** No  
**User Data:** ControlMinder ENTM

[Back](#)
[Launch](#)

## 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.

<input type="checkbox"/>	Name	Instance	AMI ID	Root Device
<input type="checkbox"/>	MSSQL Server	i-06355c63	ami-dac7bbb3	ebs
<input type="checkbox"/>	JumpBox	i-60345d05	ami-90c4b8f9	ebs
<input type="checkbox"/>	VPC NAT	i-886aadeb	ami-4f9fee26	ebs
<input checked="" type="checkbox"/>	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

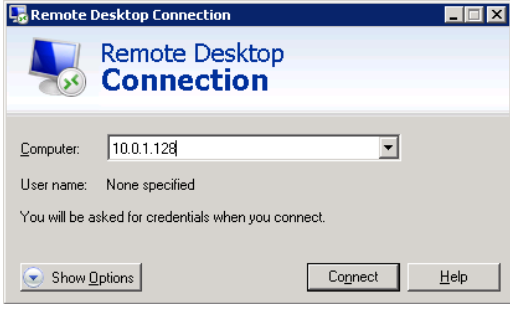
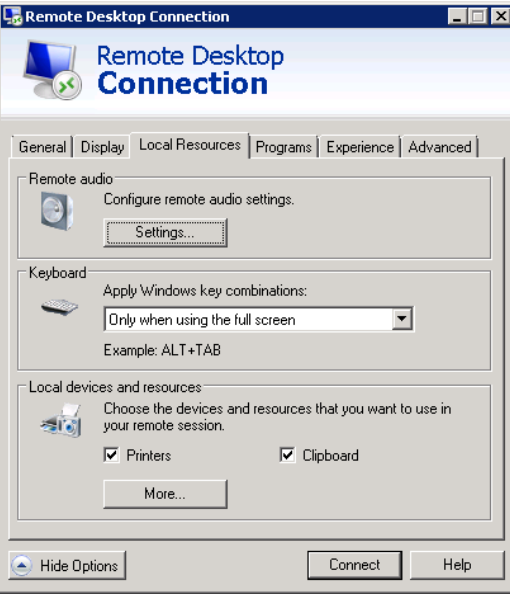
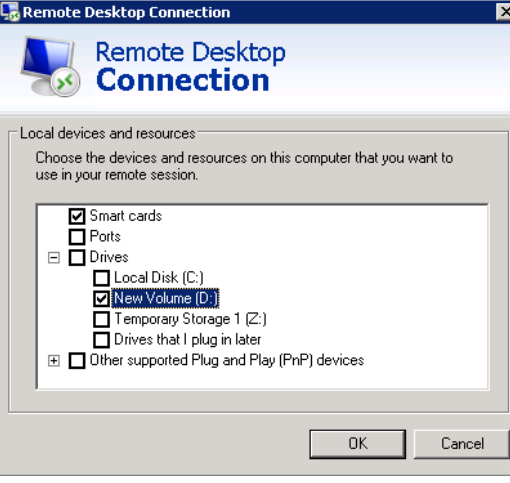
**Public DNS:**

**Private DNS:** ip-10-0-1-128.ec2.internal

**Private IPs:** 10.0.1.128

**Secondary Private IPs:**

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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



## 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

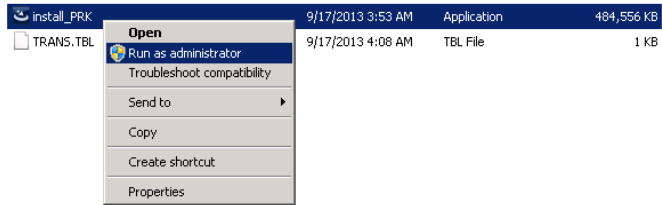
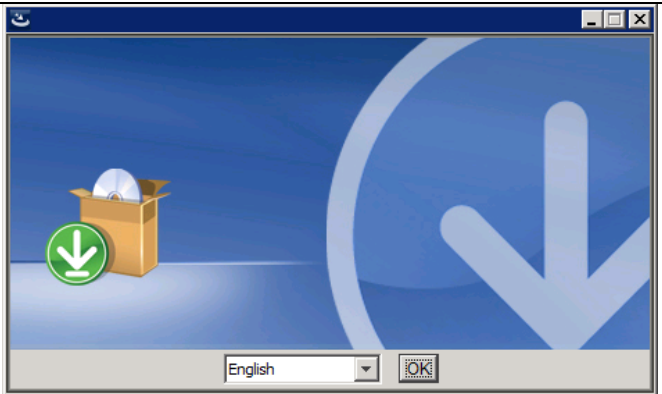
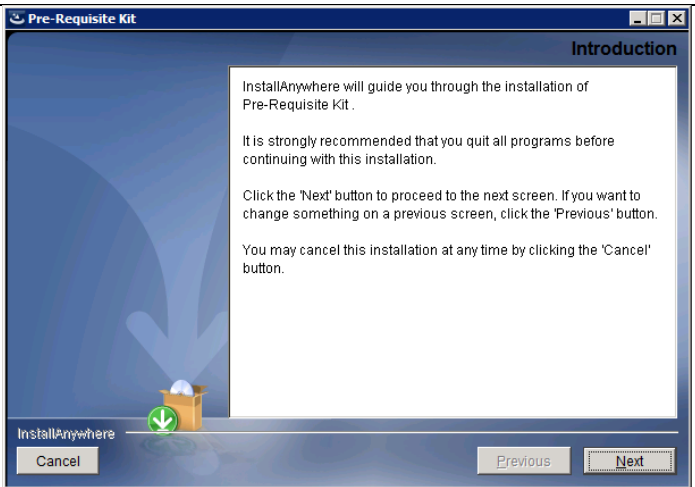
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

### Install Third-Party Components

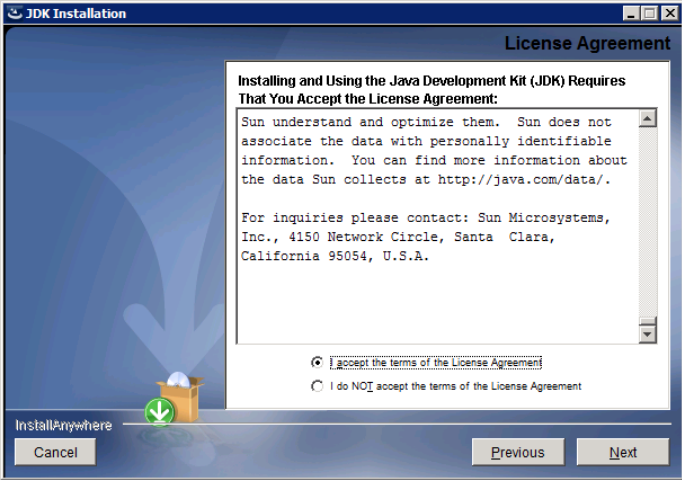
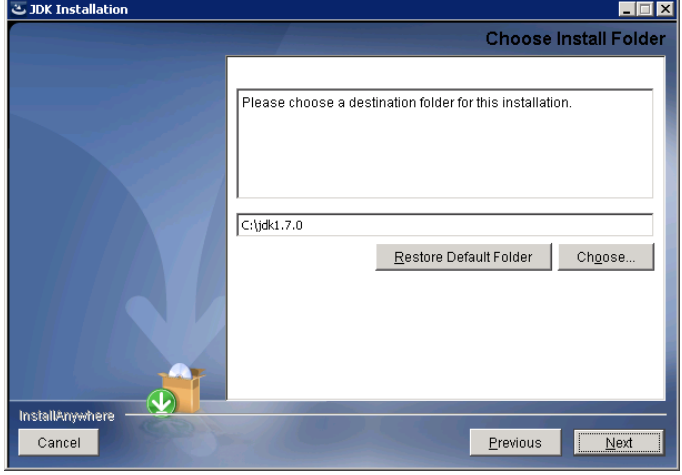
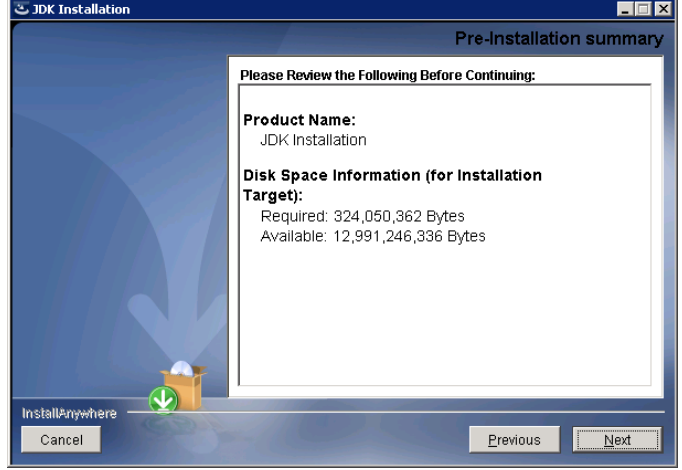
Login to the ENTM Server as a member of the local Administrators group.

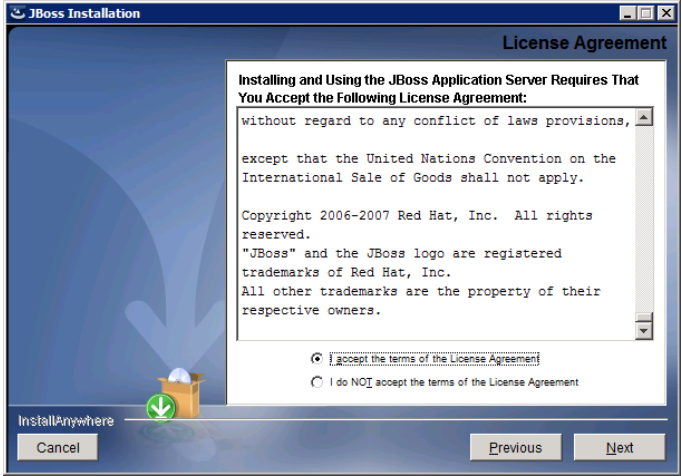
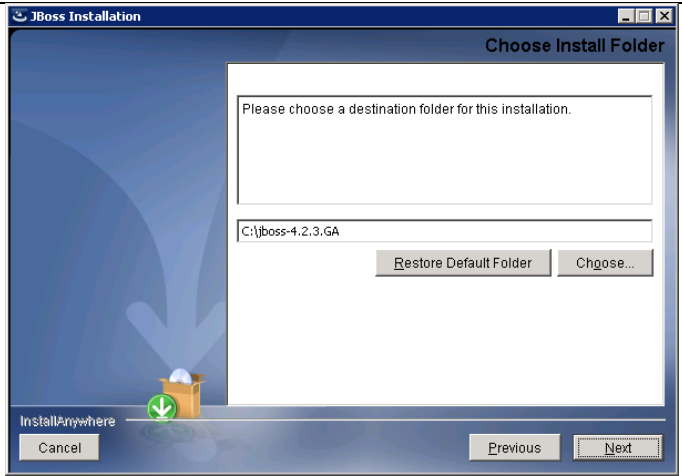
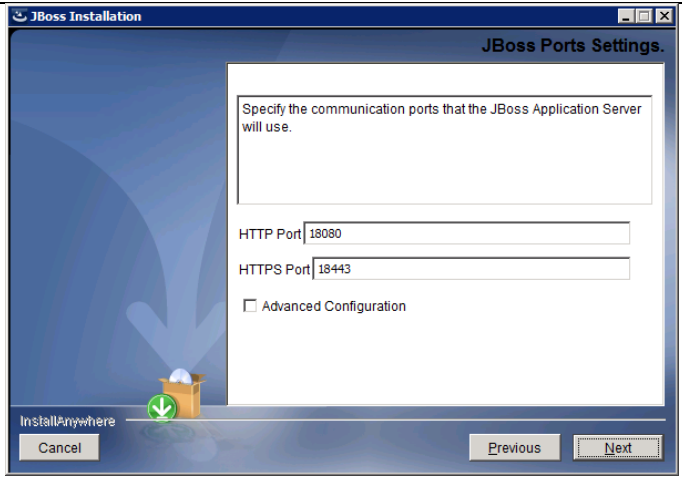
Mount the ISO image containing CA ControlMinder Third-Party Components for Windows.

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

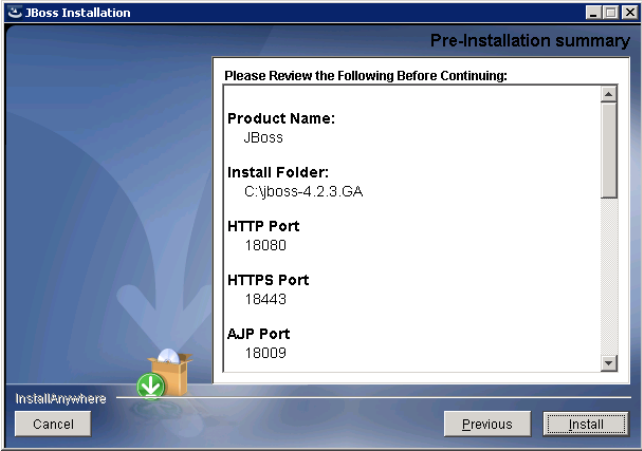
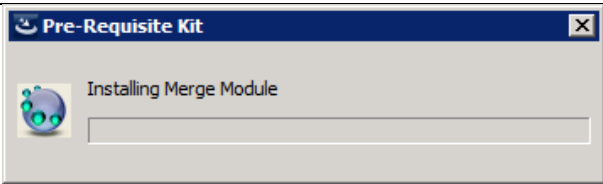
<p>Locate install_PRK.exe found in the PrereqInstaller directory of the Third-Party Components ISO image.</p> <p>Start the installation by right-clicking <b>Install_PRK.exe</b> and selecting <u>R</u>un as administrator from the menu.</p> <p>This will install the Java Development Kit and JBoss.</p>	
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

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p><b>JDK Installation</b></p> <p>Read the License Agreement as you use the scrollbar to advance through the document.</p> <p>Click the radial button noting <u>I accept the terms of the License Agreement</u>.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'JDK Installation' window with the 'License Agreement' tab selected. The text in the agreement states: 'Installing and Using the Java Development Kit (JDK) Requires That You Accept the License Agreement: Sun understand and optimize them. Sun does not associate the data with personally identifiable information. You can find more information about the data Sun collects at http://java.com/data/. For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.' Below the text, the radio button for 'I accept the terms of the License Agreement' is selected. At the bottom, the 'Next' button is visible.</p>
<p>Select the destination folder.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'JDK Installation' window with the 'Choose Install Folder' tab selected. It prompts the user to 'Please choose a destination folder for this installation.' The text box contains 'C:\jdk1.7.0'. Below the text box are 'Restore Default Folder' and 'Choose...' buttons. At the bottom, the 'Next' button is visible.</p>
<p>Click the Next button.</p>	 <p>The screenshot shows the 'JDK Installation' window with the 'Pre-Installation summary' tab selected. It prompts the user to 'Please Review the Following Before Continuing:'. The summary lists: 'Product Name: JDK Installation' and 'Disk Space Information (for Installation Target): Required: 324,050,362 Bytes, Available: 12,991,246,336 Bytes'. At the bottom, the 'Next' button is visible.</p>

<p><b>JBoss Installation</b></p> <p>Read the License Agreement as you use the scrollbar to advance through the document.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'JBoss Installation' window with the 'License Agreement' tab selected. The text in the agreement states: 'Installing and Using the JBoss Application Server Requires That You Accept the Following License Agreement: Without regard to any conflict of laws provisions, except that the United Nations Convention on the International Sale of Goods shall not apply. Copyright 2006-2007 Red Hat, Inc. All rights reserved. "JBoss" and the JBoss logo are registered trademarks of Red Hat, Inc. All other trademarks are the property of their respective owners.' At the bottom, there are two radio buttons: 'I accept the terms of the License Agreement' (which is selected) and 'I do NOT accept the terms of the License Agreement'. The 'Next' button is visible at the bottom right.</p>
<p>Select the destination folder.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'JBoss Installation' window with the 'Choose Install Folder' tab selected. It prompts the user to 'Please choose a destination folder for this installation.' Below this is a text box containing 'C:\jboss-4.2.3.GA'. There are two buttons: 'Restore Default Folder' and 'Choose...'. The 'Next' button is visible at the bottom right.</p>
<p>Click the Next button.</p>	 <p>The screenshot shows the 'JBoss Installation' window with the 'JBoss Ports Settings' tab selected. It prompts the user to 'Specify the communication ports that the JBoss Application Server will use.' There are two text boxes: 'HTTP Port' with the value '18080' and 'HTTPS Port' with the value '18443'. There is also a checkbox for 'Advanced Configuration' which is currently unchecked. The 'Next' button is visible at the bottom right.</p>

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

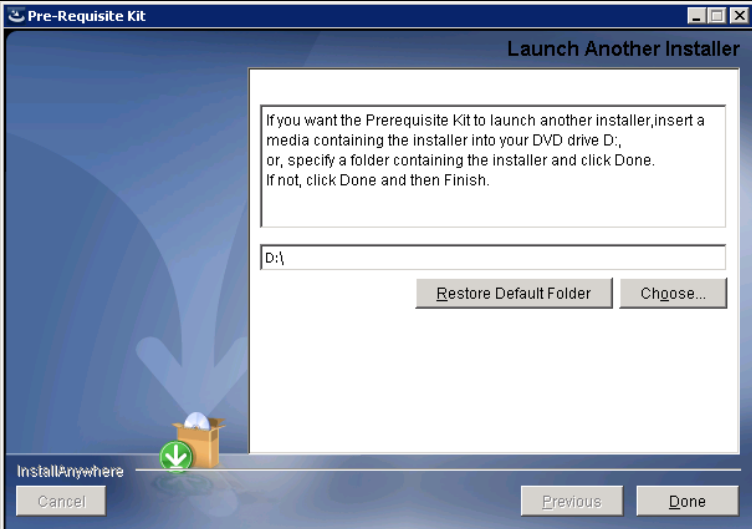
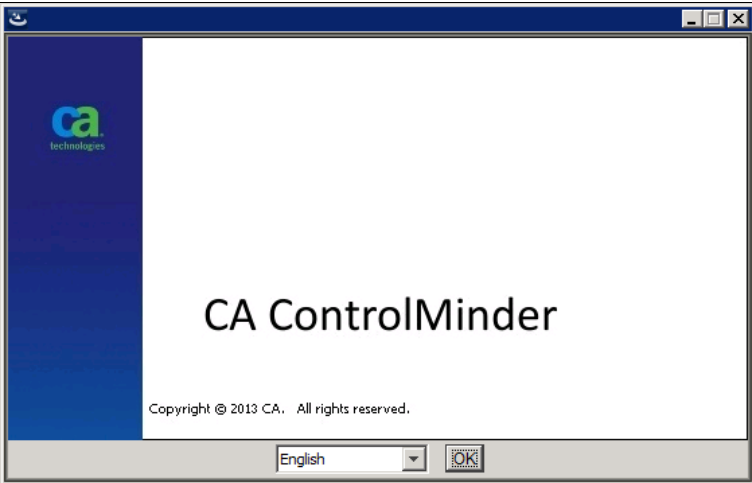
<p>Click the Install button.</p>	 <p>The screenshot shows the 'JBoss Installation' window with a 'Pre-Installation summary' tab. It lists the following details:</p> <ul style="list-style-type: none"> <li><b>Product Name:</b> JBoss</li> <li><b>Install Folder:</b> C:\jboss-4.2.3.GA</li> <li><b>HTTP Port:</b> 18080</li> <li><b>HTTPS Port:</b> 18443</li> <li><b>AJP Port:</b> 18009</li> </ul> <p>At the bottom, there is an 'InstallAnywhere' logo with a green arrow pointing down, and three buttons: 'Cancel', 'Previous', and 'Install'.</p>
<p>Wait for installation to complete</p>	 <p>The screenshot shows a 'Pre-Requisite Kit' window with the title 'Installing Merge Module'. It features a progress bar and a small icon of a globe with a green arrow.</p>

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

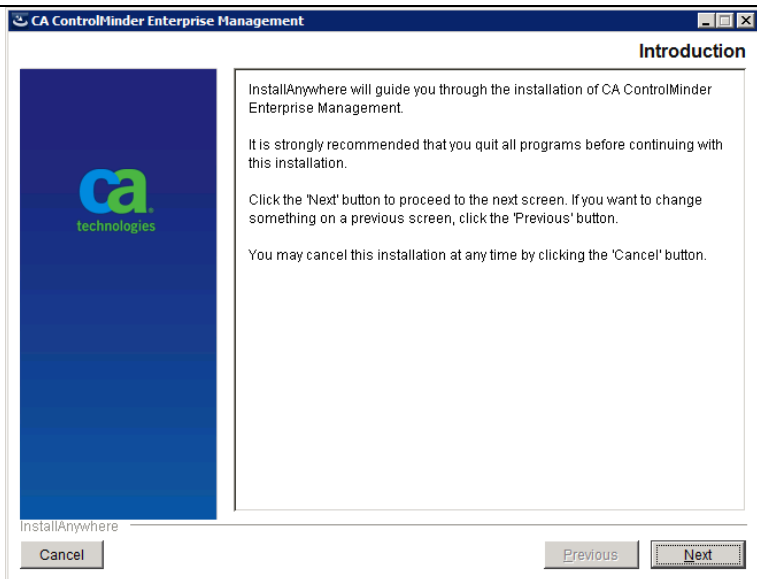
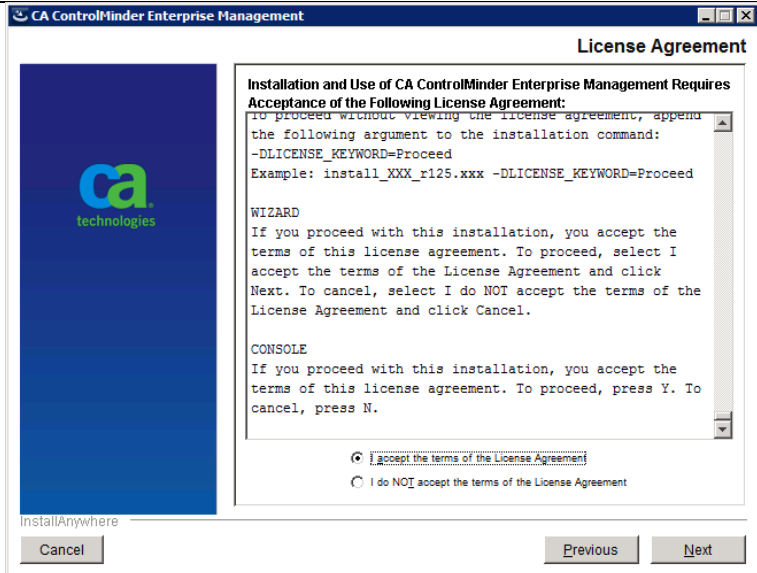
### Install Enterprise Management

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.

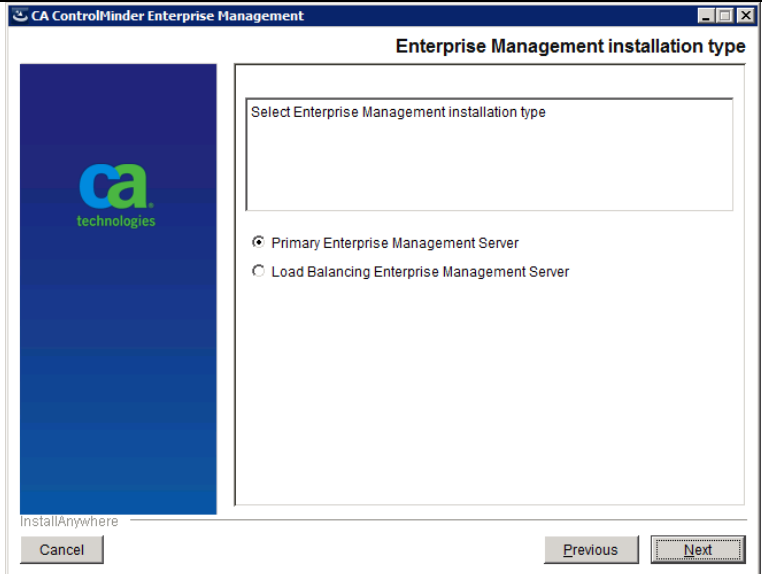
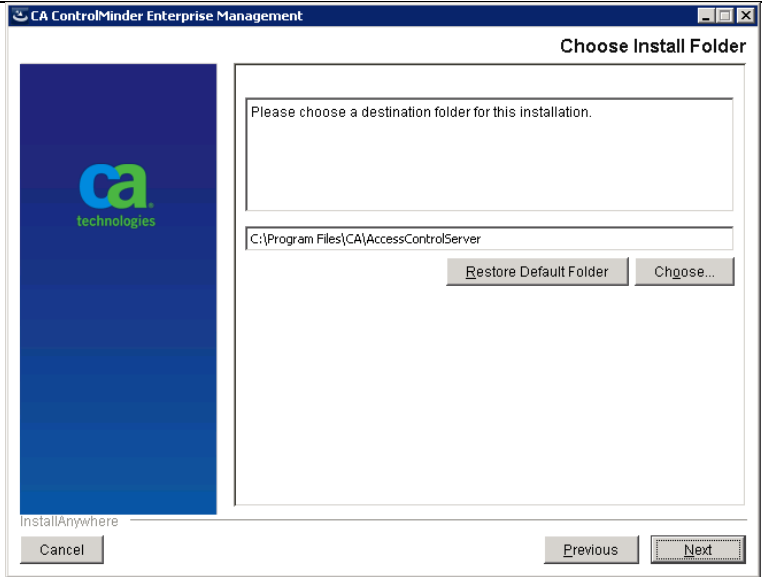
The following example has the Third-Party Components installer start the Enterprise Management installation.

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

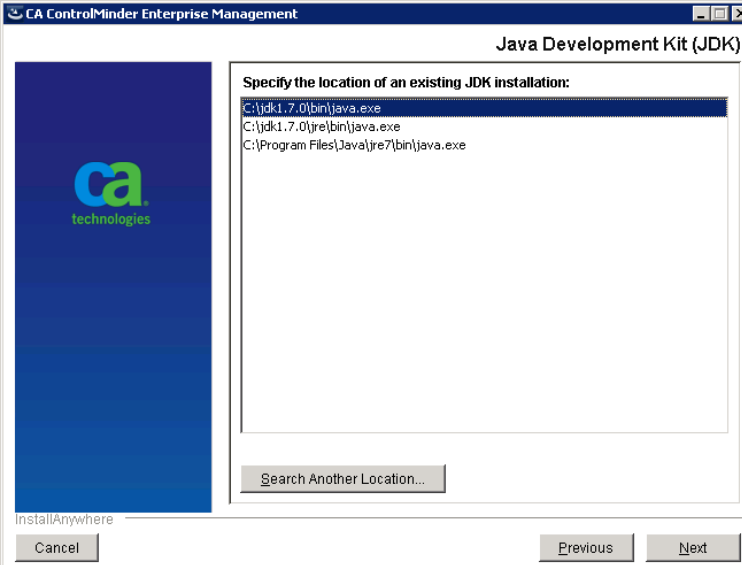
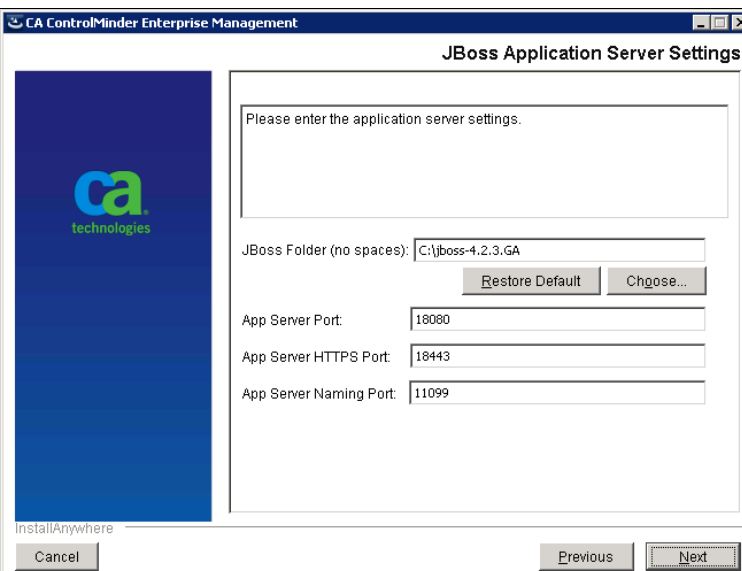
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

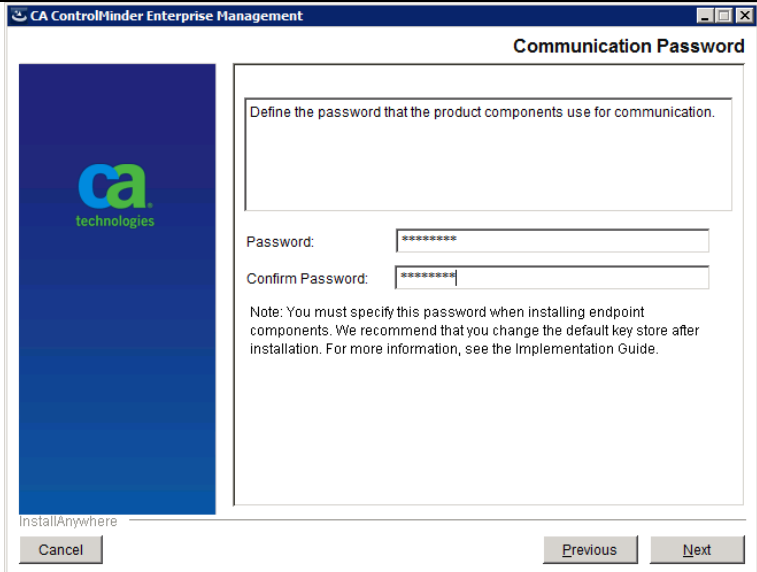
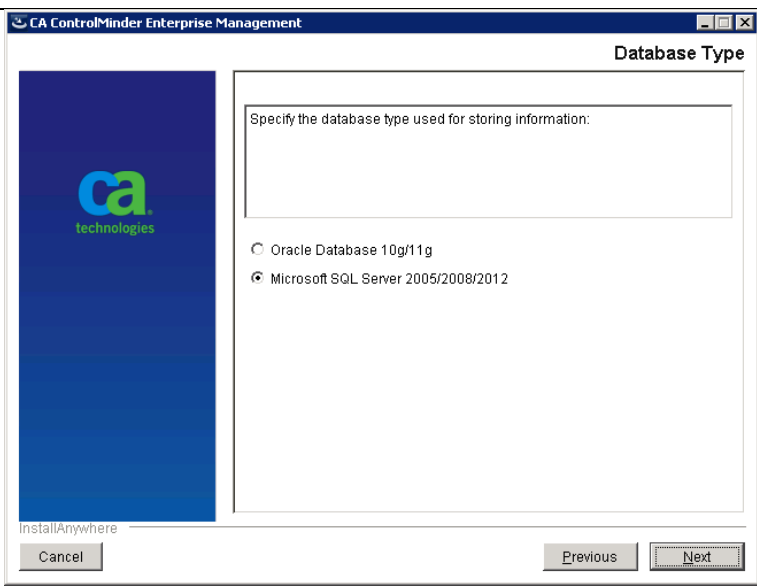
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Select the radial button next to Primary Enterprise Management Server</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'Enterprise Management installation type' window. On the left is a blue sidebar with the CA Technologies logo and the text 'InstallAnywhere'. The main area has the title 'Enterprise Management installation type' and a sub-header 'Select Enterprise Management installation type'. Below this are two radio buttons: 'Primary Enterprise Management Server' (which is selected) and 'Load Balancing Enterprise Management Server'. At the bottom are 'Cancel', 'Previous', and 'Next' buttons.</p>
<p>Select the destination folder.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'Choose Install Folder' window. On the left is a blue sidebar with the CA Technologies logo and the text 'InstallAnywhere'. The main area has the title 'Choose Install Folder' and a sub-header 'Please choose a destination folder for this installation.'. Below this is a text box containing 'C:\Program Files\CA\AccessControlServer'. To the right of the text box are 'Restore Default Folder' and 'Choose...' buttons. At the bottom are 'Cancel', 'Previous', and 'Next' buttons.</p>

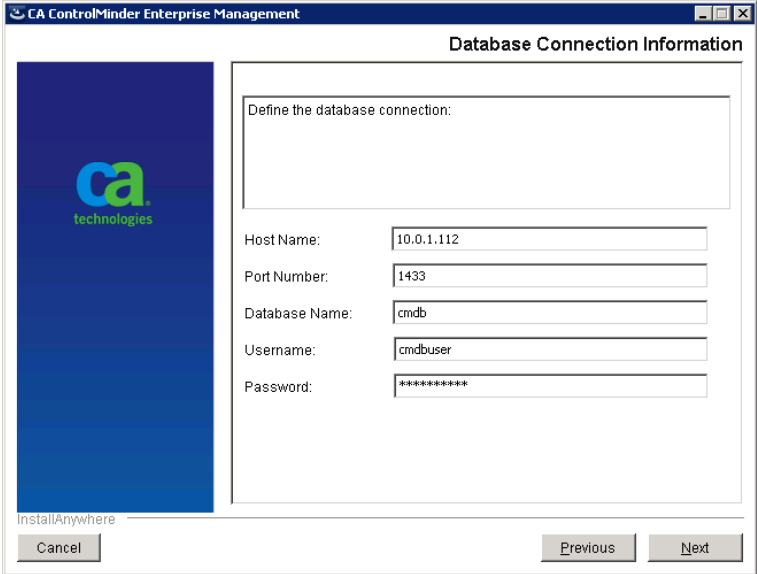
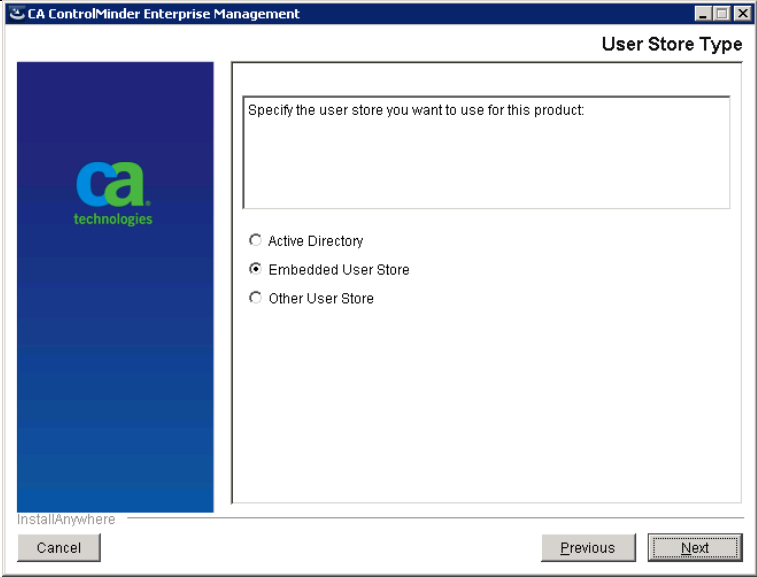


<p>Specify the location where you installed the Java JDK from the Third-Party Components ISO image.</p> <p><b>Note:</b> This page will only appear if you started the installation manually from ProductExplorer.</p>	
<p>Verify the JBoss settings.</p> <p>NOTE: The JBoss service must NOT be running at this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

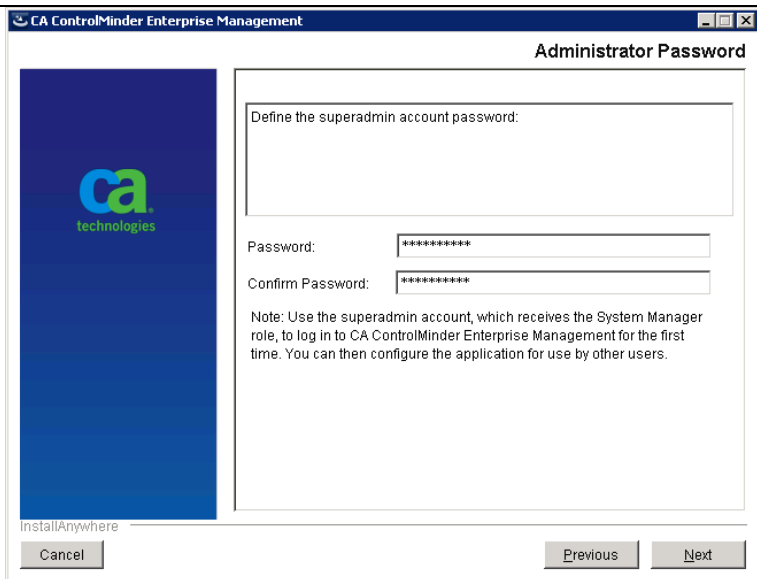
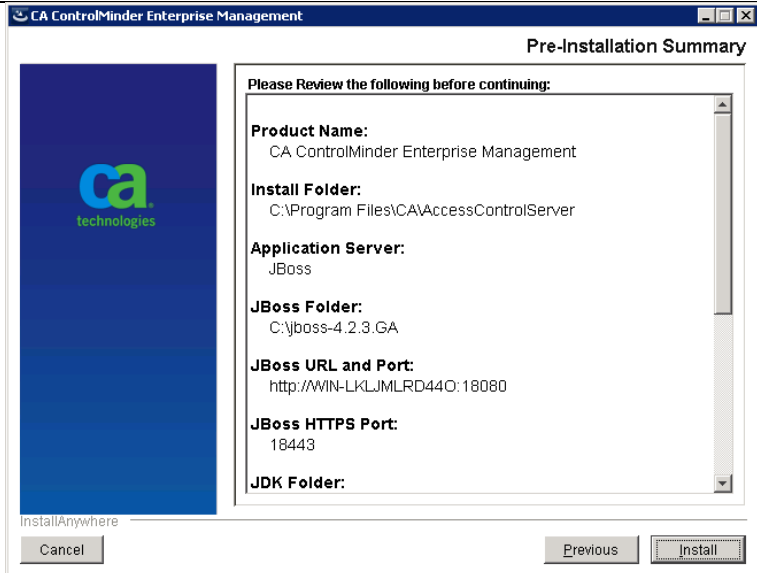
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Provide the communication password.</p> <p><b>NOTE:</b> This password is used internally by Enterprise Management components.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'Communication Password' window of the CA ControlMinder Enterprise Management installer. It features the CA Technologies logo on the left. The main area contains a text box for defining the password, followed by 'Password:' and 'Confirm Password:' fields, both masked with asterisks. A note at the bottom states: 'Note: You must specify this password when installing endpoint components. We recommend that you change the default key store after installation. For more information, see the Implementation Guide.' At the bottom of the window are 'Cancel', 'Previous', and 'Next' buttons.</p>
<p>Select the radial button for Microsoft SQL Server as the Database Type.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'Database Type' window of the CA ControlMinder Enterprise Management installer. It features the CA Technologies logo on the left. The main area contains a text box for specifying the database type, followed by two radio button options: 'Oracle Database 10g/11g' and 'Microsoft SQL Server 2005/2008/2012'. The 'Microsoft SQL Server 2005/2008/2012' option is selected. At the bottom of the window are 'Cancel', 'Previous', and 'Next' buttons.</p>

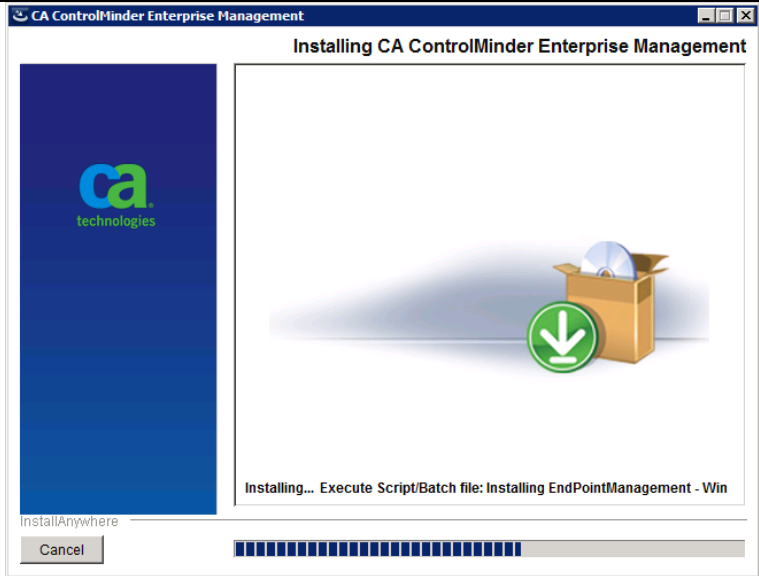
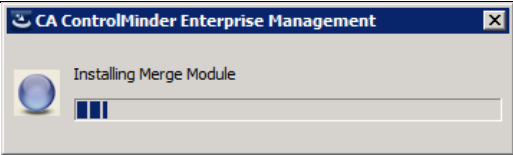
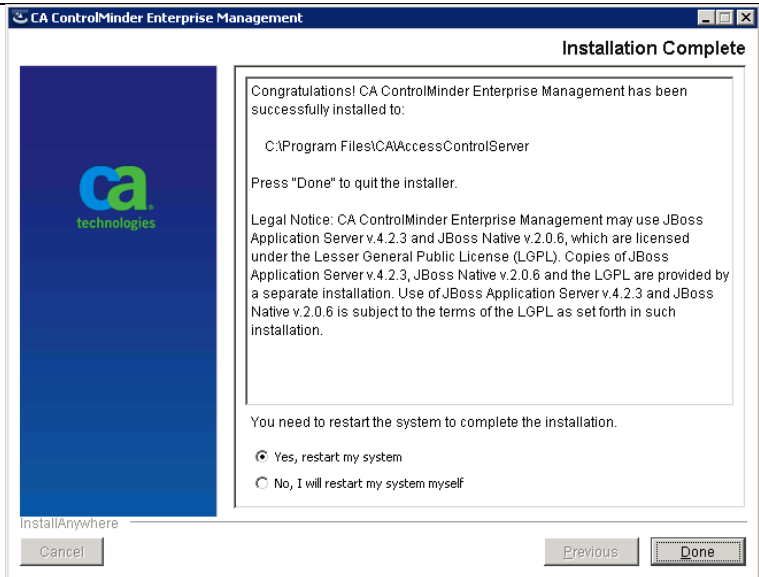
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Provide the password for the superadmin account. This will be the only user available after the installation.</p> <p>The superadmin account is assigned the System Manager role.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'Administrator Password' window of the CA ControlMinder Enterprise Management installer. It features the CA Technologies logo on the left. The main area contains a text box for 'Define the superadmin account password:', followed by 'Password:' and 'Confirm Password:' fields, both masked with asterisks. A note at the bottom states: 'Note: Use the superadmin account, which receives the System Manager role, to log in to CA ControlMinder Enterprise Management for the first time. You can then configure the application for use by other users.' At the bottom are 'Cancel', 'Previous', and 'Next' buttons.</p>
<p>Review the installation details.</p> <p>Click the Install button.</p>	 <p>The screenshot shows the 'Pre-Installation Summary' window of the CA ControlMinder Enterprise Management installer. It features the CA Technologies logo on the left. The main area is titled 'Please Review the following before continuing:' and lists the following details:         <ul style="list-style-type: none"> <li><b>Product Name:</b> CA ControlMinder Enterprise Management</li> <li><b>Install Folder:</b> C:\Program Files\CA\AccessControlServer</li> <li><b>Application Server:</b> JBoss</li> <li><b>JBoss Folder:</b> C:\jboss-4.2.3.GA</li> <li><b>JBoss URL and Port:</b> http://WIN-LKLJMLRD44O:18080</li> <li><b>JBoss HTTPS Port:</b> 18443</li> <li><b>JDK Folder:</b></li> </ul>         At the bottom are 'Cancel', 'Previous', and 'Install' buttons.       </p>

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Wait for the installation to complete</p> <p>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.</p>	 <p>The screenshot shows the 'Installing CA ControlMinder Enterprise Management' window. It features the CA Technologies logo on the left and a progress bar at the bottom. The status bar indicates 'Installing... Execute Script/Batch file: Installing EndPointManagement - Win'.</p>
<p>The installation is expected to take from 15 to 60 minutes to complete</p>	 <p>The screenshot shows a smaller window titled 'Installing Merge Module' with a progress bar.</p>
<p>After the installation successfully completes, click the Done button to reboot the server and finalize the installation.</p>	 <p>The screenshot shows the 'Installation Complete' window. It displays the CA Technologies logo on the left and a text area on the right with the following content:</p> <p>Congratulations! CA ControlMinder Enterprise Management has been successfully installed to:</p> <p>C:\Program Files\CA\AccessControlServer</p> <p>Press "Done" to quit the installer.</p> <p>Legal Notice: CA ControlMinder Enterprise Management may use JBoss Application Server v.4.2.3 and JBoss Native v.2.0.6, which are licensed under the Lesser General Public License (LGPL). Copies of JBoss Application Server v.4.2.3, JBoss Native v.2.0.6 and the LGPL are provided by a separate installation. Use of JBoss Application Server v.4.2.3 and JBoss Native v.2.0.6 is subject to the terms of the LGPL as set forth in such installation.</p> <p>You need to restart the system to complete the installation.</p> <p><input checked="" type="radio"/> Yes, restart my system</p> <p><input type="radio"/> No, I will restart my system myself</p> <p>Buttons: Previous, Done</p>

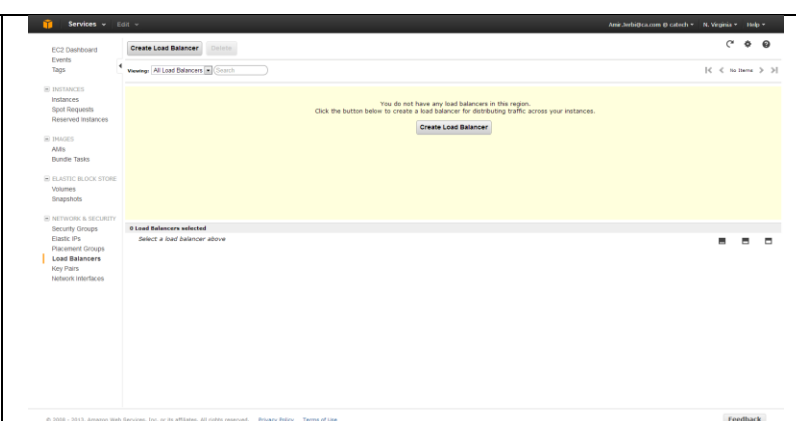
## Create Amazon Elastic Load Balancer

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

**Create a New Load Balancer** Cancel

DEFINE LOAD BALANCER | CONFIGURE HEALTH CHECK | ADD EC2 INSTANCES | REVIEW

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

**Load Balancer Name:**

Load balancer names must contain only alphanumeric characters or dashes.

**Create LB inside:**

**Create an internal load balancer:** ☐ (what's this?)

**Listener Configuration:**

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port	Actions
HTTPS (Secure HTTP)	443	HTTPS (Secure HTTP)	18443	<a href="#">Remove</a>
<input type="text" value="HTTP"/>	<input type="text" value=""/>	<input type="text" value="HTTP"/>	<input type="text" value=""/>	<a href="#">Save</a>

[Continue](#)

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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](http://www.akadia.com/services/ssh_test_certificate.html)

**Create a New Load Balancer** Cancel X

DEFINE LOAD BALANCER | CONFIGURE HEALTH CHECK | ADD EC2 INSTANCES | REVIEW

An SSL Certificate allows you to configure the HTTPS/SSL listeners of your Load Balancer. You may select a previously uploaded certificate below, or define a new SSL Certificate by supplying certificate name, a private key (pem encoded), and a public key certificate (pem encoded). You may also provide an optional public key certificate chain (pem encoded). Learn more about setting up HTTPS load balancer listeners and certificate management. (Note: The certificate you choose here will apply to all the HTTPS/SSL listeners you configured. Click [here](#) to learn about the API to use to customize the SSL certificates of your load balancer.)

☒ Choose from your existing SSL Certificates

☒ Upload a new SSL Certificate

**Certificate Name:**\*   
(e.g., myServerCert)

**Private Key:**\*   
(pem encoded)

**Public Key Certificate:**\*   
(pem encoded)

**Certificate Chain:**   
(pem encoded, Optional field)

[Back](#) [Continue](#) \* Required field

Select ELBSample-  
ELBDefaultNegotiationPolicy that includes  
SSLv3 and TLSv1.

**Create a New Load Balancer** Cancel X

DEFINE LOAD BALANCER | CONFIGURE HEALTH CHECK | ADD EC2 INSTANCES | REVIEW

You can configure SSL ciphers for the HTTPS/SSL listeners of your Load Balancer. You may select the ciphers from one of the sample cipher policies listed below or you can customize your own ciphers. Learn more about configuring SSL ciphers for HTTPS/SSL listeners. (Note: The SSL ciphers you choose here will apply to all the HTTPS/SSL listeners you configured. Click [here](#) to learn about the API to customize the SSL Ciphers for your load balancer.)

☒ ELBSample-ELBDefaultNegotiationPolicy

☐ ELBSample-OpenSSLDefaultNegotiationPolicy

☐ Custom

**SSL Protocols**

- ☐ Protocol-SSLv2
- ☒ Protocol-SSLv3
- ☒ Protocol-TLSv1
- ☐ Protocol-TLSv1.1
- ☐ Protocol-TLSv1.2

**SSL Ciphers**

- ☐ ADH-AES128-GCM-SHA256
- ☐ ADH-AES128-SHA
- ☐ ADH-AES128-SHA256
- ☐ ADH-AES256-GCM-SHA384
- ☐ ADH-AES256-SHA
- ☐ ADH-AES256-SHA256

[Back](#) [Continue](#)

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Select “Proceed without backend authentication” and click Continue.</p>	<div> <div>Create a New Load Balancer <span>Cancel</span></div> <div> <div> <div>DEFINE LOAD BALANCER</div> <div>CONFIGURE HEALTH CHECK</div> <div>ADD EC2 INSTANCES</div> <div>REVIEW</div> </div> <p>You have selected HTTPS/SSL protocol between your load balancer listener and backend application server. In order to enable backend server authentication and encryption, please provide a list of public key certificates to trust. <a href="#">Learn more</a> about configuring backend authentication policies for secure HTTPS/SSL backend ports. (Note: The list of public key certificates you selected will apply to all the secure HTTPS/SSL backend ports you configured. Click <a href="#">here</a> to learn about the API to customize it per backend port.)</p> <div> <input checked="" type="radio"/> <b>Proceed without backend authentication</b> </div> <div> <input type="radio"/> <b>Enable backend authentication</b> </div> <div> <div>I do not want to enable backend authentication.</div> <div></div> </div> <div> <div>Back</div> <div>Continue</div> </div> </div> </div>
<p>Configure the URL that will be used by the Load Balancer for health monitoring. Specify port 18433 and path “/iam/ac”.</p>	<div> <div>Create a New Load Balancer <span>Cancel</span></div> <div> <div> <div>DEFINE LOAD BALANCER</div> <div>CONFIGURE HEALTH CHECK</div> <div>ADD EC2 INSTANCES</div> <div>REVIEW</div> </div> <p>Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.</p> <p><b>Configuration Options:</b></p> <p>Ping Protocol: <span>HTTPS</span></p> <p>Ping Port: <span>18443</span></p> <p>Ping Path: <span>/iam/ac</span></p> <p><b>Advanced Options:</b></p> <div> <div>Response Timeout: <span>10</span> Seconds</div> <div>Health Check Interval: <span>0.5</span> Minutes</div> <div> Unhealthy Threshold: <span>2</span> </div> <div> Healthy Threshold: <span>10</span> </div> </div> <div> <p>Time to wait when receiving a response from the health check (2 sec - 60 sec).</p> <p>Amount of time between health checks (0.1 min - 5 min)</p> <p>Number of consecutive health check failures before declaring an EC2 instance unhealthy.</p> <p>Number of consecutive health check successes before declaring an EC2 instance healthy.</p> </div> <div> <div>Back</div> <div>Continue</div> </div> </div> </div>



## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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.


**Create a New Load Balancer** Cancel

DEFINE LOAD BALANCER ☒ CONFIGURE HEALTH CHECK ☒ ADD EC2 INSTANCES ☐ REVIEW


You will need to select a Subnet for each Availability Zone where you wish to have load balanced instances. A Virtual Network Interface will be placed inside the Subnet and allow traffic to be routed into that Availability Zone. Only one subnet per Availability Zone may be selected.

VPC: vpc-a117ebc0

**Available Subnets**

Subnet ID	Subnet CIDR	Availability Zones
 subnet-a617ebc7	10.0.1.0/24	us-east-1a

**Selected Subnets\***

Subnet ID	Subnet CIDR	Availability Zones
 subnet-aa17ebcb	10.0.0.0/24	us-east-1a

[Back](#) [Continue](#) \* Required field

Assign the Web Access Security Group to the Amazon Elastic Load Balancer.

**Create a New Load Balancer** Cancel

DEFINE LOAD BALANCER ☒ CONFIGURE HEALTH CHECK ☒ ADD EC2 INSTANCES ☐ REVIEW

You have selected the option of having your Elastic Load Balancer inside of a VPC, which allows you to assign security groups to your load balancer. Please select the security groups to assign to this load balancer. This can be changed at any time. Hold down Shift or Control (Command on Mac) to select more than one security group.

☐ Choose from your existing Security Groups

☒ Create a new Security Group

Group Name: ENTM Elastic LB

Group Description: Elastic LB Security Group

Inbound Rules

Create a new rule: Custom TCP rule

Port range:

Source:   
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

[Add Rule](#)

TCP Port (Service)	Source	Action
80 (HTTP)	0.0.0.0/0	Delete
443 (HTTPS)	0.0.0.0/0	Delete

[Back](#) [Continue](#)

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

Add the ENTM Server instance to the load balancer.

**Create a New Load Balancer** Cancel

DEFINE LOAD BALANCER CONFIGURE HEALTH CHECK **ADD EC2 INSTANCES** REVIEW

The table below lists all your running EC2 Instances that are not already behind another load balancer or part of an auto-scaling capacity group. Check the boxes in the Select column to add those instances to this load balancer.

**Manually Add Instances to Load Balancer:**

Select	Instance	Name	State	Security Groups	Availability Zone	VPC ID
<input type="checkbox"/>	i-1ce45878	Apache Reverse Proxy	running	Web	us-east-1a	vpc-a117ebc0
<input type="checkbox"/>	i-06355c63	MSSQL Server	running	MSSQL	us-east-1a	vpc-a117ebc0
<input type="checkbox"/>	i-60345d05	JumpBox	running	JumpBox	us-east-1a	vpc-a117ebc0
<input type="checkbox"/>	i-886aadeb	VPC NAT	running	default	us-east-1a	vpc-a117ebc0
<input checked="" type="checkbox"/>	i-d2c69db1	ENTM	running	ENTM	us-east-1a	vpc-a117ebc0

[select all](#) | [select none](#)

**Availability Zone Distribution:**  
1 instances in us-east-1a

[< Back](#) [Continue](#)

Click the Create button to create the new load balancer.

**Create a New Load Balancer**

DEFINE LOAD BALANCER CONFIGURE HEALTH CHECK ADD EC2 INSTANCES **REVIEW**

**DEFINE LOAD BALANCER**

**Load Balancer Name:** ENTM-LB  
**Scheme:** internet-facing  
**Port Configuration:**  
 80 (HTTP) forwarding to 80 (HTTP)  
 443 (HTTPS, Certificate: ENTM) forwarding to 443 (HTTPS)  
[Edit Load Balancer](#)

**CONFIGURE HEALTH CHECK**

**Ping Target:** HTTPS:18443  
**Timeout:** 10  
**Interval:** 0.5  
**Unhealthy Threshold:**  
**Healthy Threshold:**  
[Edit Health Check](#)

**ADD EC2 INSTANCES**

**EC2 Instances:** i-d2c69db1  
[Edit EC2 Instance](#)

**VPC INFORMATION**

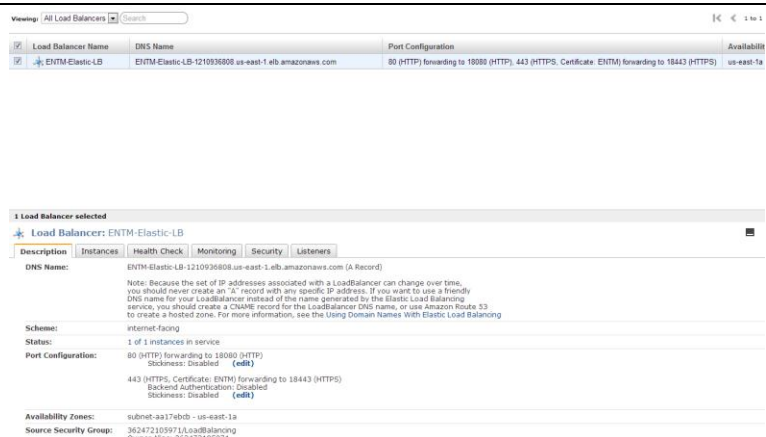
**VPC:** vpc-a117ebc0  
**Subnets:** subnet-aa17ebcb

[< Back](#) [Create](#)

Please review your selections.  
 Clicking "Create" will launch your  
 Check the Amazon EC2 product  
[balancer pricing info](#)

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

The newly created load balancer will be displayed in the list.



Viewing: All Load Balancers

Load Balancer Name	DNS Name	Port Configuration	Availability
ENTM-Elastic-LB	ENTM-Elastic-LB-1210936808-us-east-1.elb.amazonaws.com	80 (HTTP) forwarding to 18080 (HTTP), 443 (HTTPS, Certificate: ENTM) forwarding to 18443 (HTTPS)	us-east-1a

1 Load Balancer selected

Load Balancer: ENTM-Elastic-LB

Description | Instances | Health Check | Monitoring | Security | Listeners

DNS Name: ENTM-Elastic-LB-1210936808-us-east-1.elb.amazonaws.com (A Record)

Note: Because the set of IP addresses associated with a LoadBalancer can change over time, you should never create an "A" record with any specific IP address. If you want to use a friendly DNS name for your LoadBalancer instead of the name generated by the Elastic Load Balancing service, you should create a CNAME record for the LoadBalancer DNS name, or use Amazon Route 53 to create a hosted zone. For more information, see the Using Domain Names With Elastic Load Balancing

Scheme: internet-facing

Status: 1 of 1 instances in service

Port Configuration: 80 (HTTP) forwarding to 18080 (HTTP), 443 (HTTPS, Certificate: ENTM) forwarding to 18443 (HTTPS)

Backend Authentication: Disabled

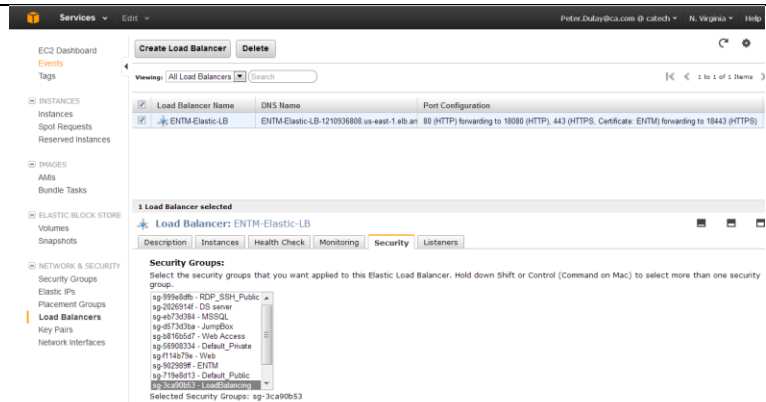
Availability Zones: subnet-aa17ebdb - us-east-1a

Source Security Groups: sg-3ca90b53

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.



Services | Edit | Peter.Dulay@ca.com | N. Virginia | Help

EC2 Dashboard | Events | Tags

INSTANCES | INSTANCES | Spot Requests | Reserved Instances

IMAGES | AMIs | Bundle Tasks

ELASTIC BLOCK STORE | Volumes | Snapshots

NETWORK & SECURITY | Security Groups | Elastic IPs | Placement Groups | Load Balancers | Key Pairs | Network Interfaces

Create Load Balancer | Delete

Viewing: All Load Balancers

Load Balancer Name	DNS Name	Port Configuration
ENTM-Elastic-LB	ENTM-Elastic-LB-1210936808-us-east-1.elb.amazonaws.com	80 (HTTP) forwarding to 18080 (HTTP), 443 (HTTPS, Certificate: ENTM) forwarding to 18443 (HTTPS)

1 Load Balancer selected

Load Balancer: ENTM-Elastic-LB

Description | Instances | Health Check | Monitoring | Security | Listeners

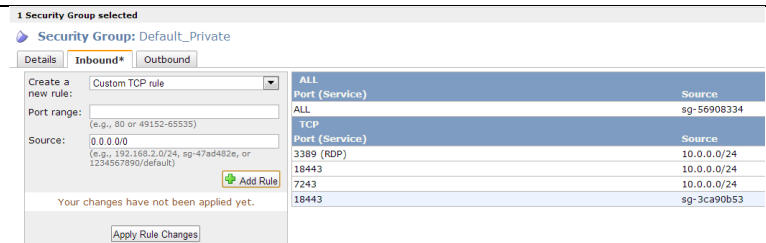
Security Groups: select the security groups that you want applied to this Elastic Load Balancer. Hold down Shift or Control (Command on Mac) to select more than one security group.

- sg-9f86a0b6 - RDP\_SSH\_Public
- sg-2626914f - DS server
- sg-a673d584 - MSSQL
- sg-df73d58a - JumpBox
- sg-a816d567 - Web Access
- sg-5690b334 - Default\_Private
- sg-f14b79e - Web
- sg-9d2989f - ENTM
- sg-716ed013 - Default\_Public
- sg-3ca90b53 - ENTM-Elastic-LB

Selected Security Groups: sg-3ca90b53

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.



1 Security Group selected

Security Group: Default\_Private

Details | Inbound\* | Outbound

Create a new rule: Custom TCP rule

Port range: (e.g., 80 or 49152-65535)

Source: 0.0.0.0/0 (e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

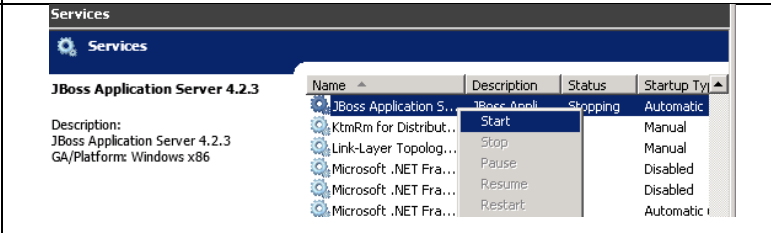
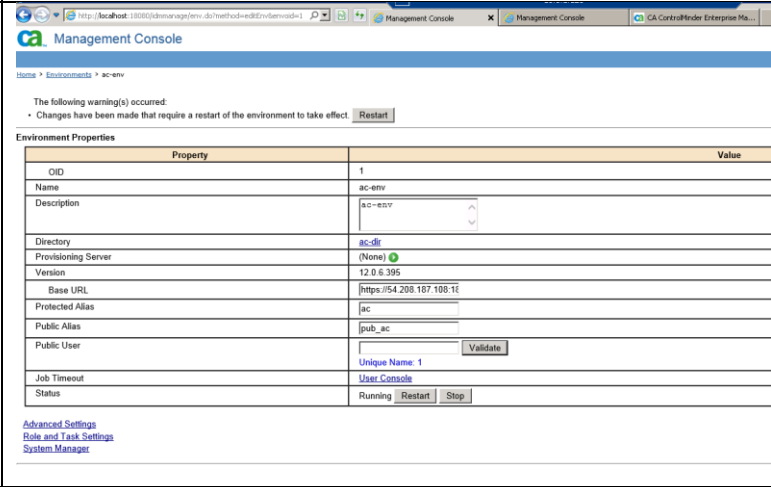
Add Rule

Your changes have not been applied yet.

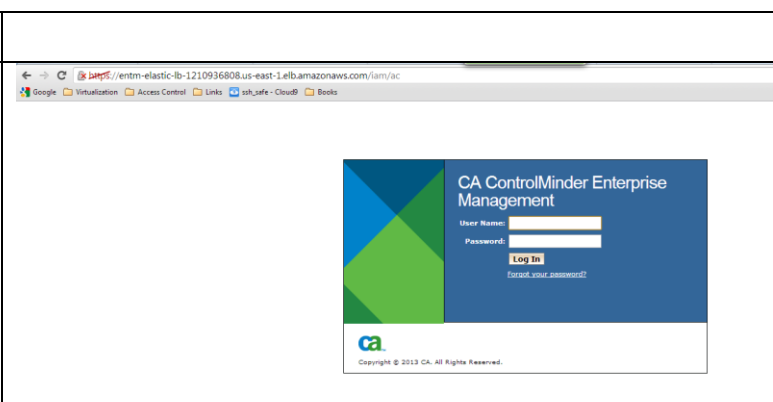
Apply Rule Changes

ALL	Port (Service)	Source
ALL	Port (Service)	sg-5690b334
TCP	Port (Service)	Source
3389 (RDP)	10.0.0.0/24	
18443	10.0.0.0/24	
7243	10.0.0.0/24	
18443	sg-3ca90b53	

## Configure ENTM to Use Amazon Elastic Load Balancer

<p>Enable the idmmanage URL on the ENTM server:</p> <p>Edit the following file:</p> <p>C:\jboss4.2.3.GA\server\default\deploy\IdentityMinder.ear\management_console.war\WEB-INF\Web.XML</p> <p>Change the “AccessFilter” token value to “true”</p>	<pre>&lt;filter&gt;   &lt;filter-name&gt;AccessFilter&lt;/filter-name&gt;   &lt;filter-class&gt;com.netegrity.ims.manage.filter.AccessFilter&lt;/filter-class&gt;   &lt;init-param&gt;     &lt;param-name&gt;Enable&lt;/param-name&gt;     &lt;param-value&gt;true&lt;/param-value&gt;   &lt;/init-param&gt; &lt;/filter&gt;</pre>
<p>Restart JBoss to effect the change.</p>	
<p>From your Remote Desktop session to the ENTM Server, browse to the idmmanage URL:</p> <p><a href="http://localhost:18080/idmmanage">http://localhost:18080/idmmanage</a></p> <p>Choose “Environments” -&gt; “ac-env”.</p> <p>Change the “Base URL” property to point to the public address of the Amazon Elastic Load Balancer (e.g. <a href="https://54.208.187.100/1">https://54.208.187.100/1</a> address&gt;)</p> <p>Click the Save button.</p>	
<p>Disable the idmmanage URL</p> <p>Edit the following file:</p> <p>C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\management_console.war\WEB-INF\Web.XML</p> <p>Reset the AccessFilter token value to false.</p> <p>Restart JBoss to effect the change.</p>	<pre>&lt;filter&gt;   &lt;filter-name&gt;AccessFilter&lt;/filter-name&gt;   &lt;filter-class&gt;com.netegrity.ims.manage.filter.AccessFilter&lt;/filter-class&gt;   &lt;init-param&gt;     &lt;param-name&gt;Enable&lt;/param-name&gt;     &lt;param-value&gt;false&lt;/param-value&gt;   &lt;/init-param&gt; &lt;/filter&gt;</pre>

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>You can now access Enterprise Management via the Amazon Elastic Load Balancer.</p>	
---	--

## 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).

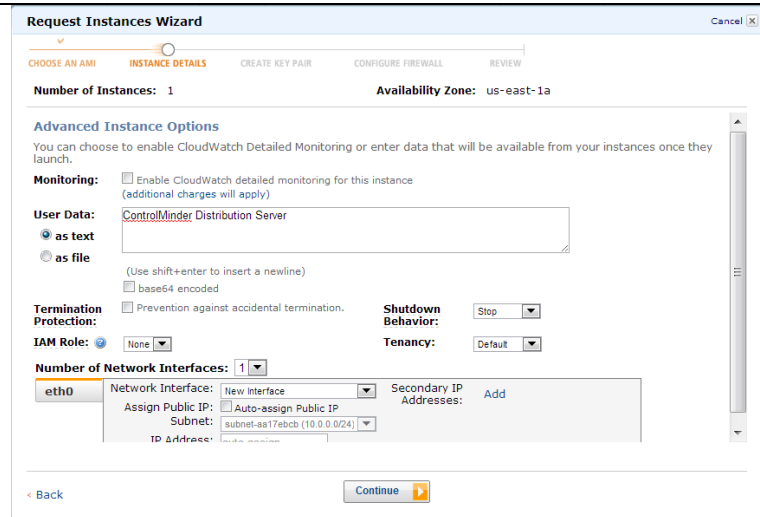
Click the Continue button.



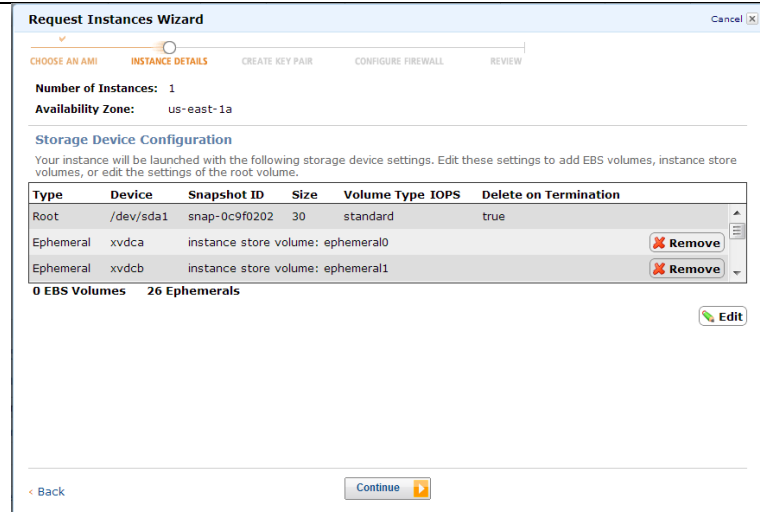
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

Provide User Data to identify your instance.

Click the Continue button.



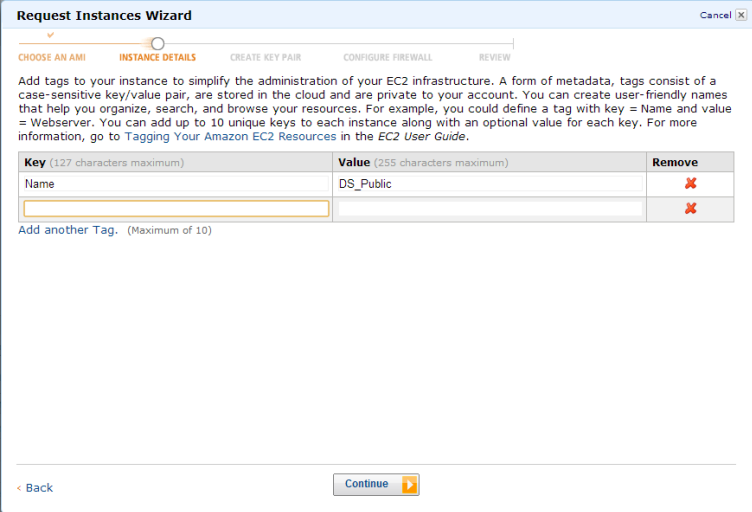

Keep the default storage configuration.  
30 gigabytes of disk storage is sufficient for the Distribution server.



Type	Device	Snapshot ID	Size	Volume Type	IOPS	Delete on Termination
Root	/dev/sda1	snap-0c9f0202	30	standard		true
Ephemeral	xvda	instance store volume: ephemeral0				
Ephemeral	xvdc	instance store volume: ephemeral1				

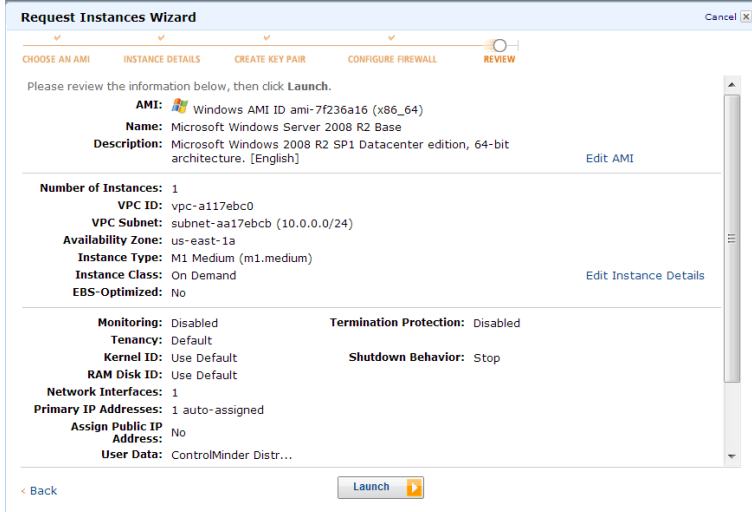
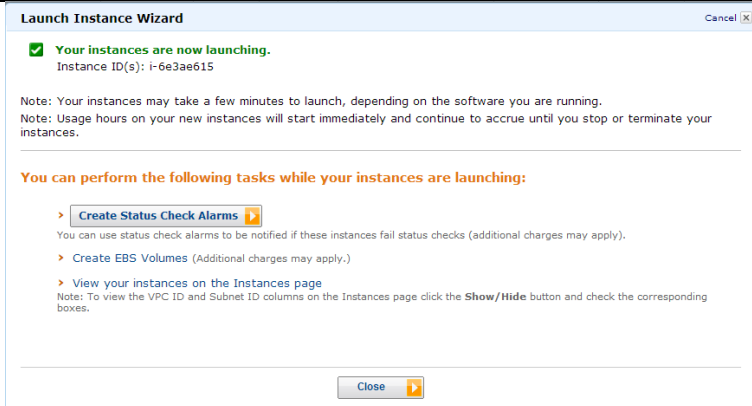
0 EBS Volumes    26 Ephemerals

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

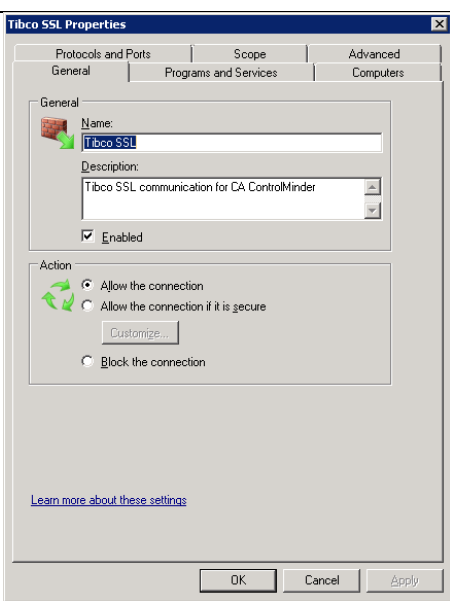
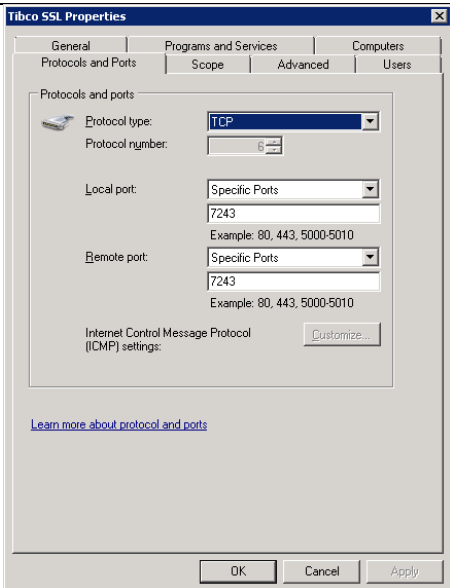


## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Click the Launch button.</p>	
<p>Click the Close button.</p>	

## Prepare to Install the Distribution Server

### Tibco Communication Configuration

<p>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).</p>	
	

## 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 |



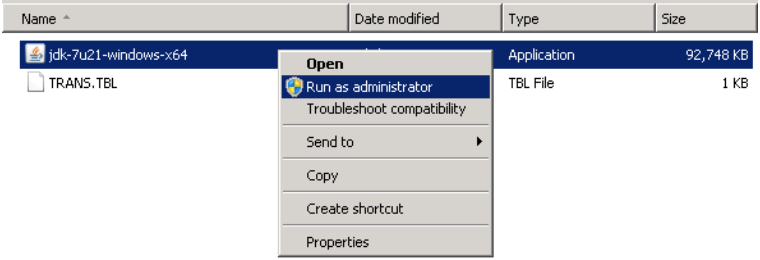
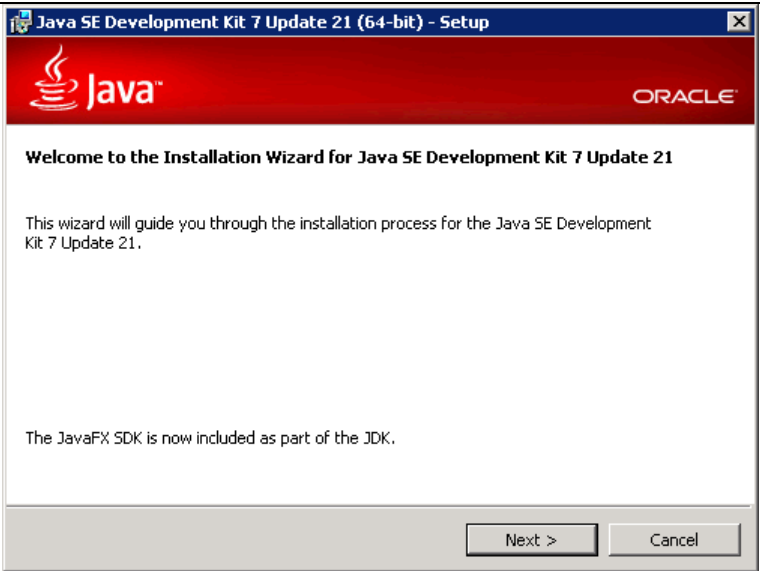
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

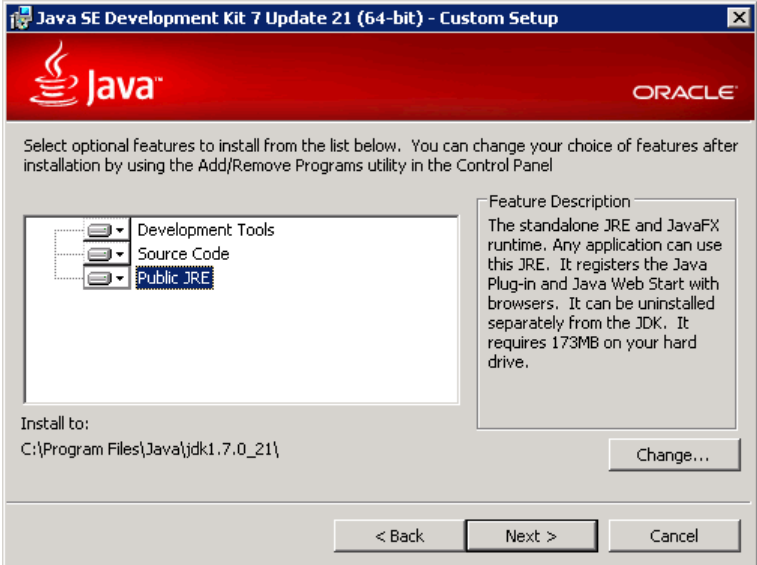
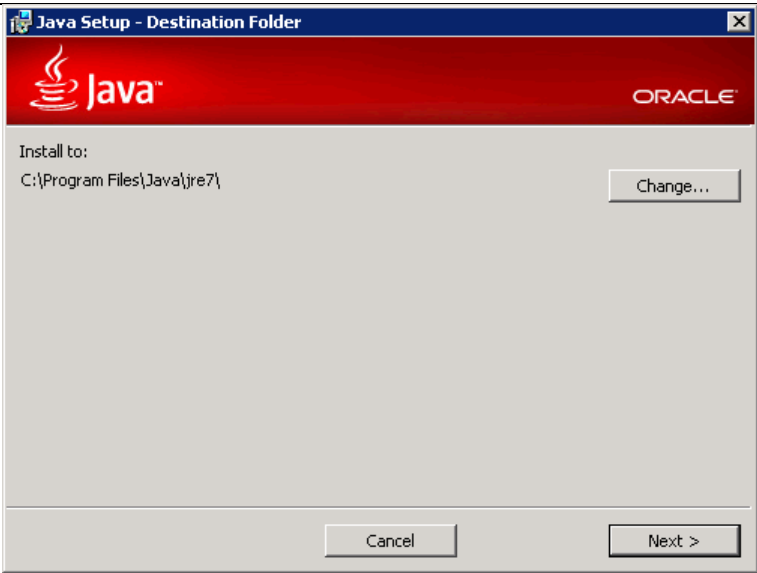
### Install Third-Party Components

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

<p>Locate the Java SDK installer, <b>jdk-7u21-windows-x64.exe</b>, from the JDK-1.7.21\_x64 directory on the DVD drive.</p> <p>Right click <b>jdk-7u21-windows-x64.exe</b> and choose <u>R</u>un as administrator.</p>	
<p>Click the Next button to start the Java SDK installation.</p>	

<p>Click the Next button.</p>	
<p>Click the Next button.</p>	

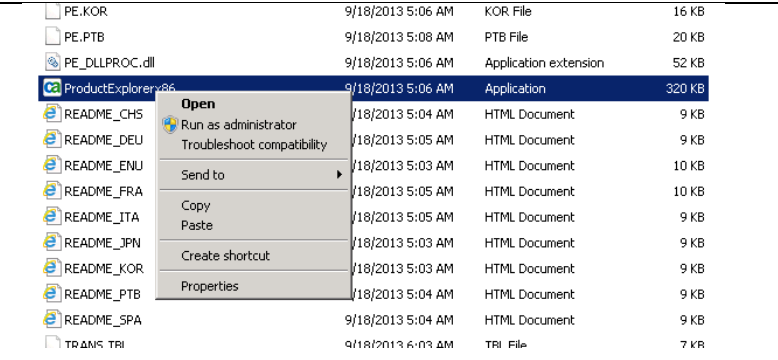
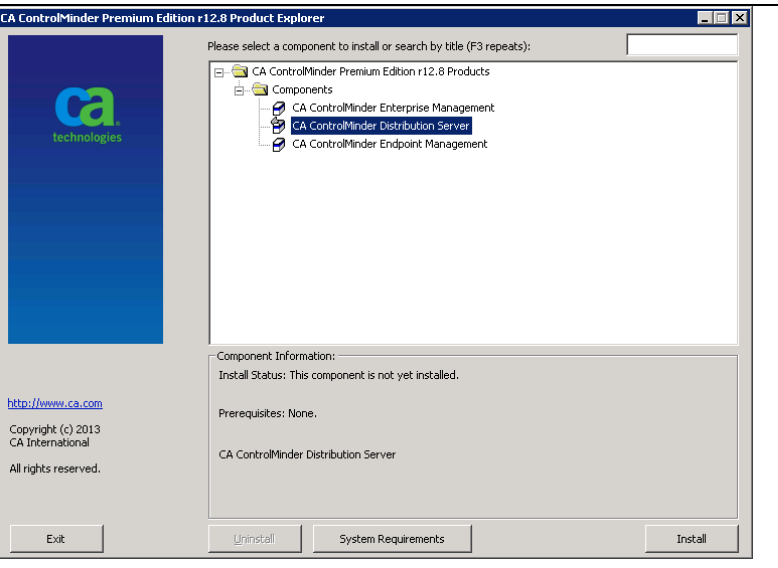


## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

### Install the Distribution Server

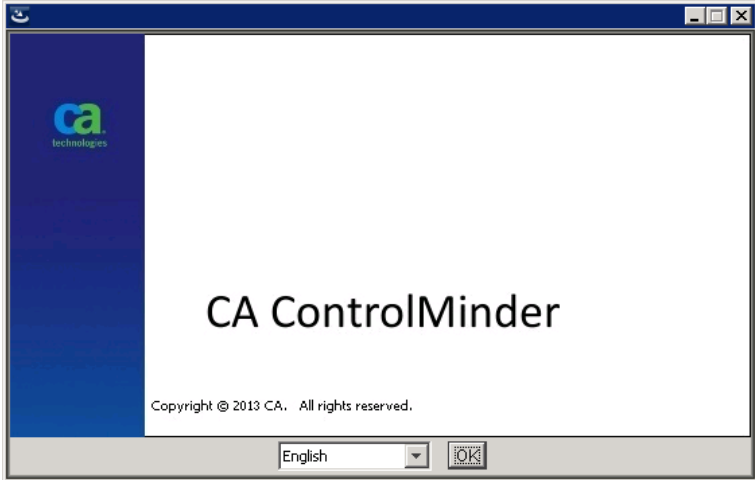
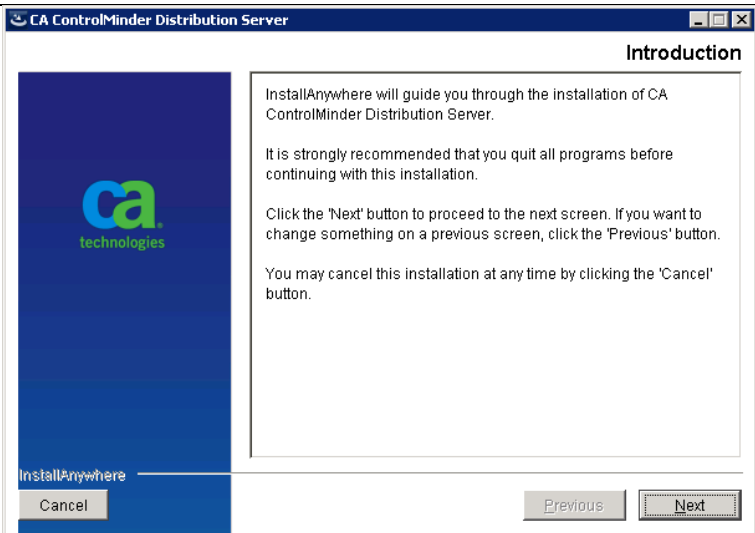
Mount the CA ControlMinder Server Components ISO image in the virtual DVD drive.

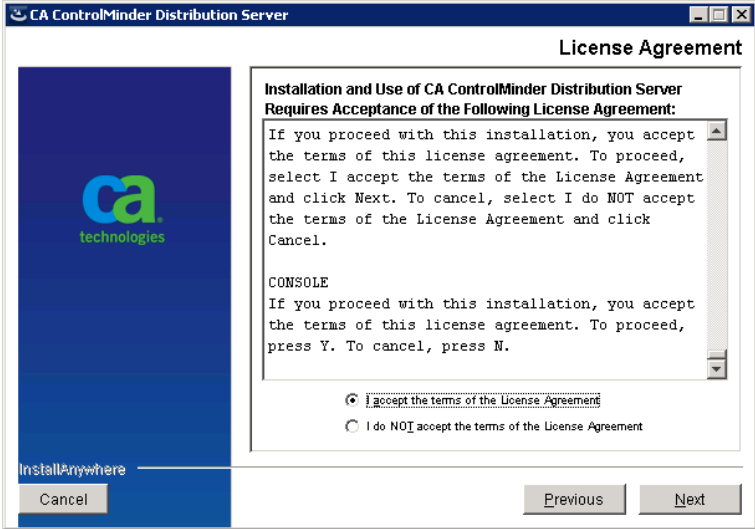
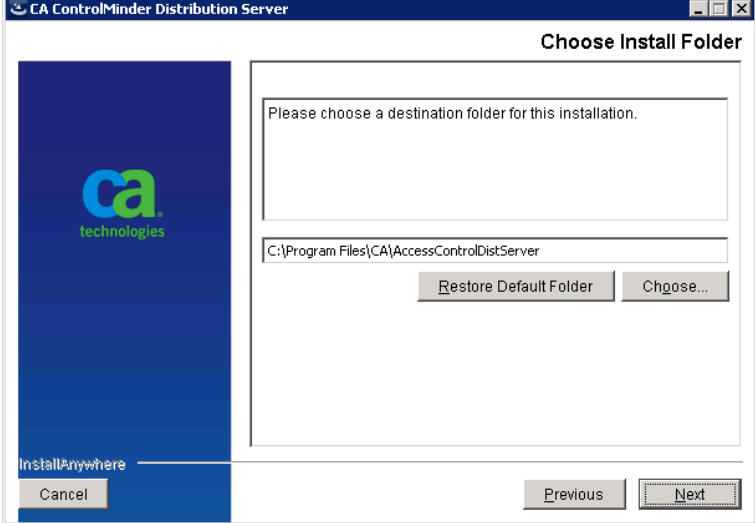
Important: Do not use a UNC path or remote share to specify the software location.

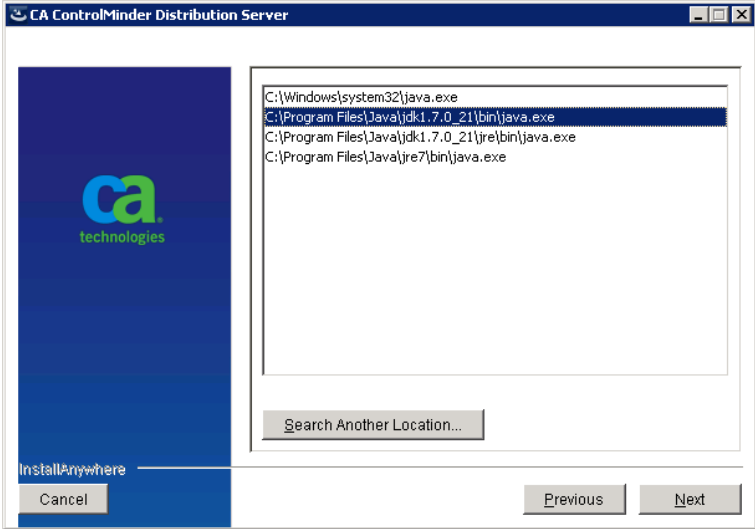
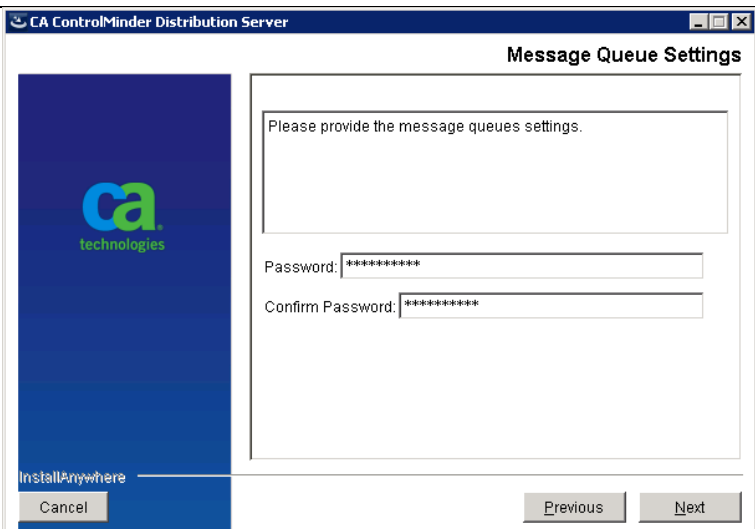
<p>Start the Distribution Server installation by launching <b>ProductExplorer</b> from the virtual DVD drive.</p> <p>Remember to start <b>ProductExplorer</b> by right-clicking the executable and choosing <u>Run as administrator</u>.</p>	
<p>From the Components folder of <b>ProductExplorer</b>, select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

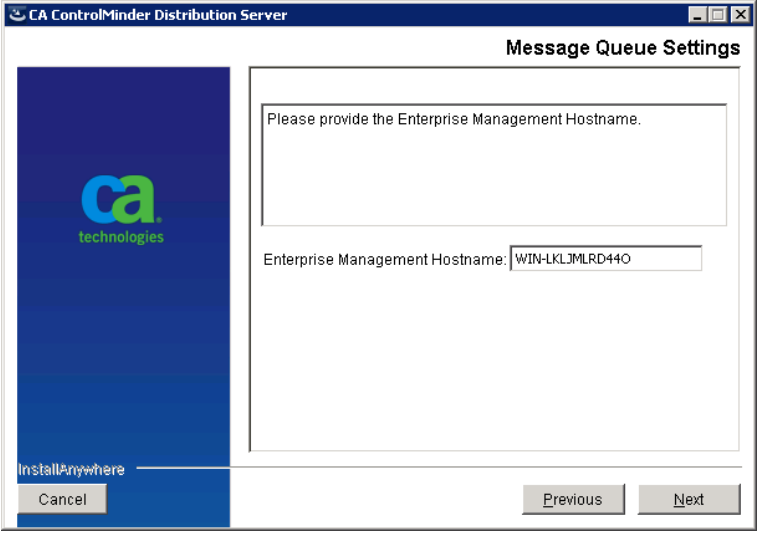
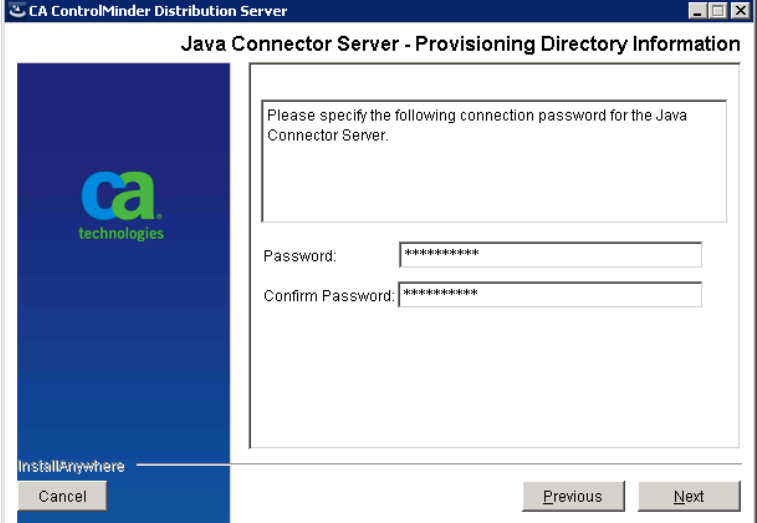


## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

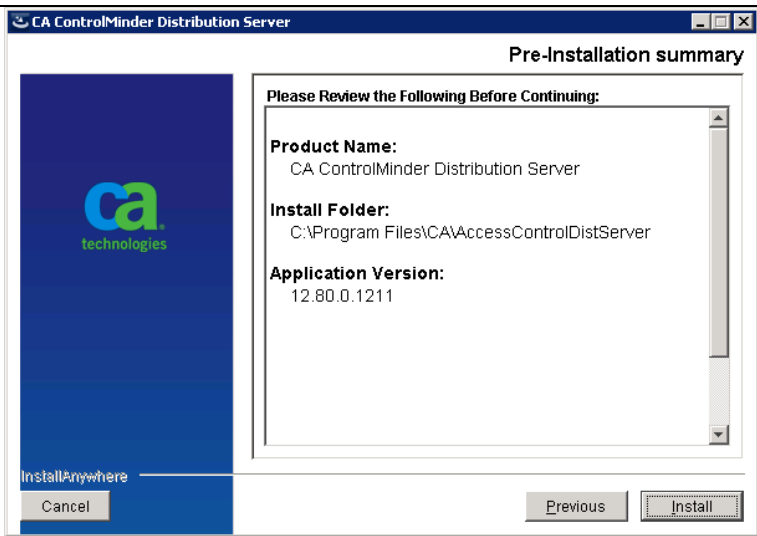
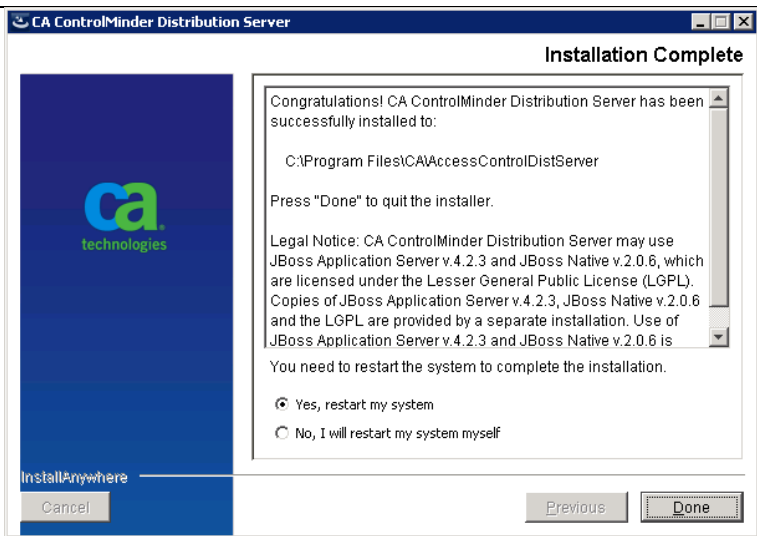
<p>Click the OK button to accept English as the language for the installation.</p>	
<p>Click the Next button.</p>	

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

<p>Select the location where you previously installed the Java JDK from the Third-Party Components ISO image.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'CA ControlMinder Distribution Server' window. On the left is the CA Technologies logo and the text 'InstallAnywhere'. On the right, a list of Java executables is displayed: 'C:\Windows\system32\java.exe', 'C:\Program Files\Java\jdk1.7.0_21\bin\java.exe' (which is highlighted), 'C:\Program Files\Java\jdk1.7.0_21\jre\bin\java.exe', and 'C:\Program Files\Java\jre7\bin\java.exe'. Below the list is a 'Search Another Location...' button. At the bottom right are 'Previous' and 'Next' buttons.</p>
<p>Provide the message queue password.</p> <p>This is the communication password you specified during the ENTM Server installation.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'CA ControlMinder Distribution Server' window with the title 'Message Queue Settings'. It prompts the user to 'Please provide the message queues settings.' Below this, there are two password fields: 'Password: *****' and 'Confirm Password: *****'. At the bottom right are 'Previous' and 'Next' buttons.</p>

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

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Click the Install button.</p>	 <p>The screenshot shows the 'Pre-Installation summary' window of the CA ControlMinder Distribution Server installer. The window has a blue sidebar with the CA Technologies logo and the text 'InstallAnywhere'. The main area is titled 'Pre-Installation summary' and contains a scrollable list box with the following information:</p> <ul style="list-style-type: none"> <li><b>Please Review the Following Before Continuing:</b></li> <li><b>Product Name:</b> CA ControlMinder Distribution Server</li> <li><b>Install Folder:</b> C:\Program Files\CA\AccessControlDistServer</li> <li><b>Application Version:</b> 12.80.0.1211</li> </ul> <p>At the bottom of the window, there are three buttons: 'Cancel', 'Previous', and 'Install'.</p>
<p>After the installation successfully completes, click the Done button to reboot the server and finalize the installation.</p>	 <p>The screenshot shows the 'Installation Complete' window of the CA ControlMinder Distribution Server installer. The window has a blue sidebar with the CA Technologies logo and the text 'InstallAnywhere'. The main area is titled 'Installation Complete' and contains a scrollable list box with the following information:</p> <ul style="list-style-type: none"> <li><b>Congratulations!</b> CA ControlMinder Distribution Server has been successfully installed to:</li> <li>C:\Program Files\CA\AccessControlDistServer</li> <li>Press "Done" to quit the installer.</li> <li><b>Legal Notice:</b> CA ControlMinder Distribution Server may use JBoss Application Server v.4.2.3 and JBoss Native v.2.0.6, which are licensed under the Lesser General Public License (LGPL). Copies of JBoss Application Server v.4.2.3, JBoss Native v.2.0.6 and the LGPL are provided by a separate installation. Use of JBoss Application Server v.4.2.3 and JBoss Native v.2.0.6 is</li> <li>You need to restart the system to complete the installation.</li> </ul> <p>At the bottom of the window, there are three buttons: 'Cancel', 'Previous', and 'Done'. There are also two radio buttons for system restart options:</p> <ul style="list-style-type: none"> <li><input checked="" type="radio"/> Yes, restart my system</li> <li><input type="radio"/> No, I will restart my system myself</li> </ul>

## **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 or 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.

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

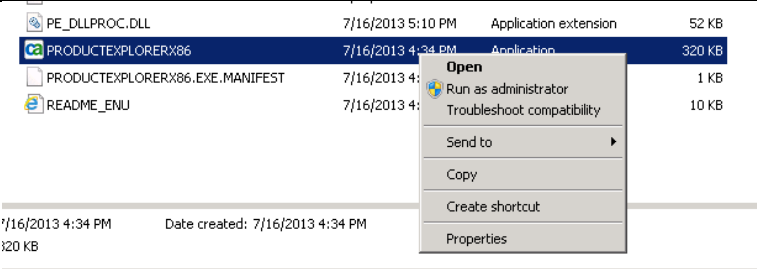
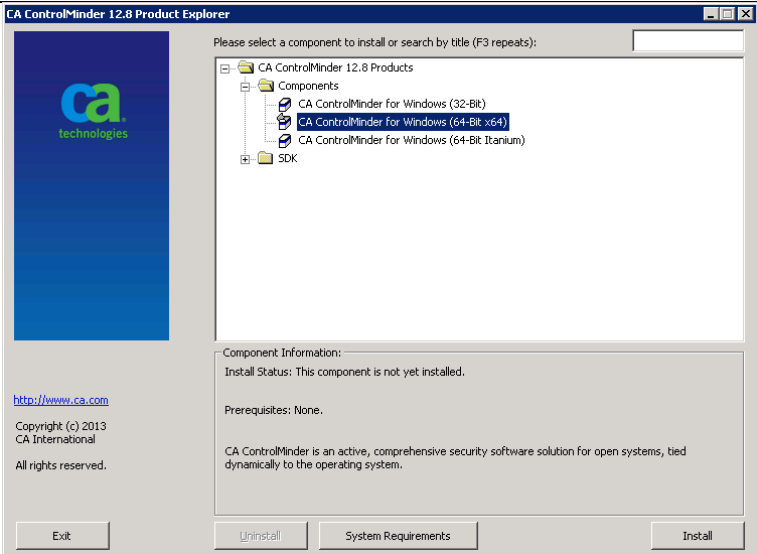
### Microsoft Windows Installation

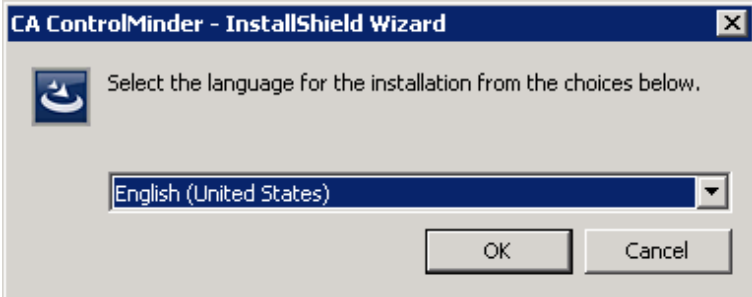
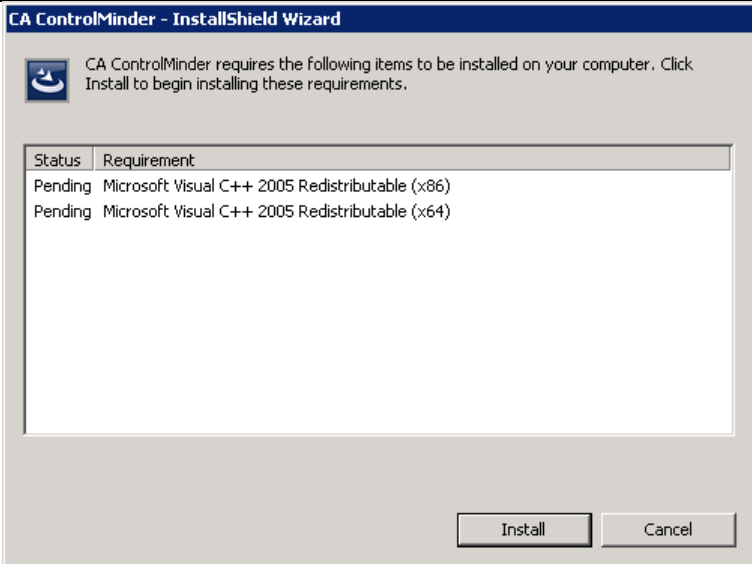
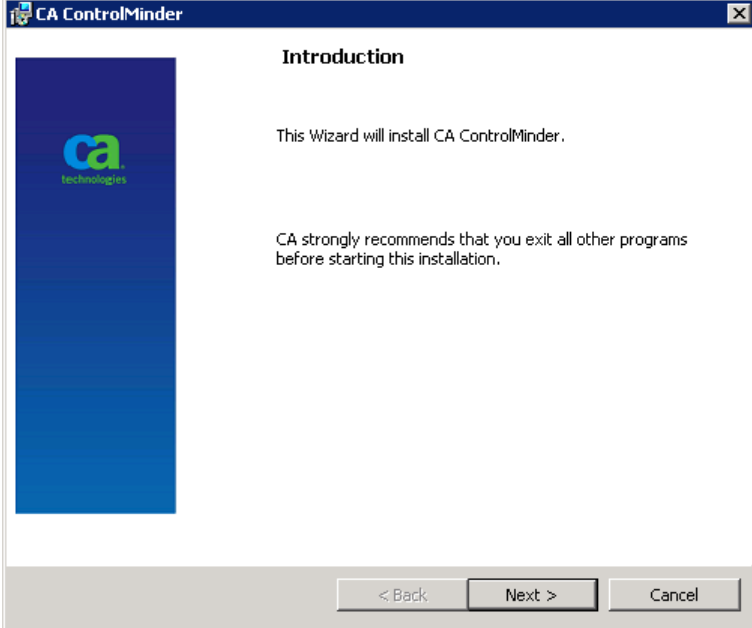
Transfer the CA ControlMinder Endpoint software to the instance.

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.

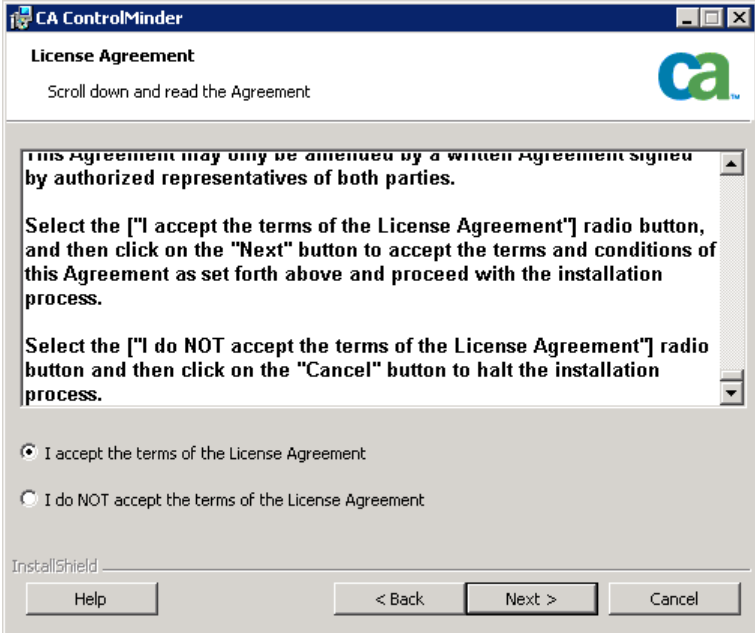
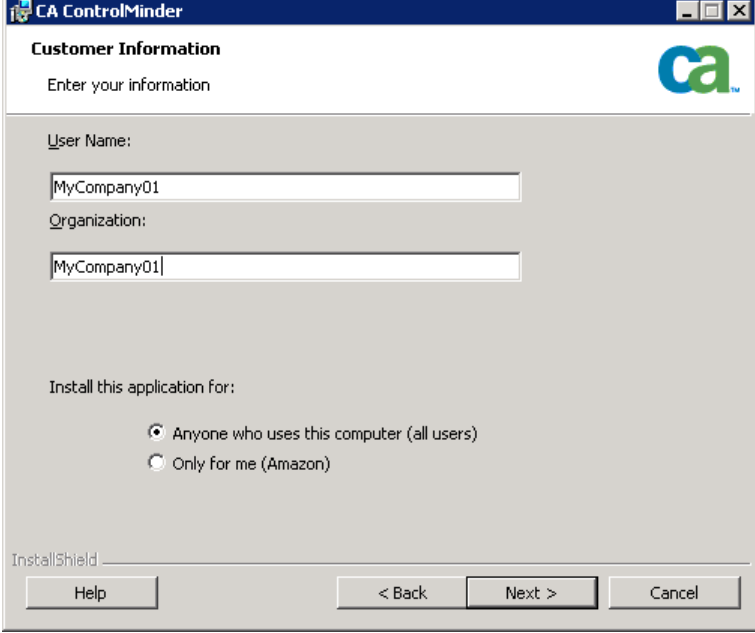
The following example leverages a graphical user interface (GUI) to install the endpoint software. Silent installation is available to facilitate unattended installation. Refer to the Implementation Guide for additional information.

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

<p>Select the language for the installation and click the OK button.</p>							
<p>If prompted to install Microsoft Visual C++ Redistributable libraries, click the Install button.</p>	 <table border="1" data-bbox="683 751 1388 1039"> <thead> <tr> <th>Status</th><th>Requirement</th></tr> </thead> <tbody> <tr> <td>Pending</td><td>Microsoft Visual C++ 2005 Redistributable (x86)</td></tr> <tr> <td>Pending</td><td>Microsoft Visual C++ 2005 Redistributable (x64)</td></tr> </tbody> </table>	Status	Requirement	Pending	Microsoft Visual C++ 2005 Redistributable (x86)	Pending	Microsoft Visual C++ 2005 Redistributable (x64)
Status	Requirement						
Pending	Microsoft Visual C++ 2005 Redistributable (x86)						
Pending	Microsoft Visual C++ 2005 Redistributable (x64)						
<p>Click the Next button to proceed with the ControlMinder endpoint software installation.</p>							



## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

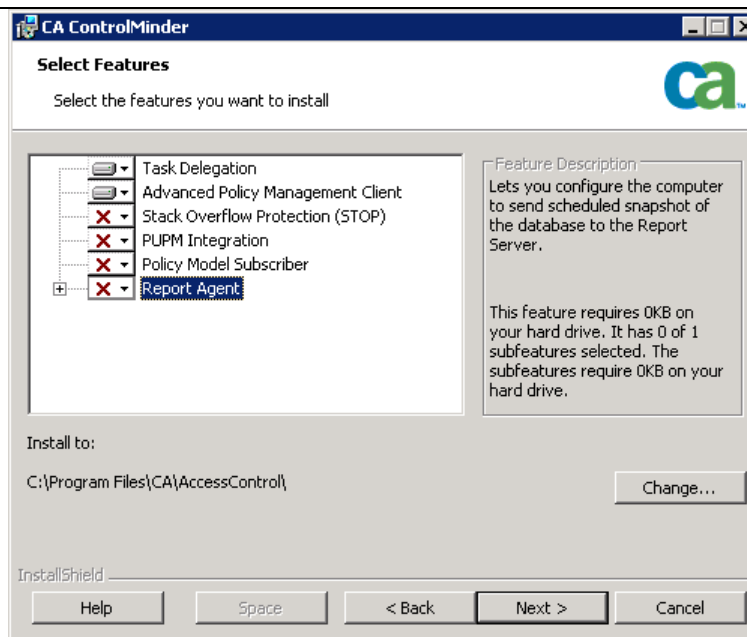
<p>Read the License Agreement as you use the scrollbar to advance through the document.</p> <p>Click the radial button noting <u>I accept the terms of the License Agreement</u>.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'License Agreement' window of the CA ControlMinder installer. It contains a scrollable text area with the following text: 'This Agreement may only be amended by a written Agreement signed by authorized representatives of both parties. Select the ["I accept the terms of the License Agreement"] radio button, and then click on the "Next" button to accept the terms and conditions of this Agreement as set forth above and proceed with the installation process. Select the ["I do NOT accept the terms of the License Agreement"] radio button and then click on the "Cancel" button to halt the installation process.' Below the text are two radio buttons: 'I accept the terms of the License Agreement' (which is selected) and 'I do NOT accept the terms of the License Agreement'. At the bottom are buttons for 'Help', '&lt; Back', 'Next &gt;', and 'Cancel'.</p>
<p>Provide customer information.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'Customer Information' window of the CA ControlMinder installer. It prompts the user to 'Enter your information'. There are two text input fields: 'User Name:' with the value 'MyCompany01' and 'Organization:' with the value 'MyCompany01'. Below these is a section 'Install this application for:' with two radio buttons: 'Anyone who uses this computer (all users)' (which is selected) and 'Only for me (Amazon)'. At the bottom are buttons for 'Help', '&lt; Back', 'Next &gt;', and 'Cancel'.</p>

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

Select the installation directory and the components to be installed.

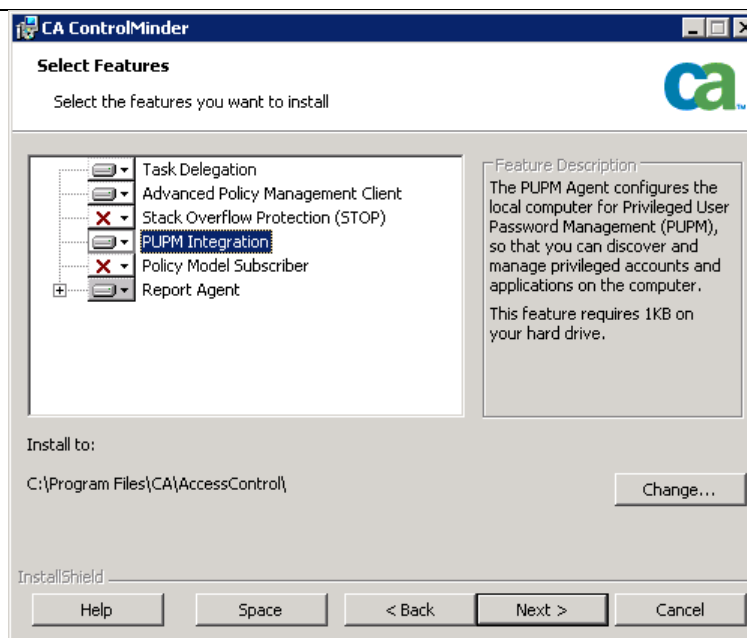
Add “PUPM Integration” and “Report Agent” out of those no selected by default.

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.



## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

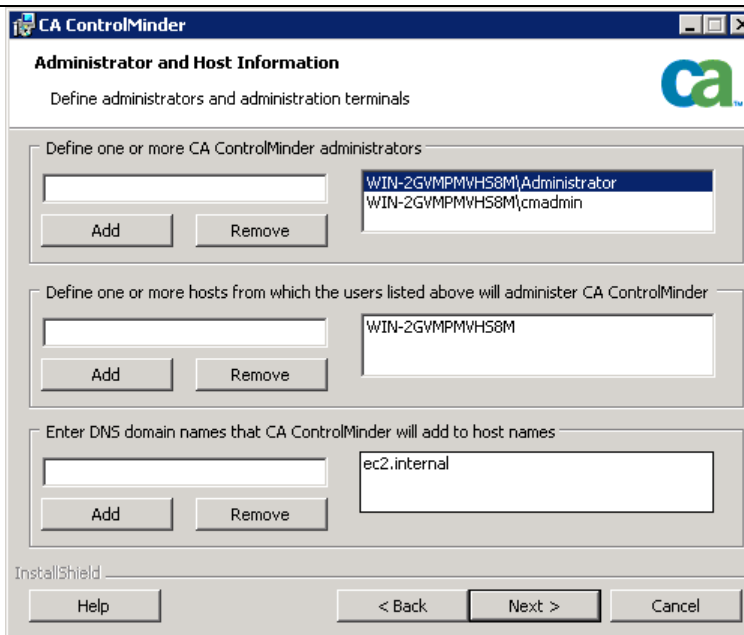
Provide the names of the ControlMinder administrators.

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.



**CA ControlMinder**

**Administrator and Host Information**

Define administrators and administration terminals

Define one or more CA ControlMinder administrators

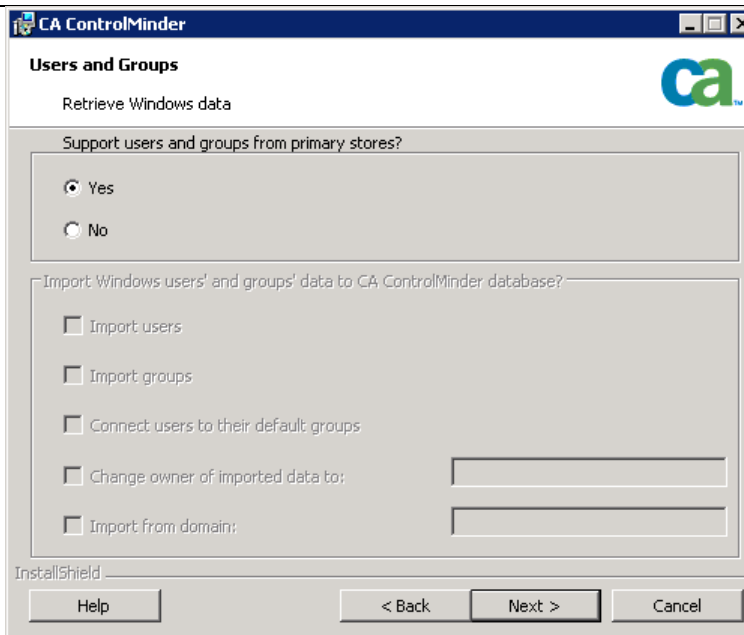
Define one or more hosts from which the users listed above will administer CA ControlMinder

Enter DNS domain names that CA ControlMinder will add to host names

InstallShield

Unless there is a specific need to do otherwise, accept the default of selecting the radial button for Yes to Support users and groups from primary stores. This allows ControlMinder to recognize users from the native environment.

Click the Next button.



**CA ControlMinder**

**Users and Groups**

Retrieve Windows data

Support users and groups from primary stores?

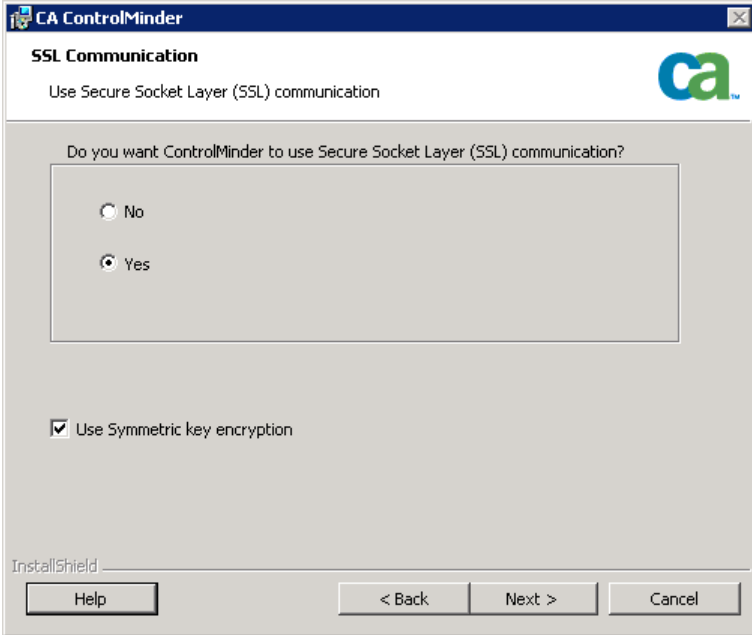
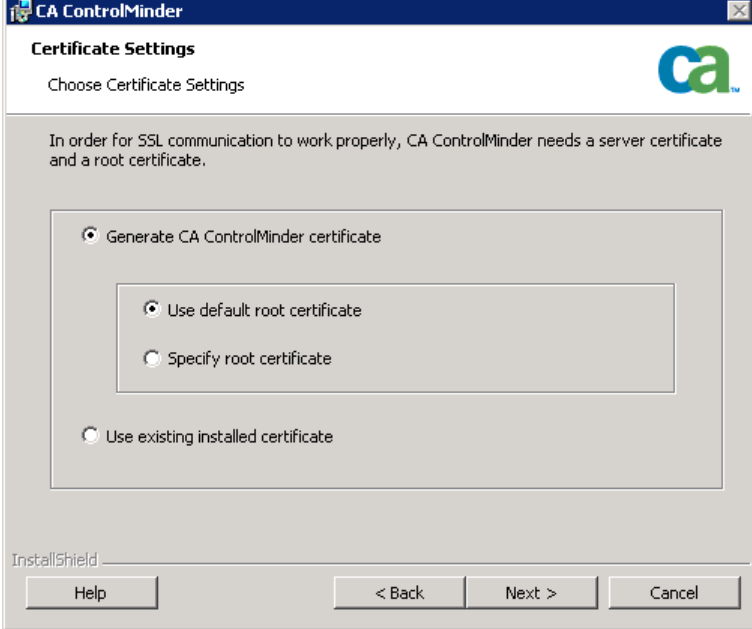
☒ Yes  
☐ No

Import Windows users' and groups' data to CA ControlMinder database?

☐ Import users  
☐ Import groups  
☐ Connect users to their default groups  
☐ Change owner of imported data to:   
☐ Import from domain:

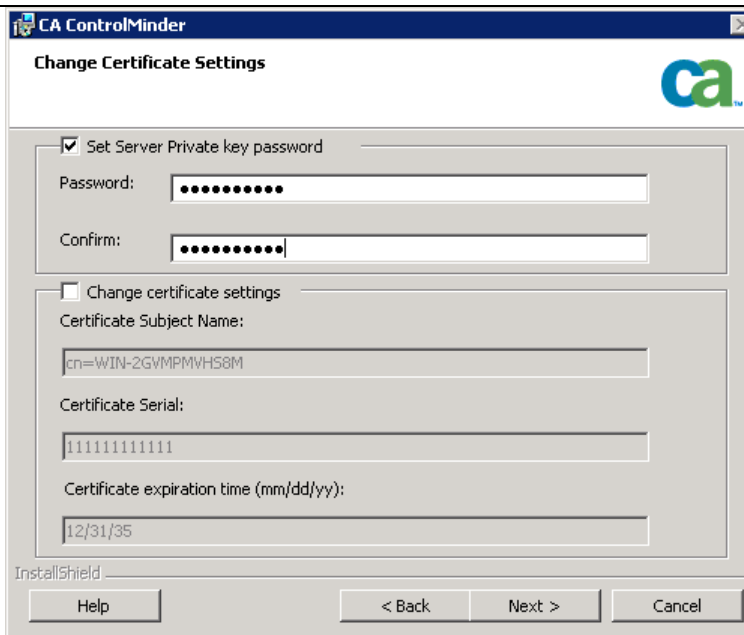
InstallShield

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

Provide the password of the certificate's private key.

Click the Next button.



**CA ControlMinder**

**Change Certificate Settings**

☒ Set Server Private key password

Password:

Confirm:

☐ Change certificate settings

Certificate Subject Name:

Certificate Serial:

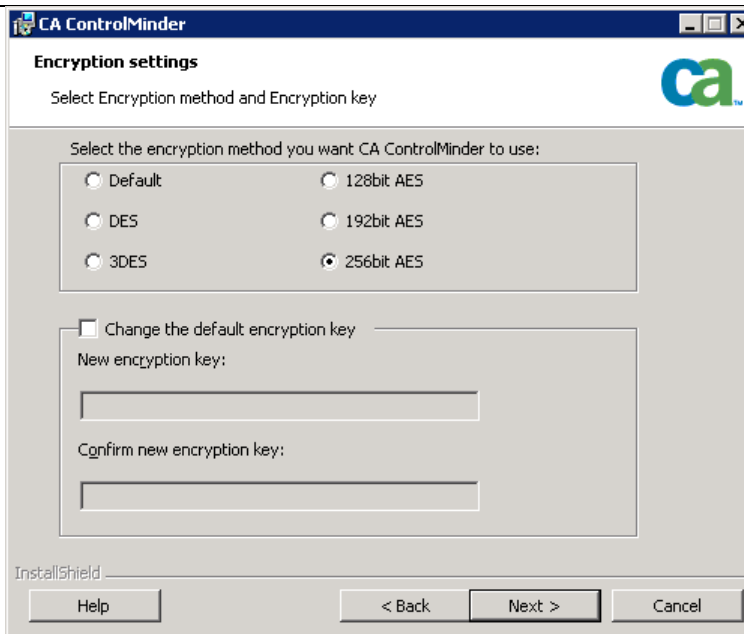
Certificate expiration time (mm/dd/yy):

InstallShield

Help < Back Next > Cancel

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.



**CA ControlMinder**

**Encryption settings**

Select Encryption method and Encryption key

Select the encryption method you want CA ControlMinder to use:

☐ Default ☐ 128bit AES

☐ DES ☐ 192bit AES

☐ 3DES ☒ 256bit AES

☐ Change the default encryption key

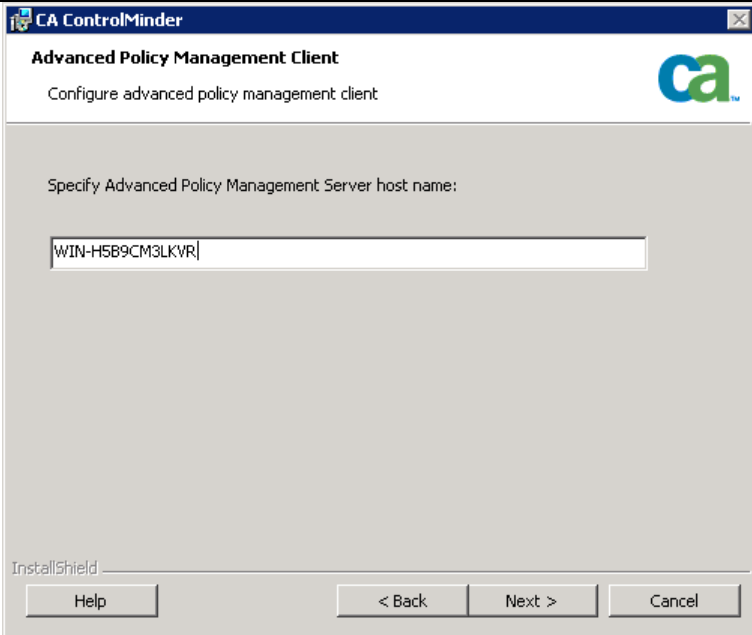
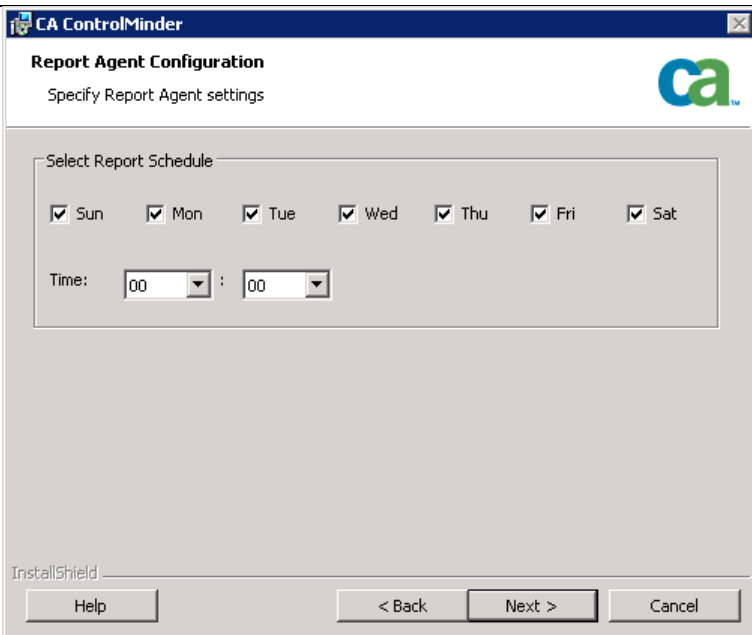
New encryption key:

Confirm new encryption key:

InstallShield

Help < Back Next > Cancel

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Provide the hostname of the Distribution Server.</p> <p>All communication between the endpoint and the ENTM Server flows through the Distribution Server.</p> <p>The endpoint must be able to resolve the hostname of the Distribution Server.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'CA ControlMinder Advanced Policy Management Client' window. The title bar says 'CA ControlMinder'. The main title is 'Advanced Policy Management Client' with a subtitle 'Configure advanced policy management client'. There is a text input field labeled 'Specify Advanced Policy Management Server host name:' containing the text 'WIN-H5B9CM3LKVR'. At the bottom, there are buttons for 'Help', '&lt; Back', 'Next &gt;', and 'Cancel'.</p>
<p>Specify when the Report Agent sends snapshots of the endpoint's ControlMinder database to the ENTM Server (via the Distribution Server).</p> <p>The snapshot data are used for reporting purposes.</p> <p>Click the Next button.</p>	 <p>The screenshot shows the 'CA ControlMinder Report Agent Configuration' window. The title bar says 'CA ControlMinder'. The main title is 'Report Agent Configuration' with a subtitle 'Specify Report Agent settings'. Under the heading 'Select Report Schedule', there are checkboxes for days of the week: Sun, Mon, Tue, Wed, Thu, Fri, and Sat, all of which are checked. Below this is a 'Time:' field with two dropdown menus, both set to '00'. At the bottom, there are buttons for 'Help', '&lt; Back', 'Next &gt;', and 'Cancel'.</p>

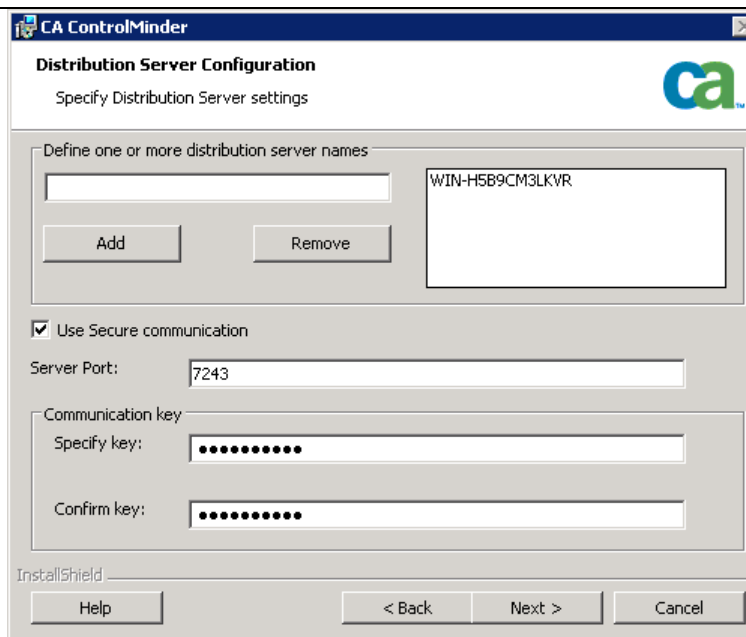
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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.



**CA ControlMinder**  
Distribution Server Configuration  
Specify Distribution Server settings

Define one or more distribution server names

WIN-H5B9CM3LKVR

Add Remove

☒ Use Secure communication

Server Port: 7243

Communication key

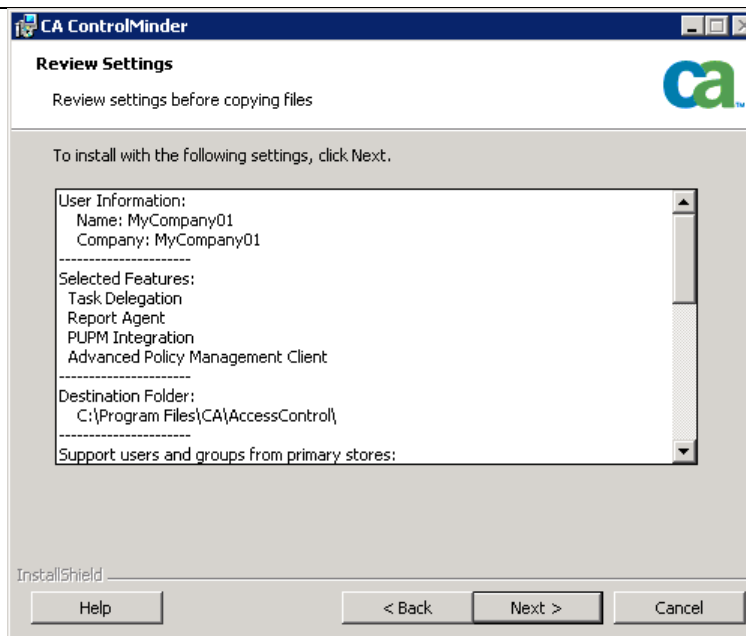
Specify key: .....

Confirm key: .....

InstallShield

Help < Back Next > Cancel

Review the installation parameters and click the Next button.



**CA ControlMinder**  
Review Settings  
Review settings before copying files

To install with the following settings, click Next.

User Information:  
Name: MyCompany01  
Company: MyCompany01

Selected Features:  
Task Delegation  
Report Agent  
PUPM Integration  
Advanced Policy Management Client

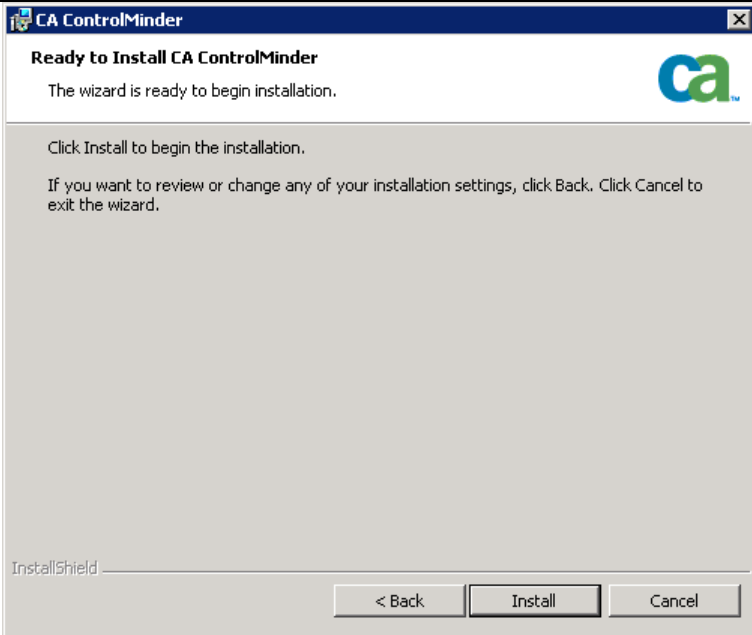
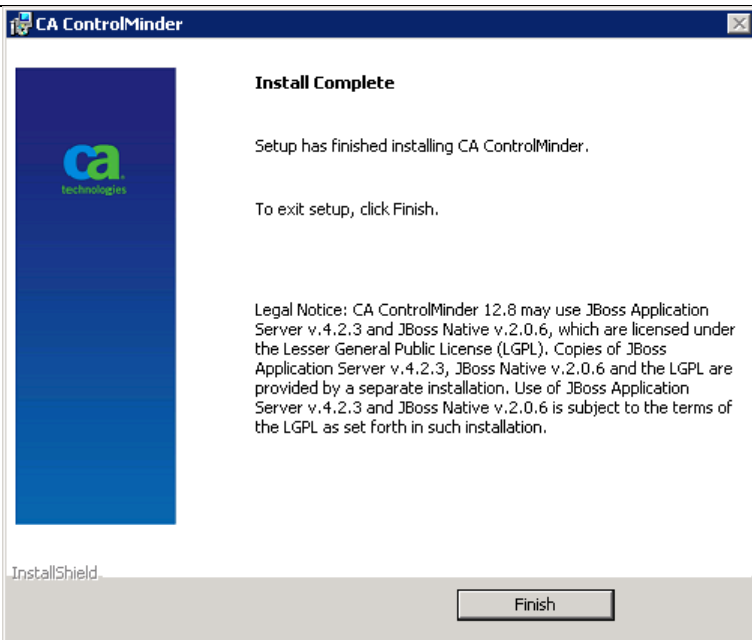
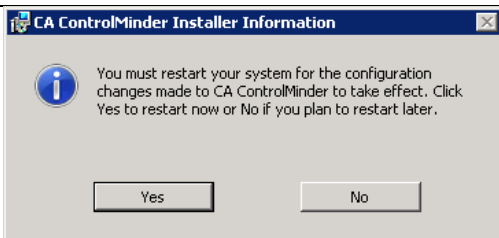
Destination Folder:  
C:\Program Files\CA\AccessControl\

Support users and groups from primary stores:

InstallShield

Help < Back Next > Cancel

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Click the Install button.</p>	 <p>The screenshot shows the 'Ready to Install CA ControlMinder' window. It contains the CA Technologies logo, a message stating 'The wizard is ready to begin installation.', and instructions to click 'Install' to begin, 'Back' to review settings, or 'Cancel' to exit. The 'Install' button is highlighted.</p>
<p>After the installation has completed, click the Finish button.</p>	 <p>The screenshot shows the 'Install Complete' window. It features the CA Technologies logo on the left and text on the right stating 'Setup has finished installing CA ControlMinder.' and 'To exit setup, click Finish.' A 'Finish' button is located at the bottom right.</p>
<p>The installation may require a reboot to load ControlMinder kernel drivers.</p> <p>Click the Yes button to reboot now or click the No button to manually reboot at a later time.</p>	 <p>The screenshot shows a dialog box titled 'CA ControlMinder Installer Information'. It contains an information icon and text stating: 'You must restart your system for the configuration changes made to CA ControlMinder to take effect. Click Yes to restart now or No if you plan to restart later.' There are 'Yes' and 'No' buttons at the bottom.</p>



## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

### 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.

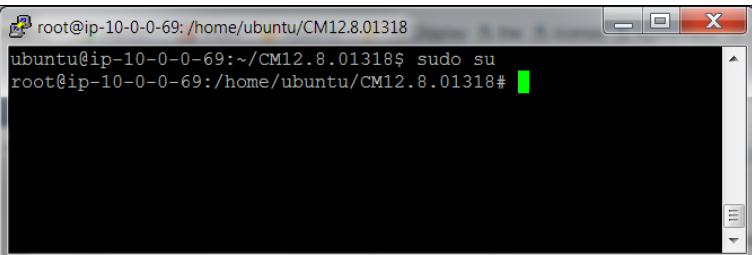
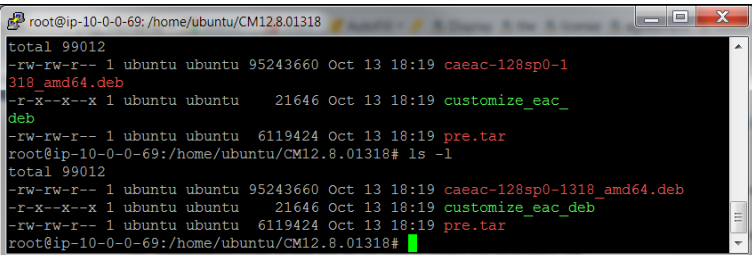
You need the following files from the CA ControlMinder UNIX Endpoint installation DVD:

- caeac-xxxspx-xxx\_amd64.deb
- customize\_eac\_deb
- pre.tar

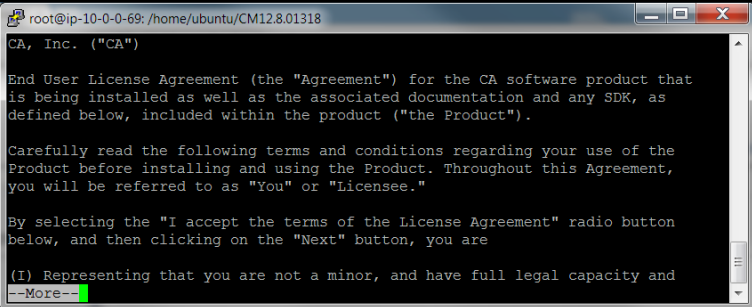
These are usually located under NativePackages\RPMPackages\DEBIAN directory.

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.

<p>Change your identity to root by running:</p> <pre>sudo su</pre>	 <pre>root@ip-10-0-0-69: /home/ubuntu/CM12.8.01318 ubuntu@ip-10-0-0-69:~/CM12.8.01318\$ sudo su root@ip-10-0-0-69: /home/ubuntu/CM12.8.01318#</pre>
<p>Change to the directory where the installation package is located.</p> <p>Make sure that customize_eac_deb is executable.</p>	 <pre>root@ip-10-0-0-69: /home/ubuntu/CM12.8.01318 total 99012 -rw-rw-r-- 1 ubuntu ubuntu 95243660 Oct 13 18:19 caeac-128sp0-1 318_amd64.deb -r-x--x--x 1 ubuntu ubuntu 21646 Oct 13 18:19 customize_eac_ deb -rw-rw-r-- 1 ubuntu ubuntu 6119424 Oct 13 18:19 pre.tar root@ip-10-0-0-69: /home/ubuntu/CM12.8.01318# ls -l total 99012 -rw-rw-r-- 1 ubuntu ubuntu 95243660 Oct 13 18:19 caeac-128sp0-1318_amd64.deb -r-x--x--x 1 ubuntu ubuntu 21646 Oct 13 18:19 customize_eac_deb -rw-rw-r-- 1 ubuntu ubuntu 6119424 Oct 13 18:19 pre.tar root@ip-10-0-0-69: /home/ubuntu/CM12.8.01318#</pre>

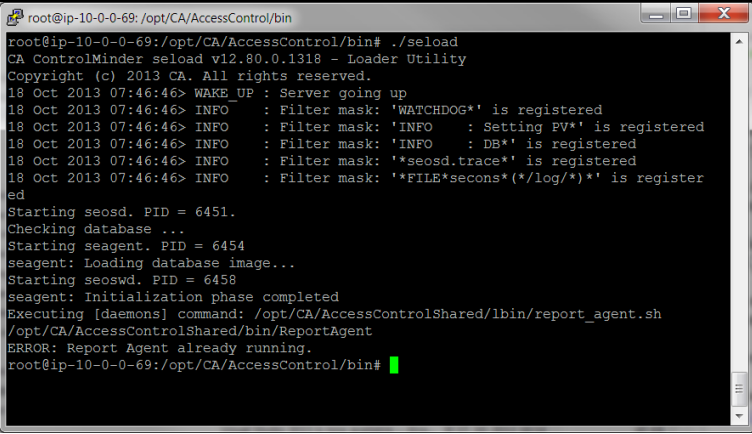
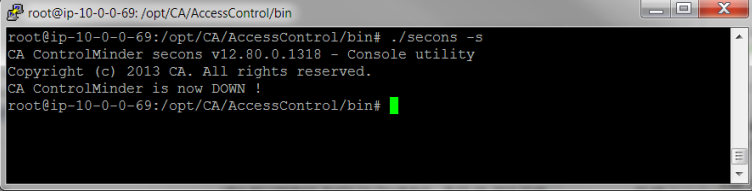
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

# CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

To configure the endpoint software for automatic startup

Navigate to:

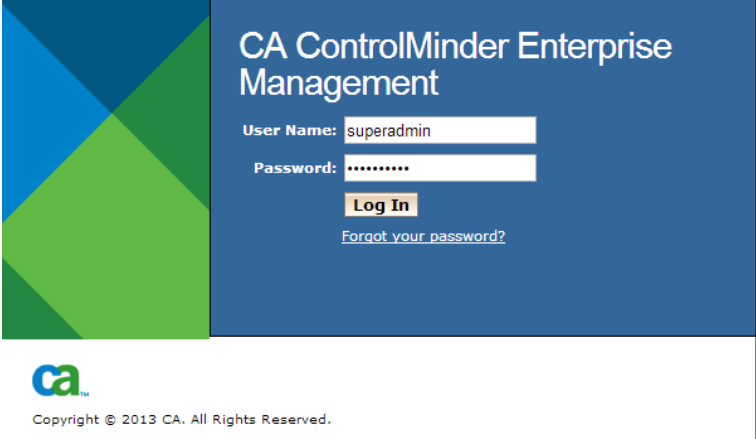
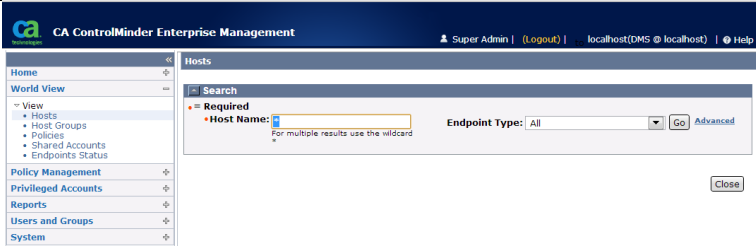
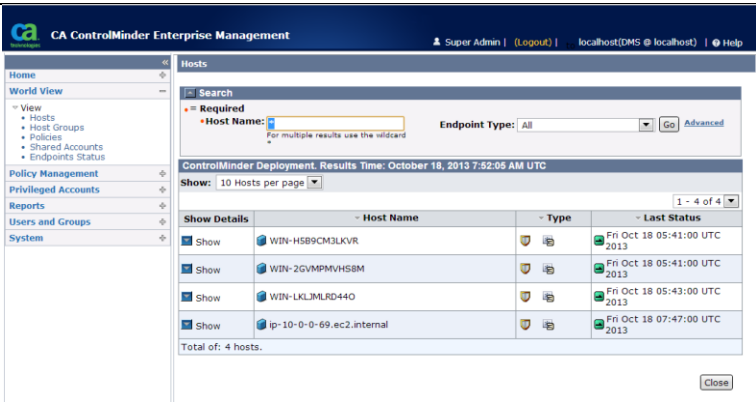
`opt/CA/AccessControl/samples/system.init/LINUX`

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.

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

### Validate Endpoint Installation

<p>Login to Enterprise Management using the superadmin account.</p> <p>NOTE: The superadmin account's password was specified when Enterprise Management was installed.</p>	 <p>The login screen for CA ControlMinder Enterprise Management. It features a blue header with the CA logo and the text 'CA ControlMinder Enterprise Management'. Below the header, there are input fields for 'User Name' (containing 'superadmin') and 'Password' (containing '*****'). A 'Log In' button is positioned below the password field, and a link for 'Forgot your password?' is located below the 'Log In' button. The footer includes the CA logo and the text 'Copyright © 2013 CA. All Rights Reserved.'</p>																				
<p>Navigate to World View -&gt; View -&gt; Hosts</p>	 <p>The 'World View' screen for Hosts in CA ControlMinder Enterprise Management. It shows a search bar with a 'Required' filter, a 'Host Name' input field, and an 'Endpoint Type' dropdown menu set to 'All'. A 'Go' button is next to the search bar. Below the search bar, there is a 'Close' button. The left sidebar contains a navigation menu with options like Home, World View, View, Hosts, Host Groups, Policies, Shared Accounts, Endpoints Status, Policy Management, Privileged Accounts, Reports, Users and Groups, and System.</p>																				
<p>Click Go to display the list of registered endpoints</p> <p>Observe that the ENTM Server, Distribution Server, and Windows and Ubuntu endpoints (on which ControlMinder endpoint software was installed) are listed.</p>	 <p>The 'Hosts' list screen in CA ControlMinder Enterprise Management. It displays a table of registered endpoints. The table has columns for 'Host Name', 'Type', and 'Last Status'. The 'Host Name' column includes icons for different operating systems (Windows, Linux, etc.) and the host names. The 'Type' column shows icons for different endpoint types. The 'Last Status' column shows the status of the endpoints and the time they were last updated. Below the table, there is a 'Total of: 4 hosts.' label and a 'Close' button.</p> <table><thead><tr><th></th><th>Host Name</th><th>Type</th><th>Last Status</th></tr></thead><tbody><tr><td>Show</td><td>WIN-HSB9CM3UKVR</td><td>Windows</td><td>Fri Oct 18 05:41:00 UTC 2013</td></tr><tr><td>Show</td><td>WIN-2GVMPMVH8SM</td><td>Windows</td><td>Fri Oct 18 05:41:00 UTC 2013</td></tr><tr><td>Show</td><td>WIN-LKLMLRD440</td><td>Windows</td><td>Fri Oct 18 05:43:00 UTC 2013</td></tr><tr><td>Show</td><td>ip-10-0-0-69.ec2.internal</td><td>Linux</td><td>Fri Oct 18 07:47:00 UTC 2013</td></tr></tbody></table>		Host Name	Type	Last Status	Show	WIN-HSB9CM3UKVR	Windows	Fri Oct 18 05:41:00 UTC 2013	Show	WIN-2GVMPMVH8SM	Windows	Fri Oct 18 05:41:00 UTC 2013	Show	WIN-LKLMLRD440	Windows	Fri Oct 18 05:43:00 UTC 2013	Show	ip-10-0-0-69.ec2.internal	Linux	Fri Oct 18 07:47:00 UTC 2013
	Host Name	Type	Last Status																		
Show	WIN-HSB9CM3UKVR	Windows	Fri Oct 18 05:41:00 UTC 2013																		
Show	WIN-2GVMPMVH8SM	Windows	Fri Oct 18 05:41:00 UTC 2013																		
Show	WIN-LKLMLRD440	Windows	Fri Oct 18 05:43:00 UTC 2013																		
Show	ip-10-0-0-69.ec2.internal	Linux	Fri Oct 18 07:47:00 UTC 2013																		

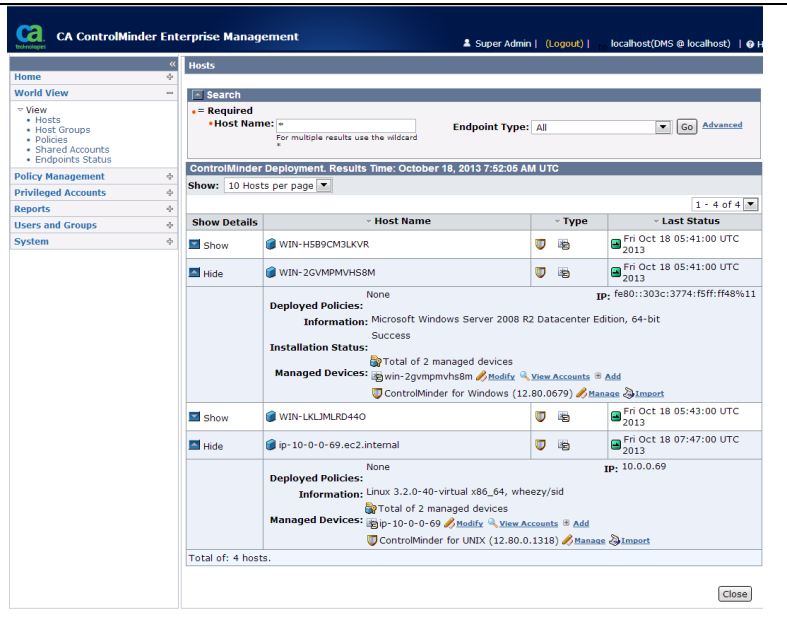
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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.



The screenshot displays the CA ControlMinder Enterprise Management web interface. The left sidebar contains navigation links: Home, World View, View (with sub-links for Hosts, Host Groups, Policies, Shared Accounts, and Endpoints Status), Policy Management, Privileged Accounts, Reports, Users and Groups, and System. The main content area is titled 'Hosts' and includes a search bar with a 'Required' filter and an 'Endpoint Type' dropdown set to 'All'. Below the search bar, a deployment results summary for October 18, 2013, at 7:52:05 AM UTC is shown, indicating 10 hosts per page. A table lists four hosts with columns for Show/Hide, Host Name, Type, and Last Status. The first two hosts are Windows-based (WIN-HSB9CM3LKVR and WIN-2GVMPMVH58M), and the last two are Linux-based (WIN-LKLJMLRD440 and ip-10-0-0-69.ec2.internal). Each host entry has a detailed view section showing deployed policies, information, installation status, and managed devices. The 'Managed Devices' section for each host lists 'ControlMinder for Windows' and 'ControlMinder for UNIX' with their respective versions and management links.

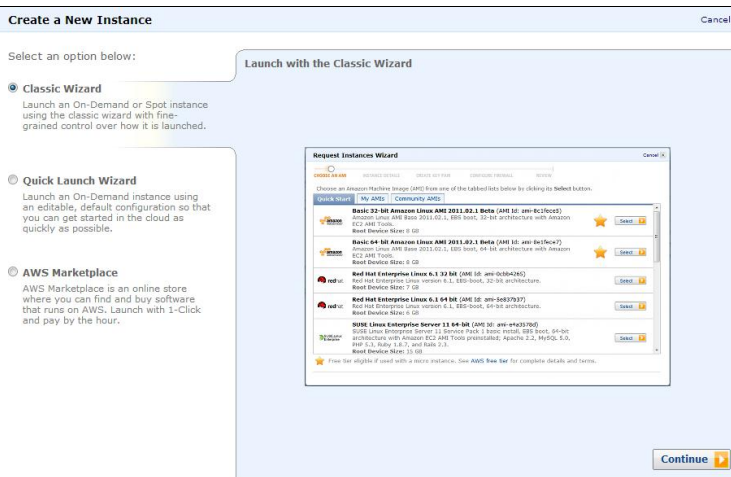
Show/Hide	Host Name	Type	Last Status
Show	WIN-HSB9CM3LKVR	Windows	Fri Oct 18 05:41:00 UTC 2013
Hide	WIN-2GVMPMVH58M	Windows	Fri Oct 18 05:41:00 UTC 2013
Show	WIN-LKLJMLRD440	Linux	Fri Oct 18 05:43:00 UTC 2013
Hide	ip-10-0-0-69.ec2.internal	Linux	Fri Oct 18 07:47:00 UTC 2013

## Appendix A – Configure Apache Reverse Proxy Server

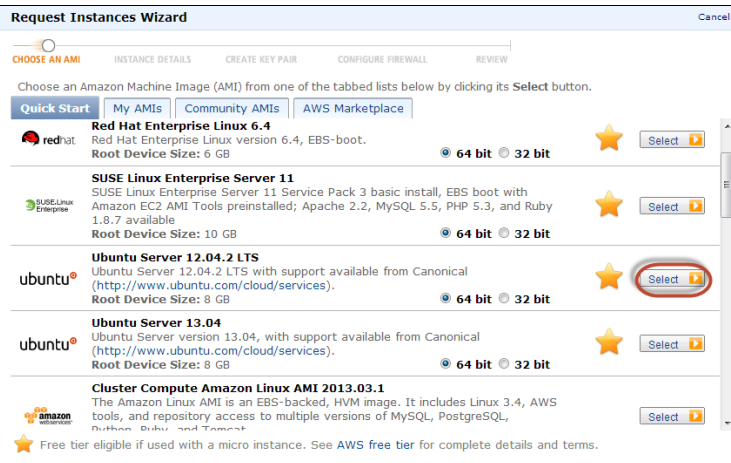
Apache Reverse Proxy is only needed in case Amazon Elastic Load Balancing is not used!  
The reverse proxy will allow HTTP/HTTPS traffic from the internet to the ENTM Server running in the private zone.

### 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.

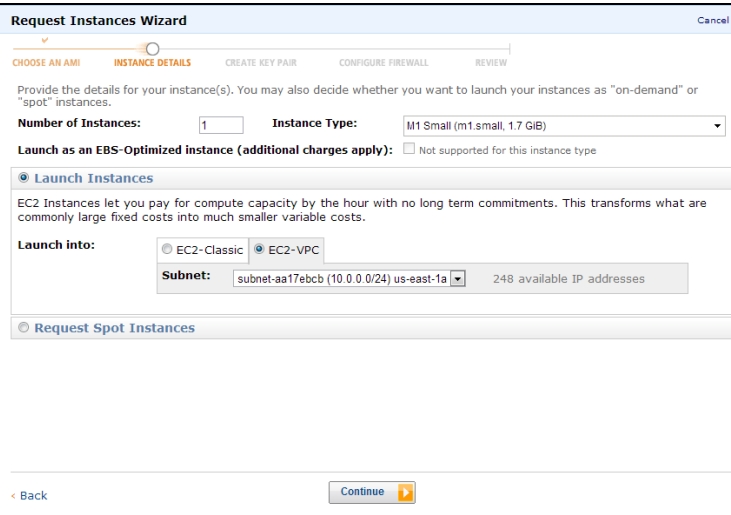


## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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).

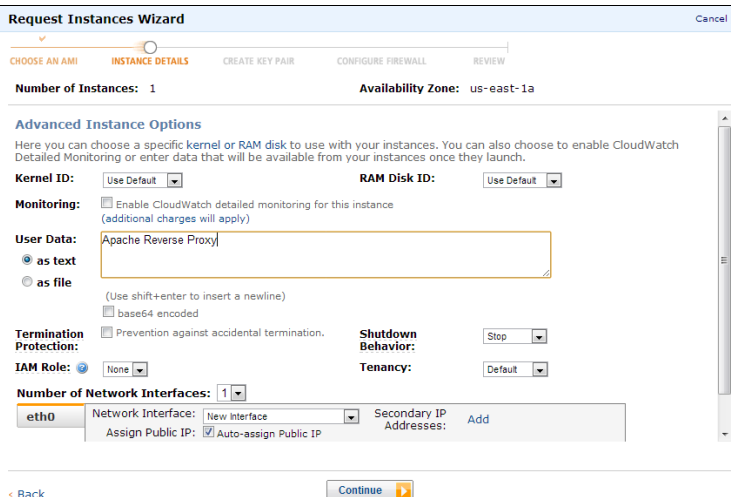
Click the Continue button.



Provide User Data to identify your instance.

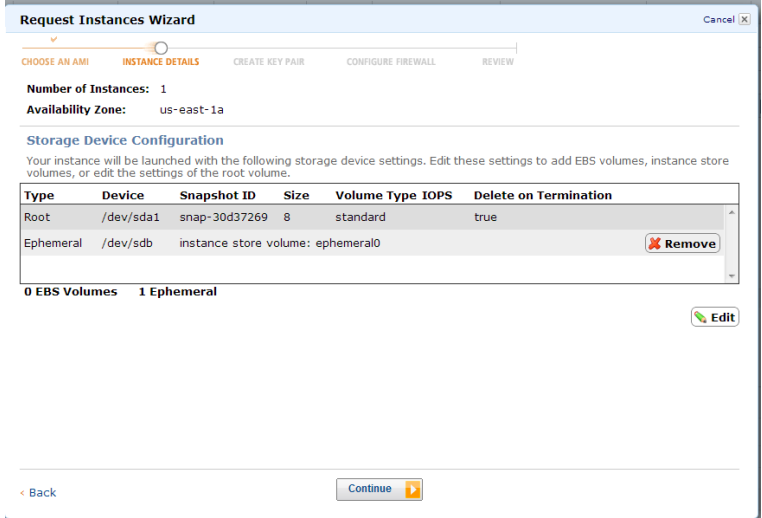
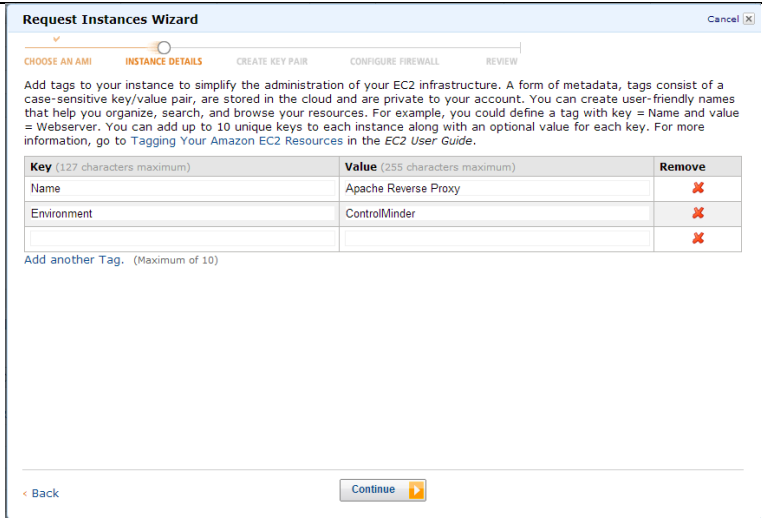
Ensure the Auto-assign Public IP checkbox is checked.

Click the Continue button.







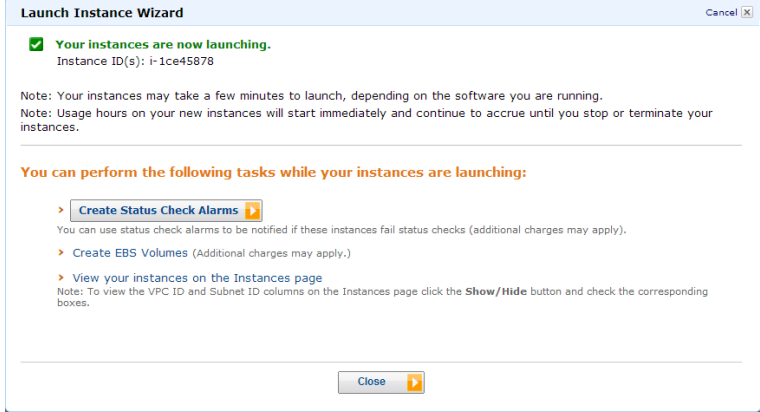


## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

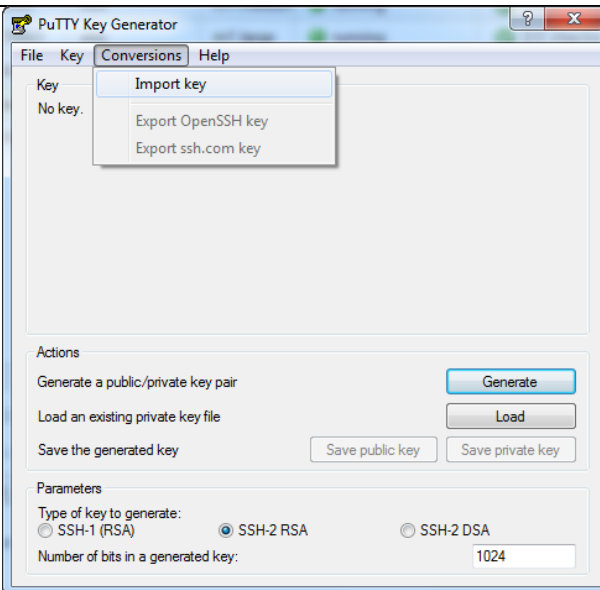
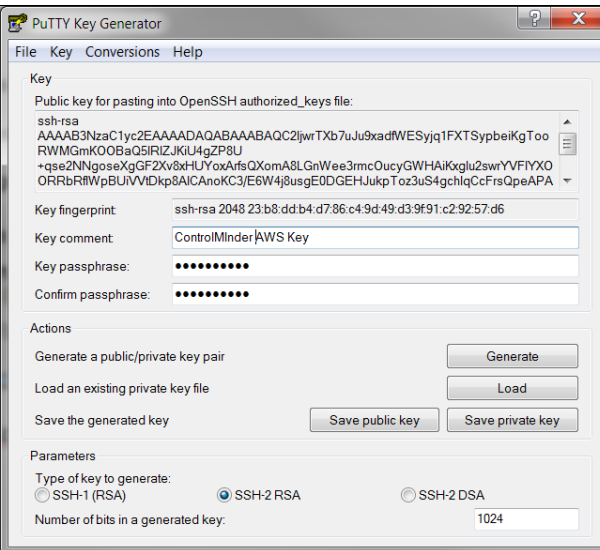
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

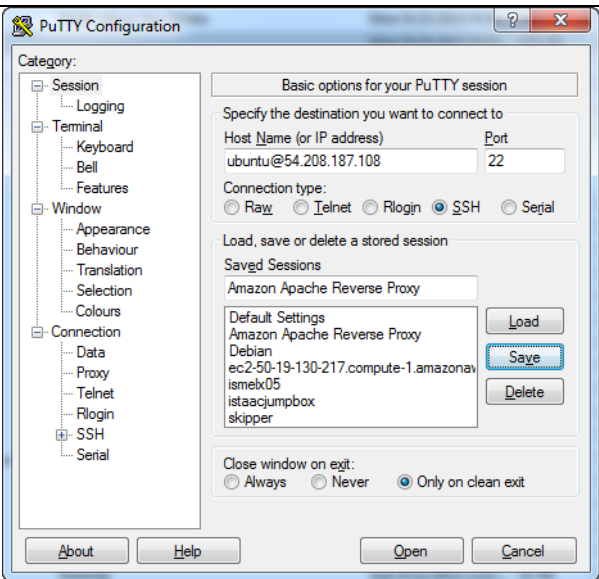
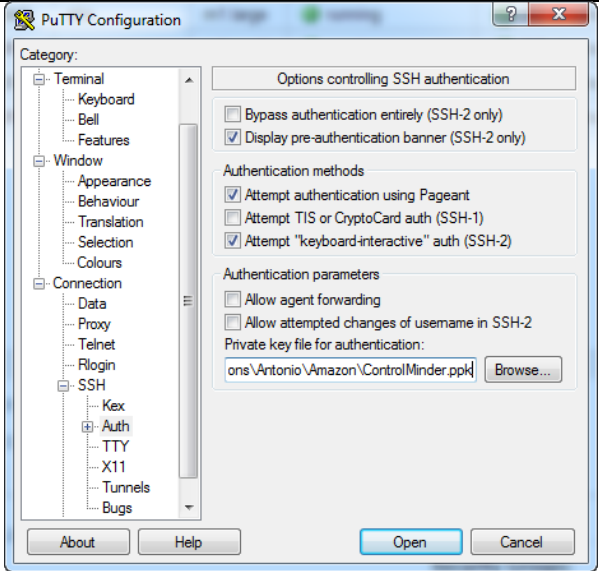
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

<p>Click the Close button.</p>	 <p><b>Launch Instance Wizard</b> <span>Cancel X</span></p> <p>✓ <b>Your instances are now launching.</b> Instance ID(s): i-1ce45878</p> <p>Note: Your instances may take a few minutes to launch, depending on the software you are running. Note: Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.</p> <hr/> <p><b>You can perform the following tasks while your instances are launching:</b></p> <ul style="list-style-type: none"> <li>&gt; <a href="#">Create Status Check Alarms</a>  You can use status check alarms to be notified if these instances fail status checks (additional charges may apply).</li> <li>&gt; <a href="#">Create EBS Volumes</a> (Additional charges may apply.)</li> <li>&gt; <a href="#">View your instances on the Instances page</a> Note: To view the VPC ID and Subnet ID columns on the Instances page click the <b>Show/Hide</b> button and check the corresponding boxes.</li> </ul> <p><span>Close</span> </p>
--------------------------------	---

## 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.
<p>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.</p> <p>You will convert the ControlMinder.PEM Key Pair into the PPK format used by PuTTY.</p> <p>Run PuTTYKeyGen.</p> <p>From the Conversions menu item, choose Import Key.</p>	
<p>Make your AWS ECS account certificate available. In the examples throughout this document, the key pair file is named ControlMinder.pem.</p> <p>Choose the ControlMinder.pem key pair file to import.</p> <p>Create and confirm a key passphrase. Remember this passphrase because you must provide it each time you login to the Apache Reverse Proxy Server.</p> <p>Click the <u>Save private key</u> button and the file as ControlMinder.ppk.</p>	

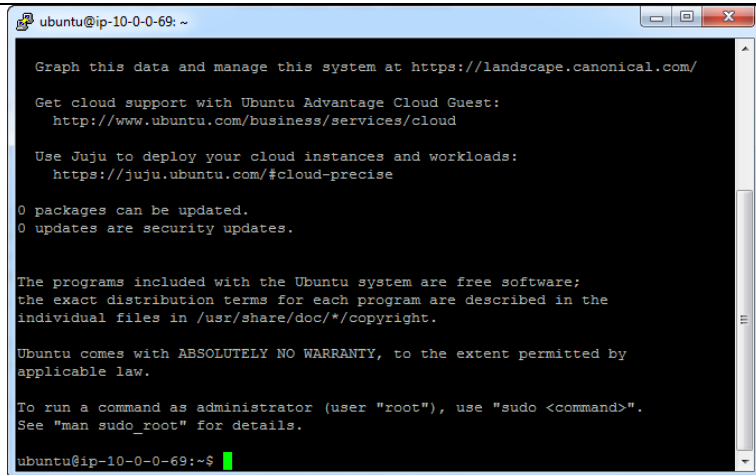
## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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.



```
ubuntu@ip-10-0-0-69: ~
Graph this data and manage this system at https://landscape.canonical.com/

Get cloud support with Ubuntu Advantage Cloud Guest:
  http://www.ubuntu.com/business/services/cloud

Use Juju to deploy your cloud instances and workloads:
  https://juju.ubuntu.com/#cloud-precise

0 packages can be updated.
0 updates are security updates.

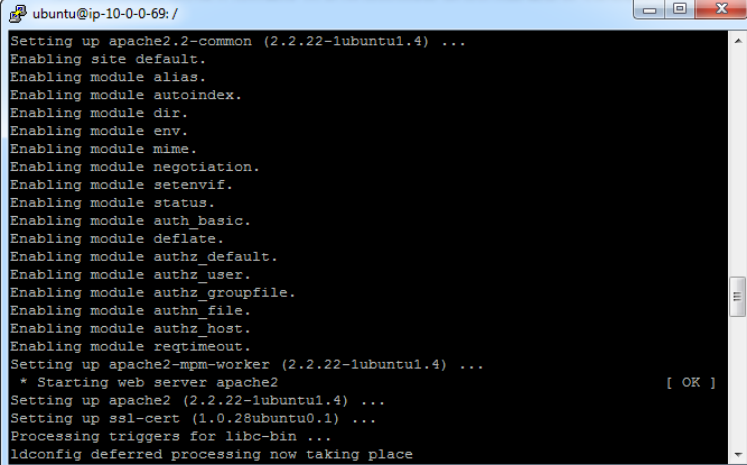
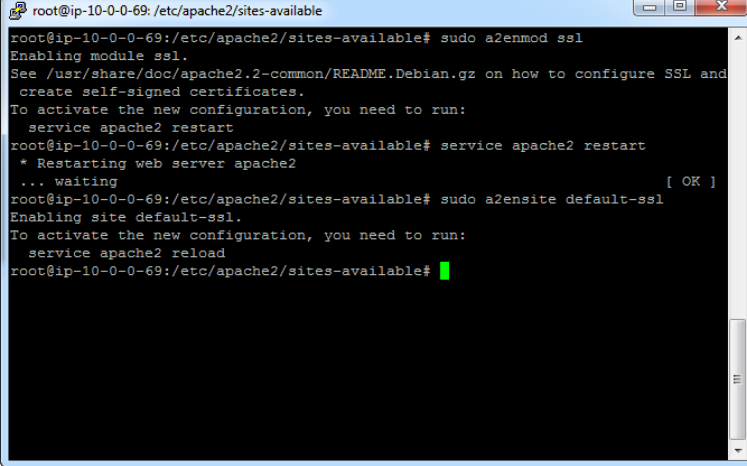
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

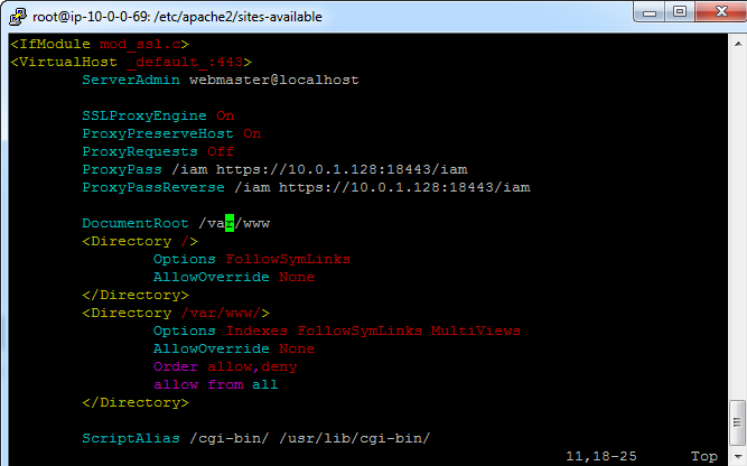
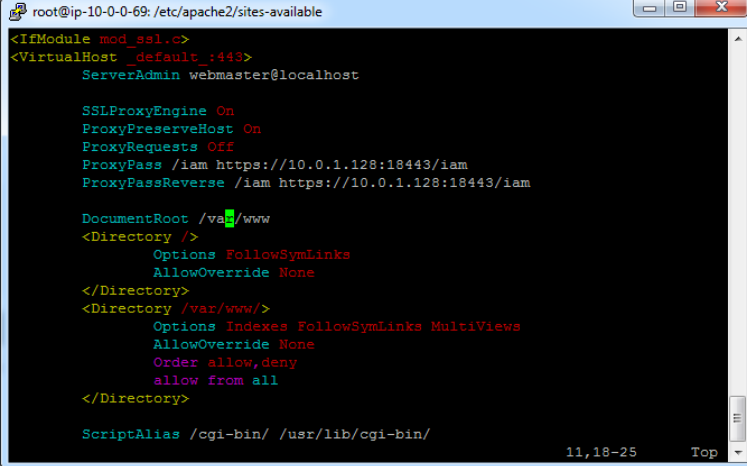
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-0-69:~$
```

## Install Apache 2.0

<p>Install Apache Reverse Proxy Server.</p> <p>Execute the following commands:</p> <ul style="list-style-type: none"> <li>• <code>sudo apt-get update</code></li> <li>• <code>sudo apt-get install apache2</code></li> </ul>	 <pre> 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 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 </pre>
<p>Enable SSL by running:</p> <ul style="list-style-type: none"> <li>• <code>sudo a2enmod ssl</code></li> <li>• <code>sudo a2ensite default-ssl</code></li> </ul>	 <pre> 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 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# </pre>
<p>Run the following commands to enable Reverse Proxy:</p> <ul style="list-style-type: none"> <li>• <code>sudo ln -s /etc/apache2/mods-available/proxy.load /etc/apache2/mods-enabled</code></li> <li>• <code>sudo ln -s /etc/apache2/mods-available/proxy_http.load /etc/apache2/mods-enabled</code></li> </ul>	 <pre> ubuntu@ip-10-0-0-69: /etc/apache2/sites-available &lt;VirtualHost *:80&gt;     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     &lt;Directory /&gt;         Options FollowSymLinks         AllowOverride None     &lt;/Directory&gt;     &lt;Directory /var/www/&gt;         Options Indexes FollowSymLinks MultiViews         AllowOverride None         Order allow,deny         allow from all     &lt;/Directory&gt;      ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/     &lt;Directory "/usr/lib/cgi-bin"&gt; </pre>

<p>Modify the reverse proxy settings:</p> <p>sudo vi /etc/apache2/sites-available/default</p> <p>Add the following lines:</p> <p>ProxyPreserveHost On ProxyRequests Off ProxyPass / <a href="http://&lt;ENTM private IP&gt;:18080/iam">http://&lt;ENTM private IP&gt;:18080/iam</a> ProxyPassReverse / <a href="http://&lt;ENTM Private IP&gt;:18080/iam">http://&lt;ENTM Private IP&gt;:18080/iam</a></p>	
<p>sudo vi /etc/apache2/sites-available/default-ssl</p> <p>Add the following lines:</p> <p>SSLProxyEngine On ProxyPreserveHost On ProxyRequests Off ProxyPass / <a href="https://&lt;ENTM private IP&gt;:18443/iam">https://&lt;ENTM private IP&gt;:18443/iam</a> ProxyPassReverse / <a href="https://&lt;ENTM Private IP&gt;:18443/iam">https://&lt;ENTM Private IP&gt;:18443/iam</a></p>	
<p>Execute the following command to restart Apache:</p> <ul style="list-style-type: none"> <li>service apache2 restart</li> </ul>	

## Appendix B - Setup email notification using Amazon SES

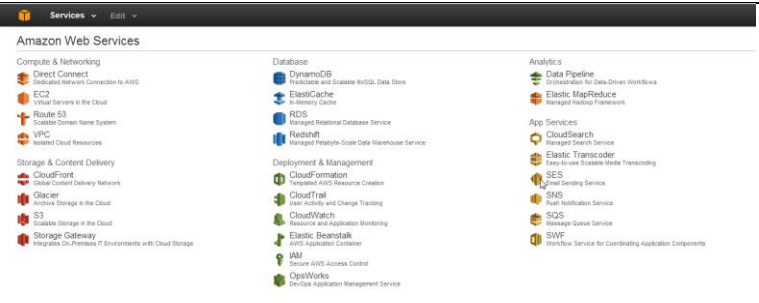
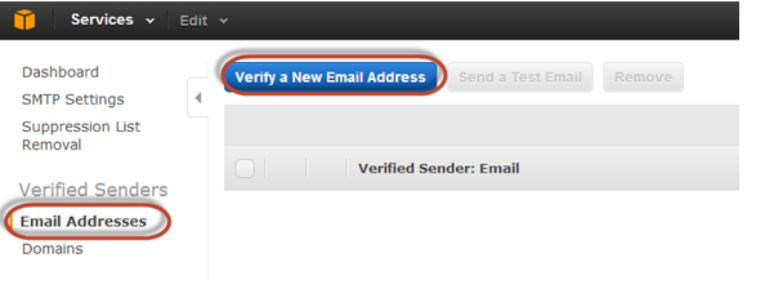
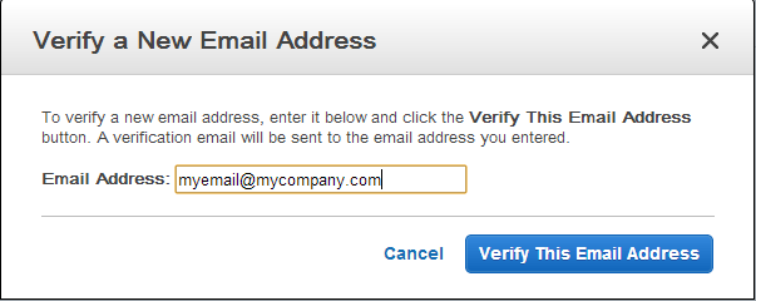
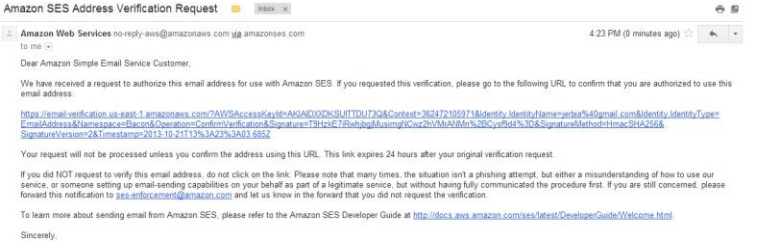
You can use Amazon SES (Simple Email Service) for CA ControlMinder workflow notification.

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

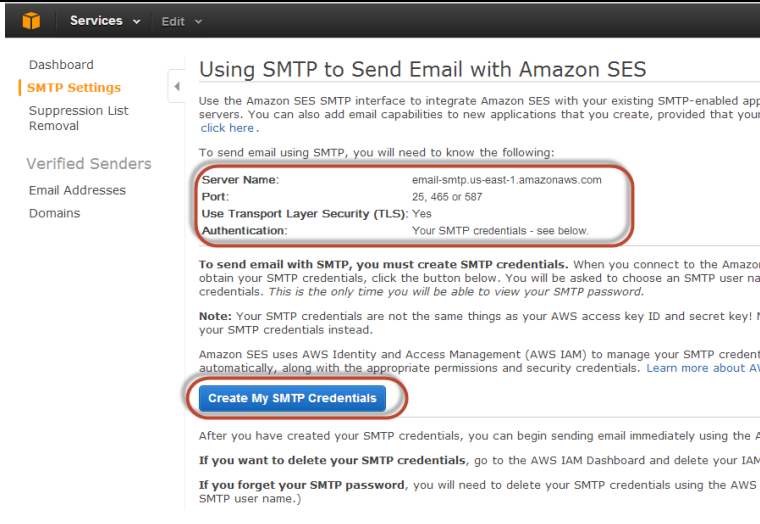
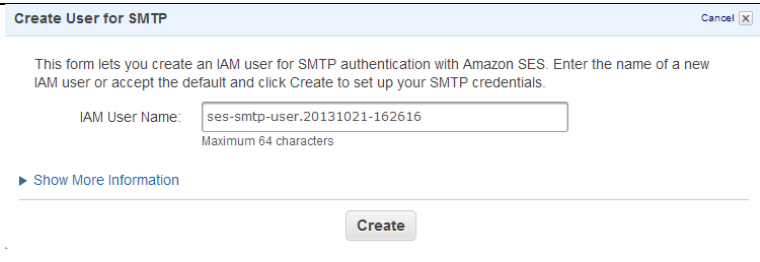
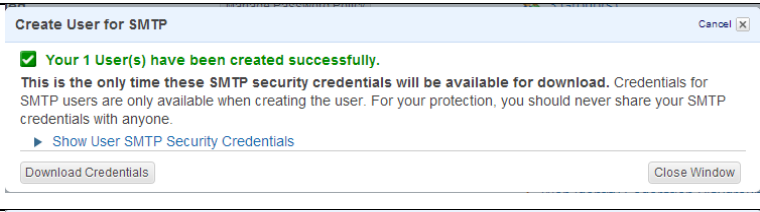
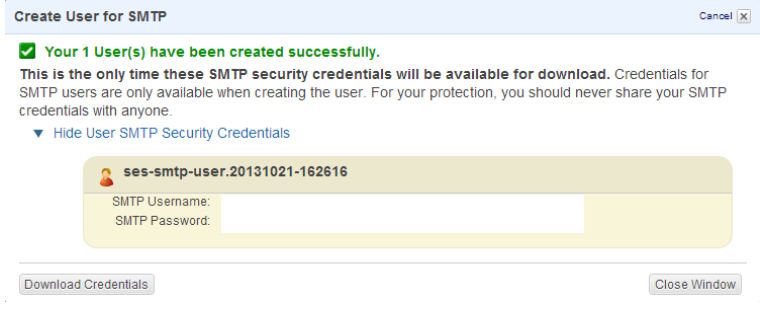


## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

### Create E-Mail Sandbox

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

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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

## 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 sent 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:

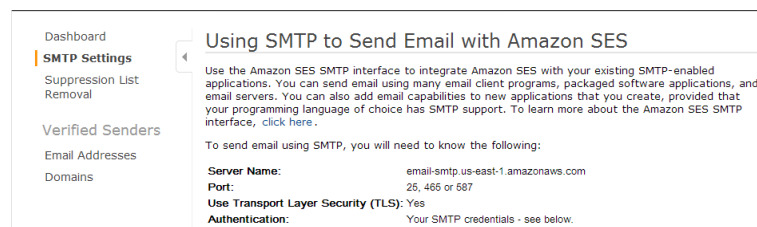
```
<property name="mail.smtp.host" value="smtp.nosuchhost.nosuchdomain.com"/>
```

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 on 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

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

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
```

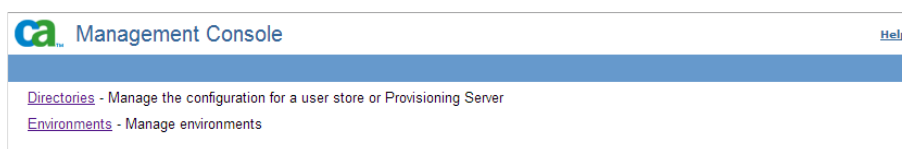
Start JBoss.

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

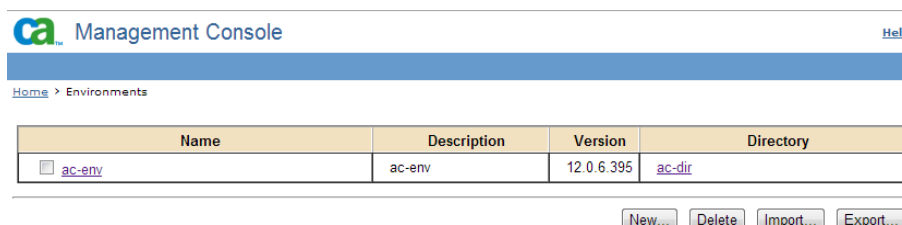
Open the IdentityMinder Management Console by browsing to the following link:

<https://localhost:18443/idmmanage>

In the CA IdentityMinder™ Management Console, click Environments.

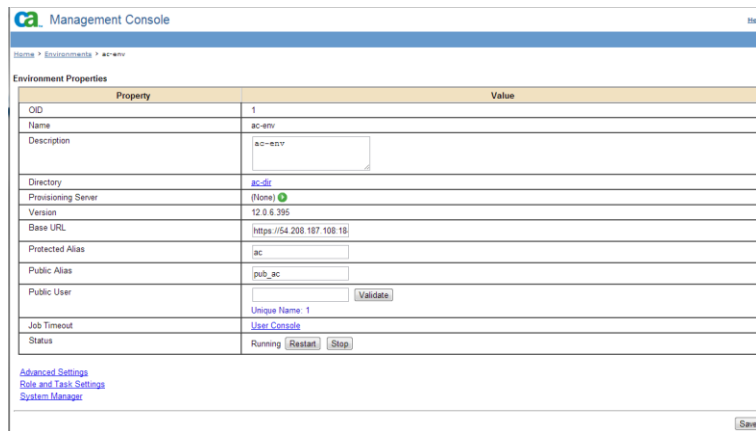


Select ac-env.



Select Advanced Settings.

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment



CA Management Console

Home > Environments > ac-env

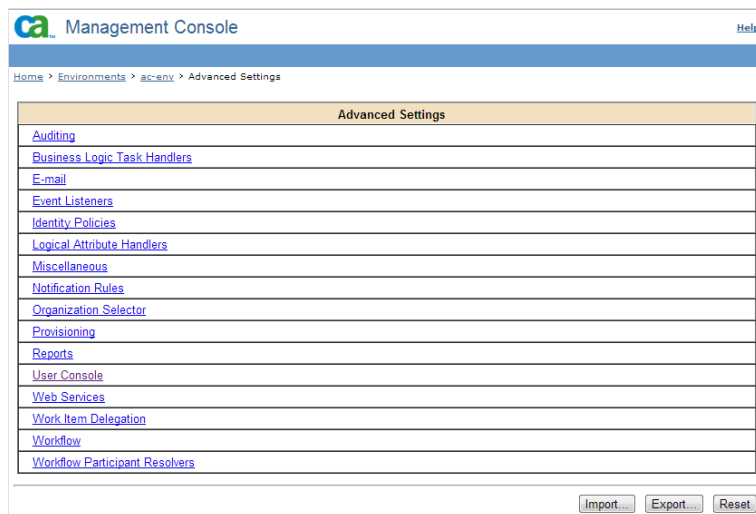
Environment Properties

Property	Value
OID	1
Name	ac-env
Description	ac-env
Directory	ac-dir
Provisioning Server	(None)
Version	12.0.6.395
Base URL	https://54.208.187.108:18
Protected Alias	ac
Public Alias	pub_ac
Public User	Unique Name: 1 <a href="#">Validate</a>
Job Timeout	<a href="#">User Console</a>
Status	Running <a href="#">Restart</a> <a href="#">Stop</a>

[Advanced Settings](#)  
[Role and Task Settings](#)  
[System Manager](#)

[Save](#)

Select E-mail.



CA Management Console

Home > Environments > ac-env > Advanced Settings

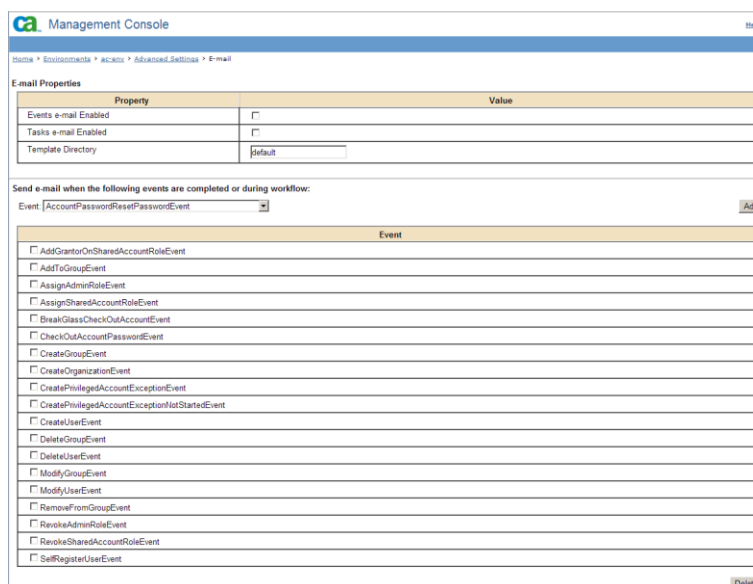
Advanced Settings

<a href="#">Auditing</a>
<a href="#">Business Logic Task Handlers</a>
<a href="#">E-mail</a>
<a href="#">Event Listeners</a>
<a href="#">Identity Policies</a>
<a href="#">Logical Attribute Handlers</a>
<a href="#">Miscellaneous</a>
<a href="#">Notification Rules</a>
<a href="#">Organization Selector</a>
<a href="#">Provisioning</a>
<a href="#">Reports</a>
<a href="#">User Console</a>
<a href="#">Web Services</a>
<a href="#">Work Item Delegation</a>
<a href="#">Workflow</a>
<a href="#">Workflow Participant Resolvers</a>

[Import...](#) [Export...](#) [Reset](#)

The E-mail Properties window appears.

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment



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.

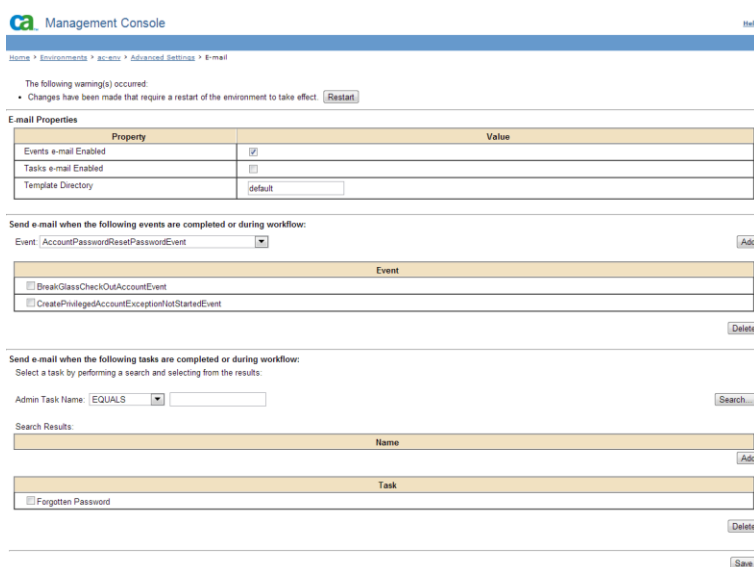
Click Save.

## CA ControlMinder Rapid Implementation Guide – Amazon EC2 Deployment

The email notification properties are saved.

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

Click the Restart button.



The screenshot shows the CA Management Console interface. At the top, there's a navigation bar with 'Home', 'Environments', 'Actions', 'Advanced Settings', and 'E-mail'. Below this, a warning message states: 'The following warning(s) occurred: Changes have been made that require a restart of the environment to take effect.' with a 'Restart' button. The main section is titled 'Email Properties' and contains a table with the following data:

Property	Value
Events e-mail Enabled	<input checked="" type="checkbox"/>
Tasks e-mail Enabled	<input checked="" type="checkbox"/>
Template Directory	default

Below the table, there are two sections for configuring email notifications. The first section is 'Send e-mail when the following events are completed or during workflow:' with a dropdown menu showing 'AccountPasswordResetPasswordEvent' and an 'Add' button. Below this is a table of events:

Event
<input type="checkbox"/> BreakGlassCheckOutAccountEvent
<input type="checkbox"/> CreatePrivilegedAccountExceptionNotStartedEvent

A 'Delete' button is located to the right of the event table. The second section is 'Send e-mail when the following tasks are completed or during workflow:' with a dropdown menu showing 'Admin Task Name: EQUALS' and a 'Search...' button. Below this is a 'Search Results' section with a table of tasks:

Task
<input type="checkbox"/> Forgotten Password

A 'Delete' button is located to the right of the task table. At the bottom right of the console, there is a 'Save' 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.