CA Technologies

CA ControlMinder™ Rapid Implementation Guide

Amazon EC2 Deployment

CA Technologies
8/30/2013

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 HTLM format in the following folder:

…\AccessControlServer\MessageQueue\tibco\ems\5.1\doc

CA ControlMinder References

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

Tibco References

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

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.

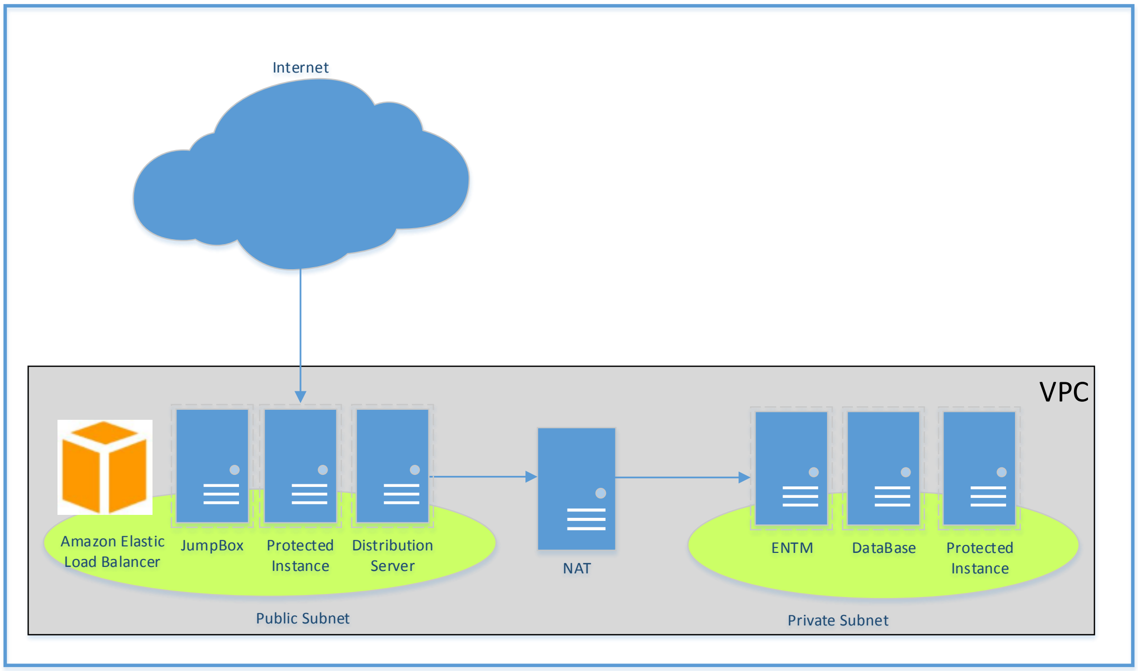


Figure 1 – Reference Deployment Architecture

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

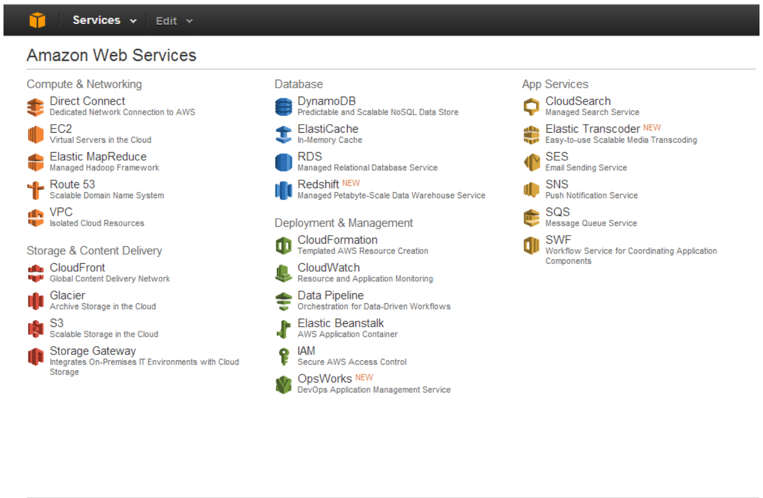
Prerequisites and Getting Started

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

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

You can the console at:

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



Amazon Web Services

Compute & Networking

Direct Connect
Dedicated Network Connection to AWS

EC2
Virtual Servers in the Cloud

Elastic MapReduce
Managed Hadoop Framework

Route 53
Scalable Domain Name System

VPC
Isolated Cloud Resources

Storage & Content Delivery

CloudFront
Global Content Delivery Network

Glacier
Archive Storage in the Cloud

S3
Scalable Storage in the Cloud

Storage Gateway
Integrates On-Premises IT Environments with Cloud Storage

Database

DynamoDB
Predictable and Scalable NoSQL Data Store

ElastiCache
In-Memory Cache

RDS
Managed Relational Database Service

Redshift NEW
Managed Petabyte-Scale Data Warehouse Service

Deployment & Management

CloudFormation
Templated AWS Resource Creation

CloudWatch
Resource and Application Monitoring

Data Pipeline
Orchestration for Data-Driven Workflows

Elastic Beanstalk
AWS Application Container

IAM
Secure AWS Access Control

OpsWorks NEW
DevOps Application Management Service

App Services

CloudSearch
Managed Search Service

Elastic Transcoder NEW
Easy-to-use Scalable Media Transcoding

SES
Email Sending Service

SNS
Push Notification Service

SQS
Message Queue Service

SWF
Workflow Service for Coordinating Application Components

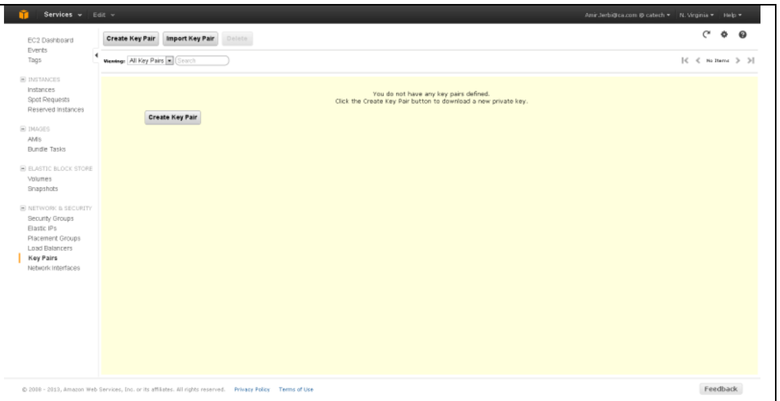
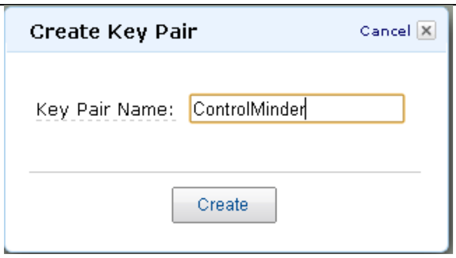
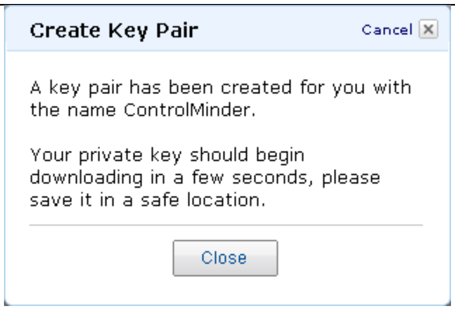
Generating a Key Pair

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

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

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

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

Select AWS Services to create a Key Pair.	 You do not have any key pairs defined. Click the Create Key Pair button to download a new private key. Services Edit Amir.Jerbi@ca.com @ catech 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 Key Pair Import Key Pair Delete Viewing: All Key Pairs Search No Items Create Key Pair © 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Feedback
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.	 Create Key Pair Key Pair Name: ControlMinder
Select Close once the Key Pair has been created. Save the private key file to your local machine and remember the location. Note that the Key Pair is downloaded to your browser and once the downloaded Key Pair has been retrieved then you cannot retrieve the Key Pair from Amazon again.	 Create Key Pair A key pair has been created for you with the name ControlMinder. Your private key should begin downloading in a few seconds, please save it in a safe location.

Creating a Virtual Private Cloud

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

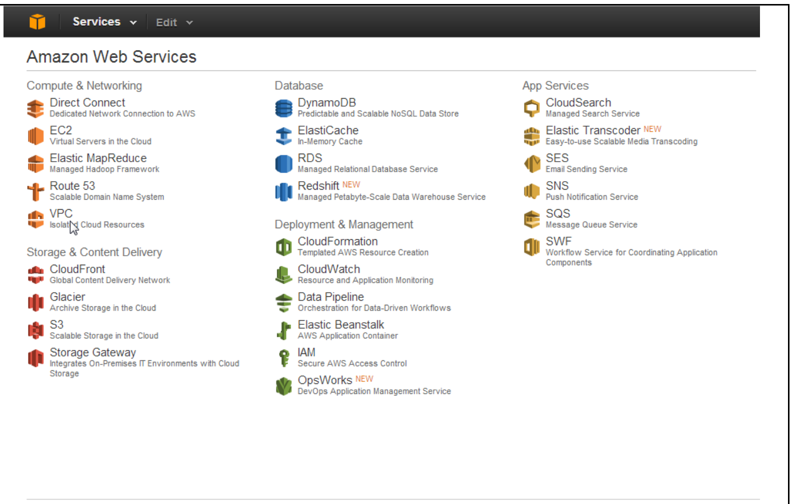
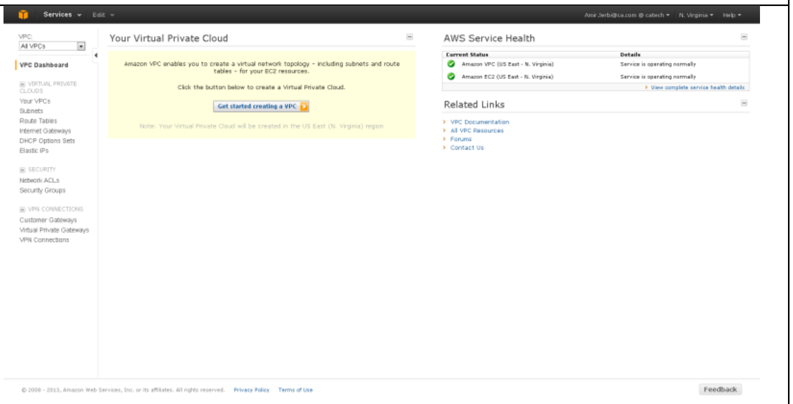
This virtual network closely resembles a traditional network that you operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

We will create 2 subnets:

- Public subnet
- Private subnet

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

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

<table>
<tr>
<td>Login to the AWS Console. Click VPC,</td>
<td>

Services
Edit
Amazon Web Services
Compute &amp; Networking
Direct Connect
Dedicated Network Connection to AWS
EC2
Virtual Servers in the Cloud
Elastic MapReduce
Managed Hadoop Framework
Route 53
Scalable Domain Name System
VPC
Isolated Cloud Resources
Storage &amp; Content Delivery
CloudFront
Global Content Delivery Network
Glacier
Archive Storage in the Cloud
S3
Scalable Storage in the Cloud
Storage Gateway
Integrates On-Premises IT Environments with Cloud Storage
Database
DynamoDB
Predictable and Scalable NoSQL Data Store
ElastiCache
In-Memory Cache
RDS
Managed Relational Database Service
Redshift NEW
Managed Petabyte-Scale Data Warehouse Service
Deployment &amp; Management
CloudFormation
Templated AWS Resource Creation
CloudWatch
Resource and Application Monitoring
Data Pipeline
Orchestration for Data-Driven Workflows
Elastic Beanstalk
AWS Application Container
IAM
Secure AWS Access Control
OpsWorks NEW
DevOps Application Management Service
App Services
CloudSearch
Managed Search Service
Elastic Transcoder NEW
Easy-to-use Scalable Media Transcoding
SES
Email Sending Service
SNS
Push Notification Service
SQS
Message Queue Service
SWF
Workflow Service for Coordinating Application Components
</td>
</tr>
<tr>
<td>Click the <u>Get started creating a VPC</u> button (ensure that correct region has been selected in which to create the VPC).</td>
<td>


Amazon VPC enables you to create a virtual network topology – including subnets and route tables – for your EC2 resources.
Click the button below to create a Virtual Private Cloud.
Note: Your Virtual Private Cloud will be created in the US East (N. Virginia) region
Current Status | Details
✓ Amazon VPC (US East - N. Virginia) | Service is operating normally
✓ Amazon EC2 (US East - N. Virginia) | Service is operating normally
© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved.
</td>
</tr>
</table>

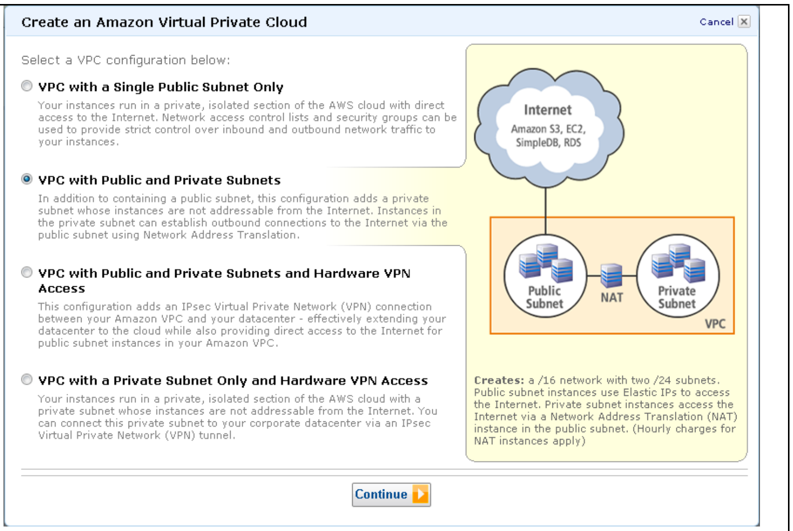
For this example, "VPC with Public and Private Subnets" was chosen.

The ENTM server and the Microsoft SQL server will be isolated on the private subnet.

Other instances will be public facing.

Choose the type of VPC that meets your needs.

Click the Continue button to proceed.



Create an Amazon Virtual Private Cloud

Select a VPC configuration below:

○ **VPC with a Single Public Subnet Only**
Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.

● **VPC with Public and Private Subnets**
In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation.

○ **VPC with Public and Private Subnets and Hardware VPN Access**
This configuration adds an IPsec Virtual Private Network (VPN) connection between your Amazon VPC and your datacenter - effectively extending your datacenter to the cloud while also providing direct access to the Internet for public subnet instances in your Amazon VPC.

○ **VPC with a Private Subnet Only and Hardware VPN Access**
Your instances run in a private, isolated section of the AWS cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate datacenter via an IPsec Virtual Private Network (VPN) tunnel.

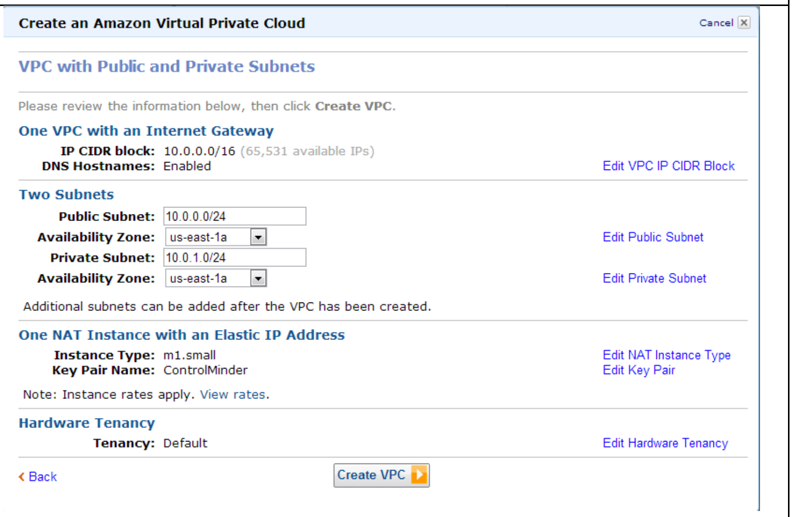
Creates: a /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via a Network Address Translation (NAT) instance in the public subnet. (Hourly charges for NAT instances apply)

This VPC has two subnets:

- a public subnet (10.0.0.0/24)
- a private subnet (10.0.1.0/24)

Verify that both subnets are deployed on the same availability zone.

Click the Create VPC button.



Create an Amazon Virtual Private Cloud

VPC with Public and Private Subnets

Please review the information below, then click **Create VPC**.

One VPC with an Internet Gateway
IP CIDR block: 10.0.0.0/16 (65,531 available IPs)
DNS Hostnames: Enabled

Two Subnets
Public Subnet: 10.0.0.0/24
Availability Zone: us-east-1a
Private Subnet: 10.0.1.0/24
Availability Zone: us-east-1a

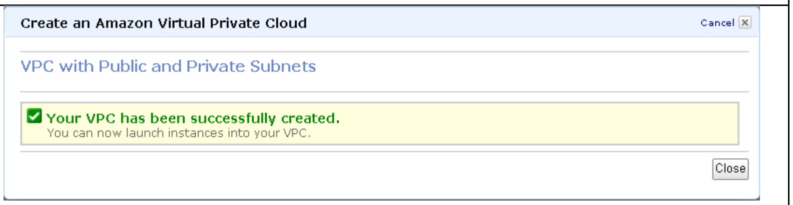
Additional subnets can be added after the VPC has been created.

One NAT Instance with an Elastic IP Address
Instance Type: m1.small
Key Pair Name: ControlMinder

Note: Instance rates apply. View rates.

Hardware Tenancy
Tenancy: Default

You will see confirmation that the VPC was successfully created.



Create an Amazon Virtual Private Cloud

VPC with Public and Private Subnets

☑ Your VPC has been successfully created.
You can now launch instances into your VPC.

Defining Security Groups

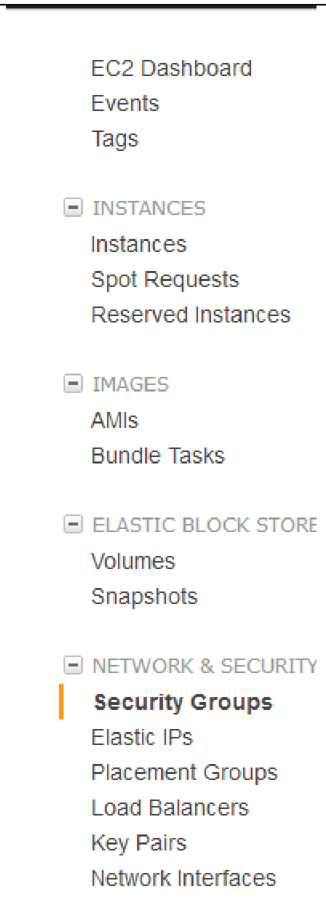
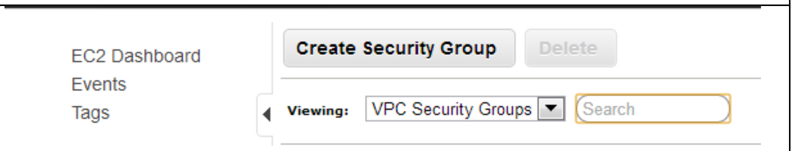
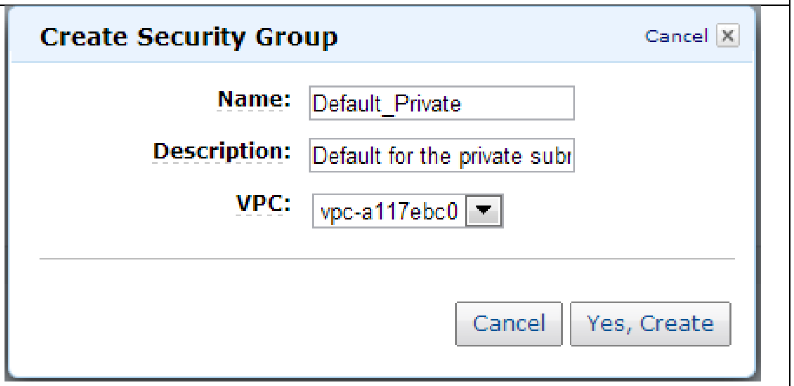
A security group acts as a firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for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

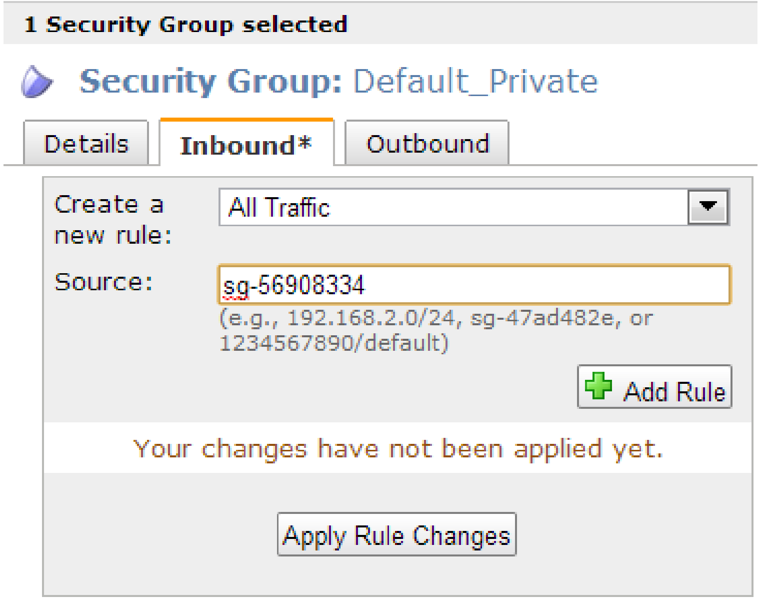
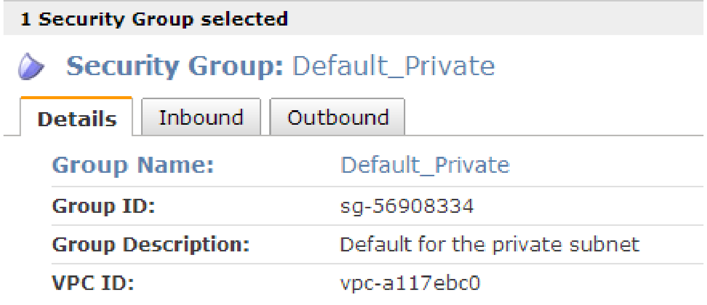
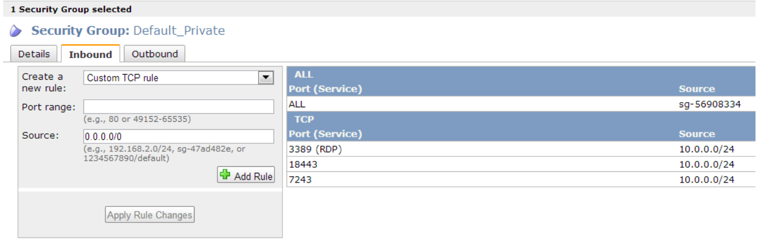
You need to create security groups to open all the necessary ports for implementing and running CA ControlMinder.

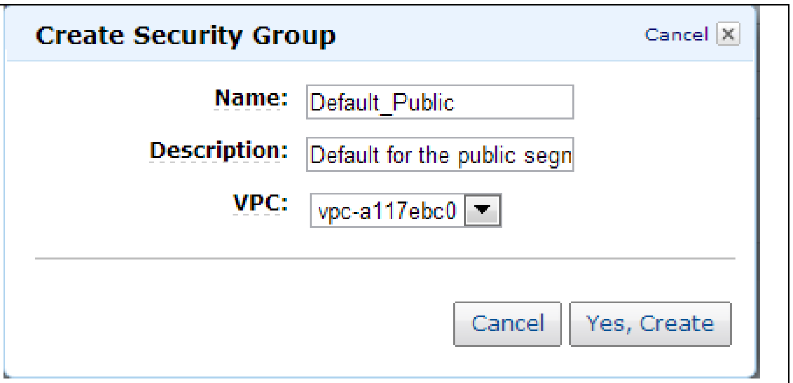
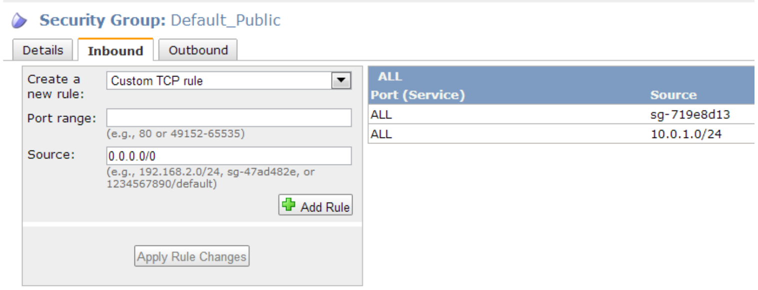
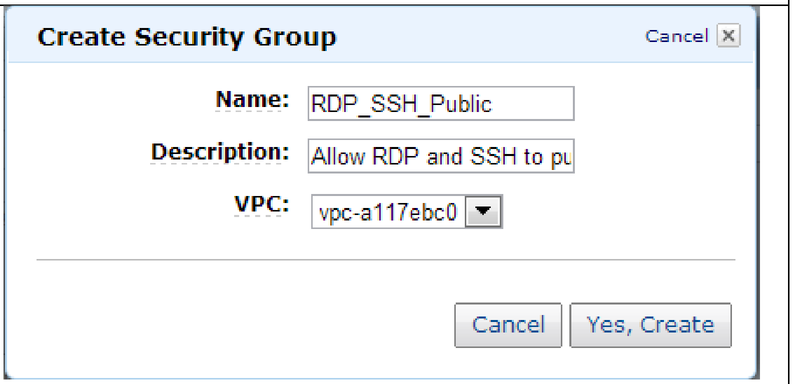
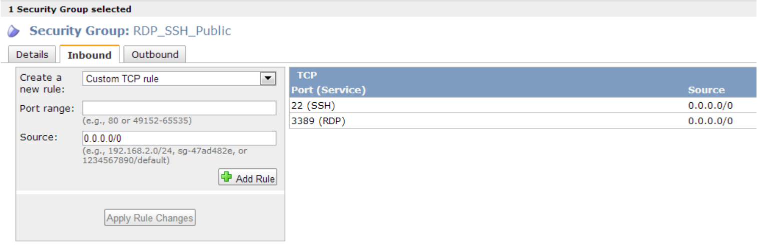
We will use the following groups:

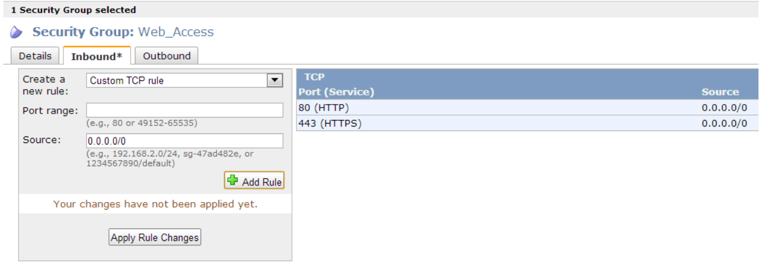
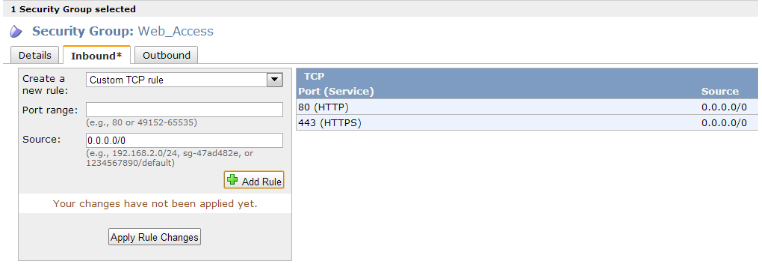
- Default_Private - Defines default access to the private subnet.
- Default_Public - Defines default access to the public subnet.
- RDP_SSH_Public – Allow Remote Desktop (RDP) and Secure Shell (SSH) access to members of this group from the internet. NOTE: Only instances on the public subnet can be members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

Follow the steps below to create the security groups.

Go to Amazon AWS console and select EC2. Select "Security Groups" from the EC2 dashboard.	 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
Click "Create Security Group". Select "VPC Security Groups"	 EC2 Dashboard Events Tags Create Security Group Delete Search Viewing: VPC Security Groups
Provide the name and description for the group and select the VPC you created previously. You will use Default_Private for the group name.	 Name: Default_Private Description: Default for the private subı VPC: vpc-a117ebc0

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 Create a new rule: All Traffic Source: sg-56908334 (e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default) Your changes have not been applied yet.  1 Security Group selected Security Group: Default_Private 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: 0.0.0.0/0 (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

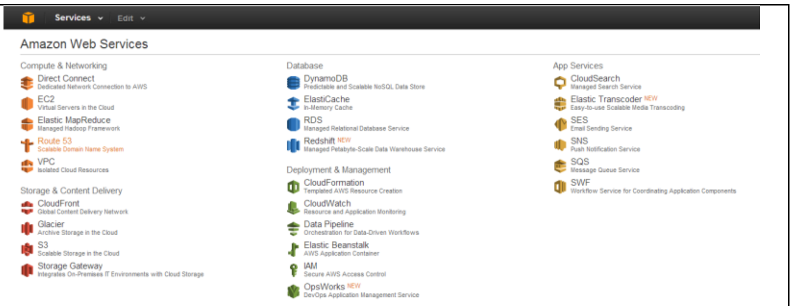
Create group Default_Public”	 Create Security Group Cancel ☒ Name: Default_Public Description: Default for the public segn VPC: vpc-a117ebc0 ▼ Cancel Yes, Create
Add rules that permit access from all members of the public subnet and all members of the private subnet. This is achieved by adding the security group ID of the public subnet as the source and All Traffic as the port/service. Allow also all the communication from the private segment (10.0.1.x in our case).	 Security Group: Default_Public 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 Apply Rule Changes ALL Port (Service) — Source ALL — sg-719e8d13 ALL — 10.0.1.0/24
Create a Security Group to allow Remote Desktop (RDP) and Secure Shell (SSH) access to group members.	 Create Security Group Cancel ☒ Name: RDP_SSH_Public Description: Allow RDP and SSH to pu VPC: vpc-a117ebc0 ▼ Cancel Yes, Create
Add rules to allow members of the public subnet access to members of the private subnet over the following ports: • Remote Desktop (3389) • Secure Shell (22) This example allows access to group members from the public subnet, the private subnet, and the internet. Limit access further to meet your specific requirements. Click “Apply Rule Changes”	 1 Security Group selected Security Group: RDP_SSH_Public 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 Apply Rule Changes TCP Port (Service) — Source 22 (SSH) — 0.0.0.0/0 3389 (RDP) — 0.0.0.0/0

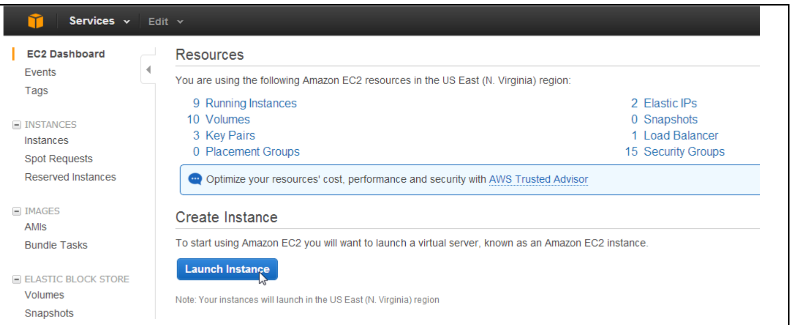
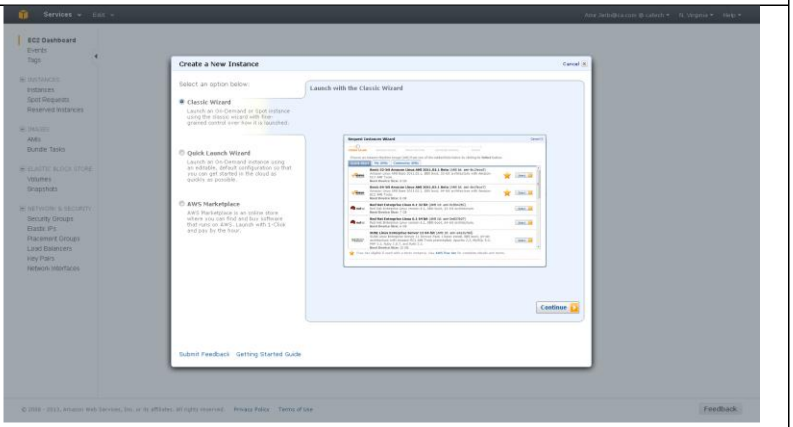
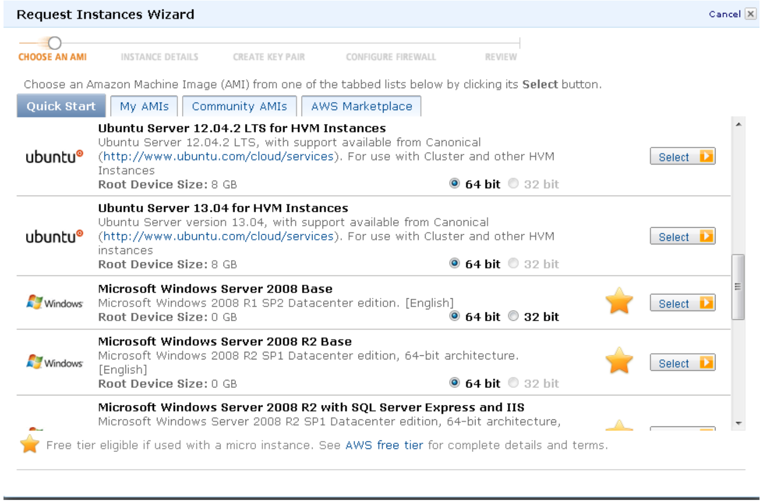
Create the Web_Access group to allow browser access.	 1 Security Group selected Security Group: Web_Access Details · Inbound* · Outbound Create a new rule: Custom TCP rule Port range: (e.g., 80 or 49152-65535) Source: 0.0.0.0/0 (e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default) Add Rule Your changes have not been applied yet. Apply Rule Changes TCP Port (Service) — Source 80 (HTTP) — 0.0.0.0/0 443 (HTTPS) — 0.0.0.0/0
Allow browser access to the: • Default HTTP port (80) • Default HTTPS port (443) This example allows access to group members from the public subnet, the private subnet, and the internet. Limit access further to meet your specific requirements.	 1 Security Group selected Security Group: Web_Access 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 TCP Port (Service) — Source 80 (HTTP) — 0.0.0.0/0 443 (HTTPS) — 0.0.0.0/0

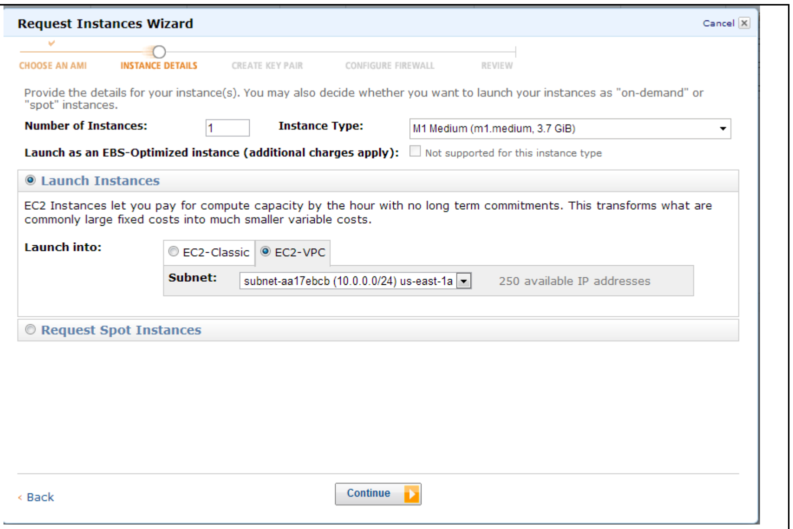
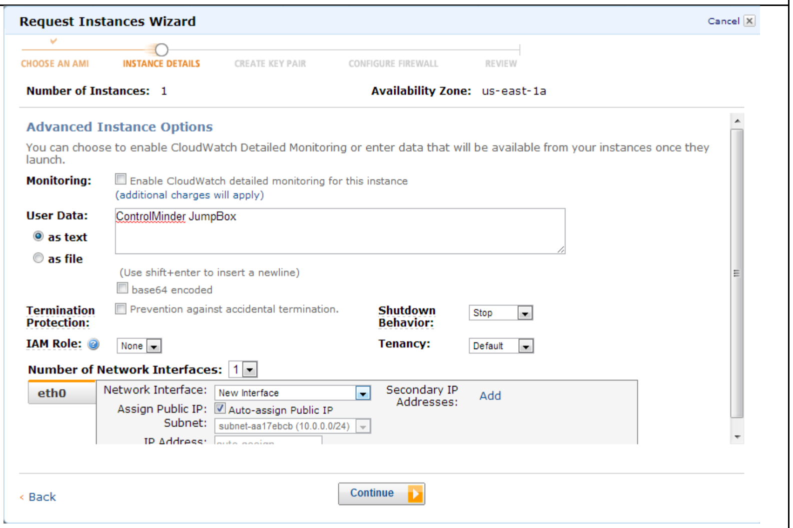
Setting Up a Jump Box

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

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

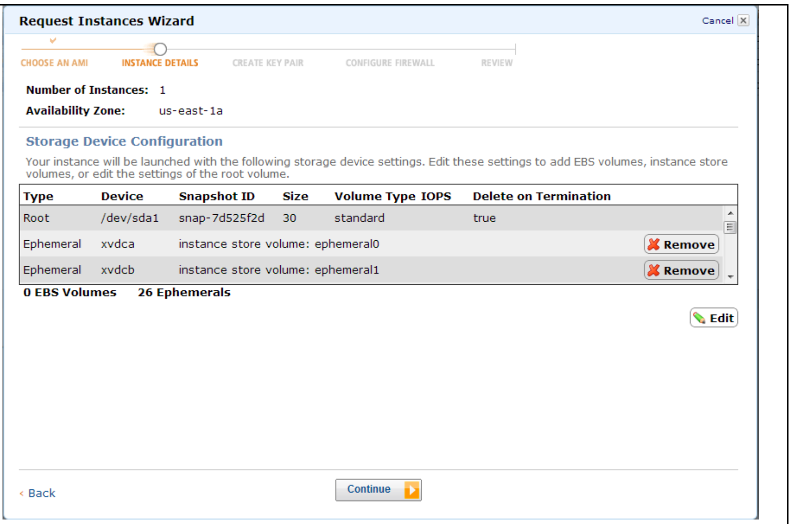
Click the EC2 tab on the Amazon Web Services (AWS) Console.	 Services · Edit Amazon Web Services Compute & Networking Direct Connect – Dedicated Network Connection to AWS EC2 – Virtual Servers in the Cloud Elastic MapReduce – Managed Hadoop Framework Route 53 – Scalable Domain Name System VPC – Isolated Cloud Resources Storage & Content Delivery CloudFront – Global Content Delivery Network Glacier – Archive Storage in the Cloud S3 – Scalable Storage in the Cloud Storage Gateway – Integrates On-Premises IT Environments with Cloud Storage Database DynamoDB – Predictable and Scalable NoSQL Data Store ElastiCache – In-Memory Cache RDS – Managed Relational Database Service Redshift NEW – Managed Petabyte-Scale Data Warehouse Service Deployment & Management CloudFormation – Templated AWS Resource Creation CloudWatch – Resource and Application Monitoring Data Pipeline – Orchestration for Data-Driven Workflows Elastic Beanstalk – AWS Application Container IAM – Secure AWS Access Control OpsWorks NEW – DevOps Application Management Service App Services CloudSearch – Managed Search Service Elastic Transcoder NEW – Easy-to-use Scalable Media Transcoding SES – Email Sending Service SNS – Push Notification Service SQS – Message Queue Service SWF – Workflow Service for Coordinating Application Components

Click the “Launch Instances” button.	 Services Edit EC2 Dashboard Events Tags INSTANCES Instances Spot Requests Reserved Instances IMAGES AMIs Bundle Tasks ELASTIC BLOCK STORE Volumes Snapshots Resources You are using the following Amazon EC2 resources in the US East (N. Virginia) region: 9 Running Instances 10 Volumes 3 Key Pairs 0 Placement Groups 2 Elastic IPs 0 Snapshots 1 Load Balancer 15 Security Groups Optimize your resources' cost, performance and security with AWS Trusted Advisor Create Instance To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance. Launch Instance Note: Your instances will launch in the US East (N. Virginia) region
Click the radial button for the Classic Wizard.	 Create a New Instance Cancel Select an option below: ● Classic Wizard Launch an On-Demand or Spot instance using the classic wizard with fine-grained control over how it is launched. ○ Quick Launch Wizard Launch an On-Demand instance using an editable, default configuration so that you can get started in the cloud as quickly as possible. ○ AWS Marketplace AWS Marketplace is an online store where you can find and buy software that runs on AWS. Launch with 1-Click and pay by the hour. Launch with the Classic Wizard Continue Submit Feedback Getting Started Guide Privacy Policy Terms of Use Feedback
Scroll through the Quick Start list of Amazon Machine Images (AMIs) and select Microsoft Windows 2008 R2 Base.	 Request Instances Wizard Cancel CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its **Select** button. Quick Start My AMIs Community AMIs AWS Marketplace **Ubuntu Server 12.04.2 LTS for HVM Instances** Ubuntu Server 12.04.2 LTS, with support available from Canonical (http://www.ubuntu.com/cloud/services). For use with Cluster and other HVM Instances **Root Device Size:** 8 GB ● 64 bit ○ 32 bit Select **Ubuntu Server 13.04 for HVM Instances** Ubuntu Server version 13.04, with support available from Canonical (http://www.ubuntu.com/cloud/services). For use with Cluster and other HVM instances **Root Device Size:** 8 GB ● 64 bit ○ 32 bit Select **Microsoft Windows Server 2008 Base** Microsoft Windows 2008 R1 SP2 Datacenter edition. [English] **Root Device Size:** 0 GB ● 64 bit ○ 32 bit Select **Microsoft Windows Server 2008 R2 Base** Microsoft Windows 2008 R2 SP1 Datacenter edition, 64-bit architecture. [English] **Root Device Size:** 0 GB ● 64 bit ○ 32 bit Select **Microsoft Windows Server 2008 R2 with SQL Server Express and IIS** Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Free tier eligible if used with a micro instance. See AWS free tier for complete details and terms.

Select M1 Medium instance. Ensure that the JumpBox is deployed on the public subnet (10.0.0.0/24). Click the Continue button.	 Request Instances Wizard Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances. Number of Instances: 1 Instance Type: M1 Medium (m1.medium, 3.7 GiB) Launch as an EBS-Optimized instance (additional charges apply): □ Not supported for this instance type ● Launch Instances EC2 Instances let you pay for compute capacity by the hour with no long term commitments. This transforms what are commonly large fixed costs into much smaller variable costs. Launch into: ○ EC2-Classic ● EC2-VPC Subnet: subnet-aa17ebcb (10.0.0.0/24) us-east-1a 250 available IP addresses ○ Request Spot Instances Cancel CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW ‹ Back Continue
Provide User data to identify your instance. Ensure that the Auto assign Public IP option is chosen to make the JumpBox internet accessible. Click the Continue button.	 Request Instances Wizard 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 JumpBox ● 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-aa17ebcb (10.0.0.0/24) IP Address: auto-assign Secondary IP Addresses: Add Cancel CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW ‹ Back Continue

Keep the default storage configuration.

30 gigabytes of disk storage is sufficient for the JumpBox server.



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

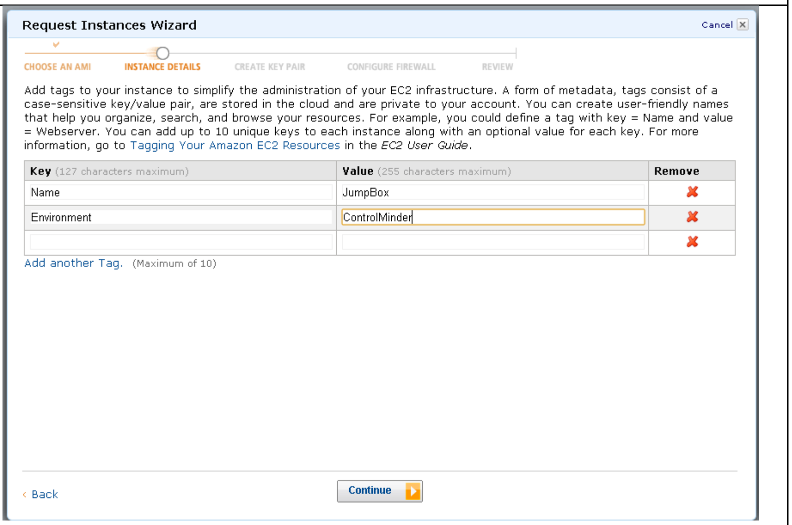
Storage Device Configuration

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-7d525f2d	30	standard		true	
Ephemeral	xvdca	instance store volume: ephemeral0					Remove
Ephemeral	xvdcb	instance store volume: ephemeral1					Remove

0 EBS Volumes **26 Ephemerals**

Name your instance and provide any additional tags as required.

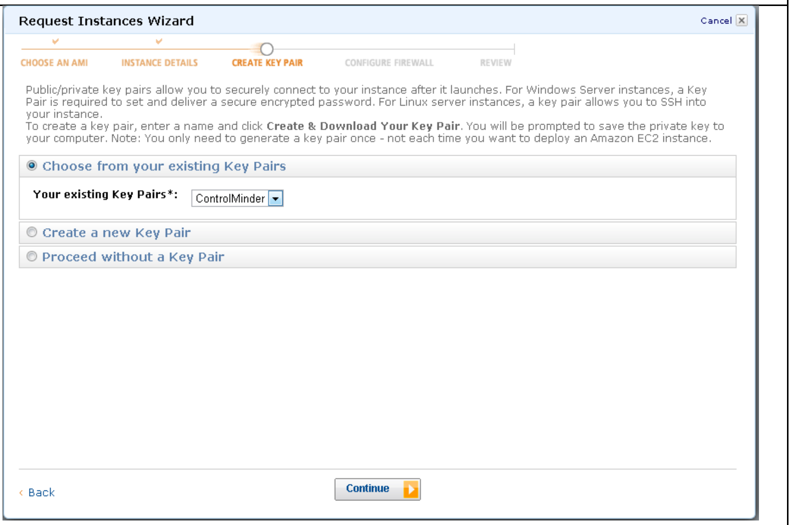


Add tags to your instance to simplify the administration of your EC2 infrastructure. A form of metadata, tags consist of a case-sensitive key/value pair, are stored in the cloud and are private to your account. You can create user-friendly names that help you organize, search, and browse your resources. For example, you could define a tag with key = Name and value = Webserver. You can add up to 10 unique keys to each instance along with an optional value for each key. For more information, go to Tagging Your Amazon EC2 Resources in the *EC2 User Guide*.

Key (127 characters maximum)	**Value** (255 characters maximum)	**Remove**
Name	JumpBox	✗
Environment	ControlMinder	✗
		✗

Add another Tag. (Maximum of 10)

Use the key pair associated you're your AWS ECS Account.



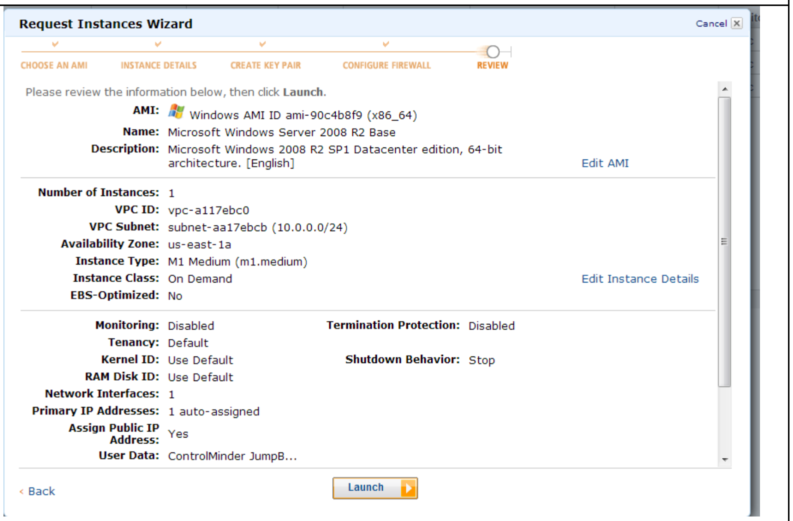
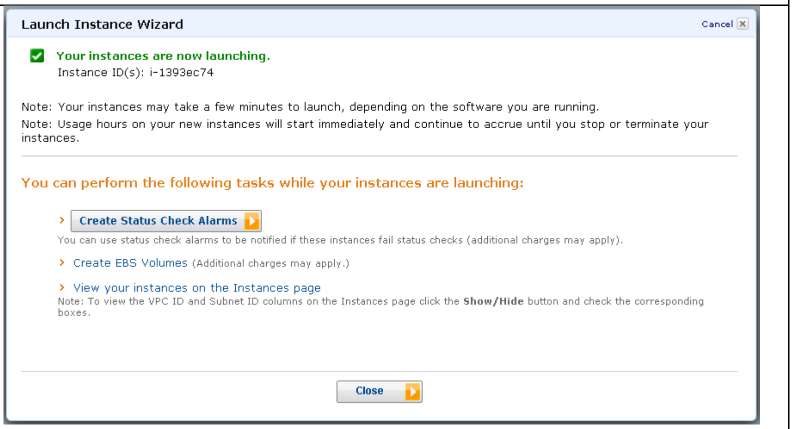
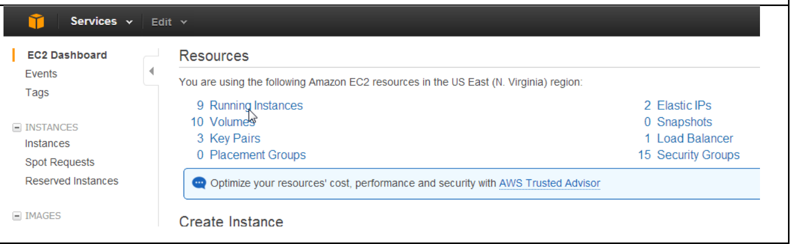
Public/private key pairs allow you to securely connect to your instance after it launches. For Windows Server instances, a Key Pair is required to set and deliver a secure encrypted password. For Linux server instances, a key pair allows you to SSH into your instance.
To create a key pair, enter a name and click **Create & Download Your Key Pair**. You will be prompted to save the private key to your computer. Note: You only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.

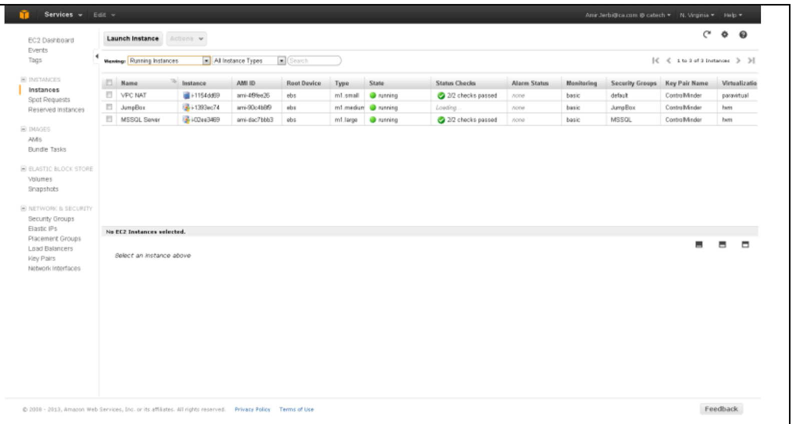
● Choose from your existing Key Pairs

Your existing Key Pairs*: ControlMinder

○ Create a new Key Pair

○ Proceed without a Key Pair

Assign the following Security Groups to the JumpBox: • Default_Public • RDP_SSH_Public	
Click 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-aa17ebcb (10.0.0.0/24) **Availability Zone:** us-east-1a **Instance Type:** M1 Medium (m1.medium) **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:** Yes **User Data:** ControlMinder JumpB... ‹ Back Launch
	 Launch Instance Wizard Cancel ☑ Your instances are now launching. Instance ID(s): i-1393ec74 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. You can perform the following tasks while your instances are launching: › Create Status Check Alarms You can use status check alarms to be notified if these instances fail status checks (additional charges may apply). › Create EBS Volumes (Additional charges may apply.) › View your instances on the Instances page Note: To view the VPC ID and Subnet ID columns on the Instances page click the **Show/Hide** button and check the corresponding boxes. Close
Click on “Running Instances” on the EC2 Dashboard to verify that your instance is up and running.	 Services Edit EC2 Dashboard Events Tags INSTANCES Instances Spot Requests Reserved Instances IMAGES Resources You are using the following Amazon EC2 resources in the US East (N. Virginia) region: 9 Running Instances 2 Elastic IPs 10 Volumes 0 Snapshots 3 Key Pairs 1 Load Balancer 0 Placement Groups 15 Security Groups Optimize your resources' cost, performance and security with AWS Trusted Advisor Create Instance

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

Launch Instance

Viewing: Running Instances | All Instance Types

1 to 3 of 3 Instances

Name	Instance	AMI ID	Root Device	Type	State	Status Checks	Alarm Status	Monitoring	Security Groups	Key Pair Name	Virtualizatio
VPC NAT	i-1154dd69	ami-4f9fee26	ebs	m1.small	running	✓ 2/2 checks passed	none	basic	default	ControlMinder	paravirtual
JumpBox	i-1393ec74	ami-90c4b8f9	ebs	m1.mediun	running	Loading...	none	basic	JumpBox	ControlMinder	hvm
MSSQL Server	i-02ae3469	ami-dac7bbb3	ebs	m1.large	running	✓ 2/2 checks passed	none	basic	MSSQL	ControlMinder	hvm

No EC2 Instances selected.

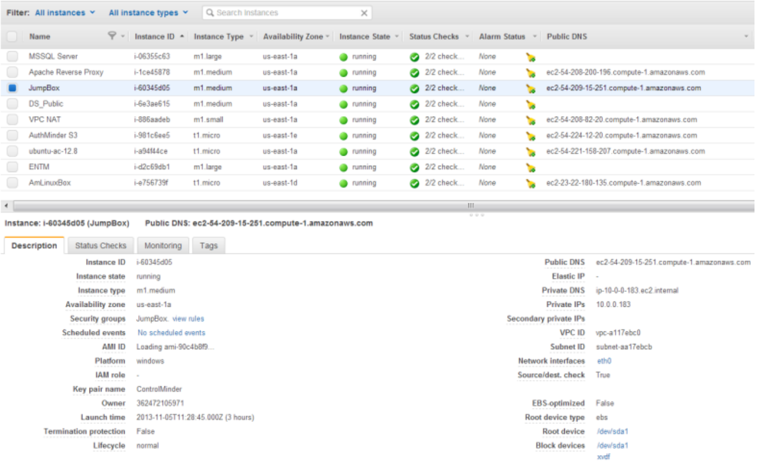
Select an instance above

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.

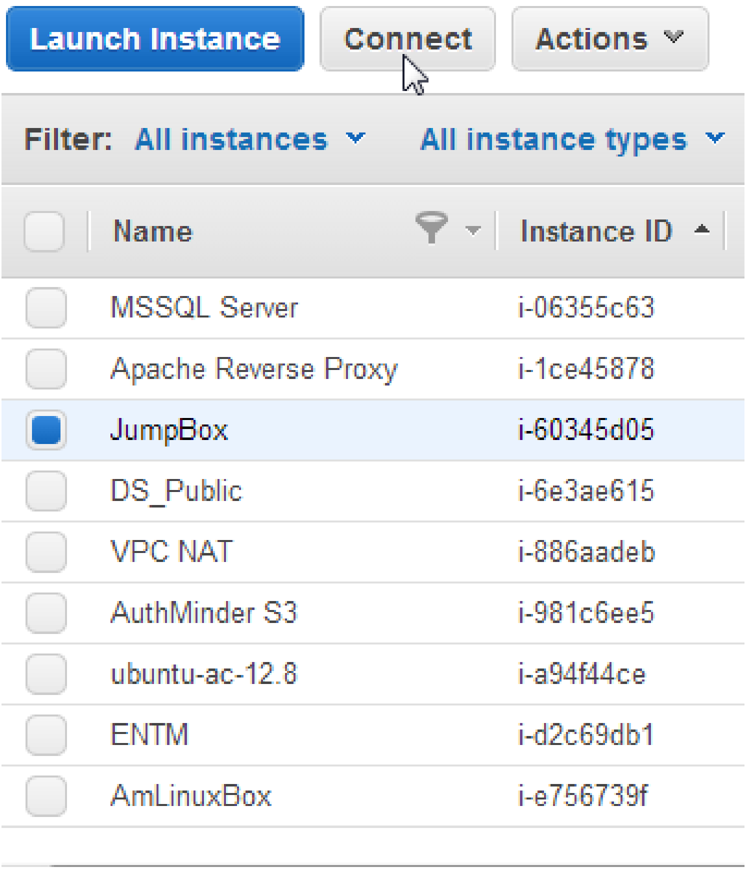


☐	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
☐	MSSQL Server	i-06355c63	m1.large	us-east-1a	● running	✓ 2/2 check...	None	
☐	Apache Reverse Proxy	i-1ce45878	m1.medium	us-east-1a	● running	✓ 2/2 check...	None	ec2-54-208-200-196.compute-1.amazonaws.com
■	JumpBox	i-60345d05	m1.medium	us-east-1a	● running	✓ 2/2 check...	None	ec2-54-209-15-251.compute-1.amazonaws.com
☐	DS_Public	i-6e3ae615	m1.medium	us-east-1a	● running	✓ 2/2 check...	None	
☐	VPC NAT	i-886aadeb	m1.small	us-east-1a	● running	✓ 2/2 check...	None	ec2-54-208-82-20.compute-1.amazonaws.com
☐	AuthMinder S3	i-981c6ee5	t1.micro	us-east-1e	● running	✓ 2/2 check...	None	ec2-54-224-12-20.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	
☐	AmLinuxBox	i-e756739f	t1.micro	us-east-1d	● running	✓ 2/2 check...	None	ec2-23-22-180-135.compute-1.amazonaws.com

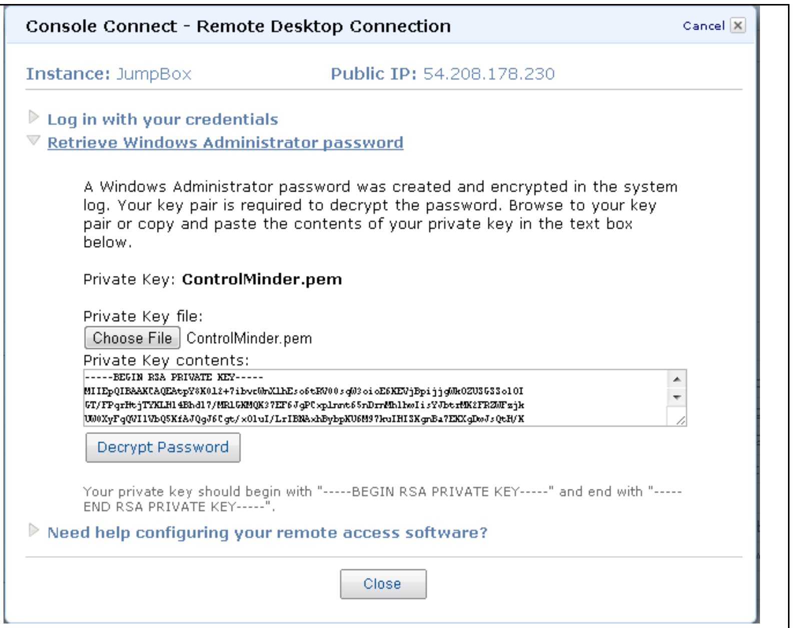
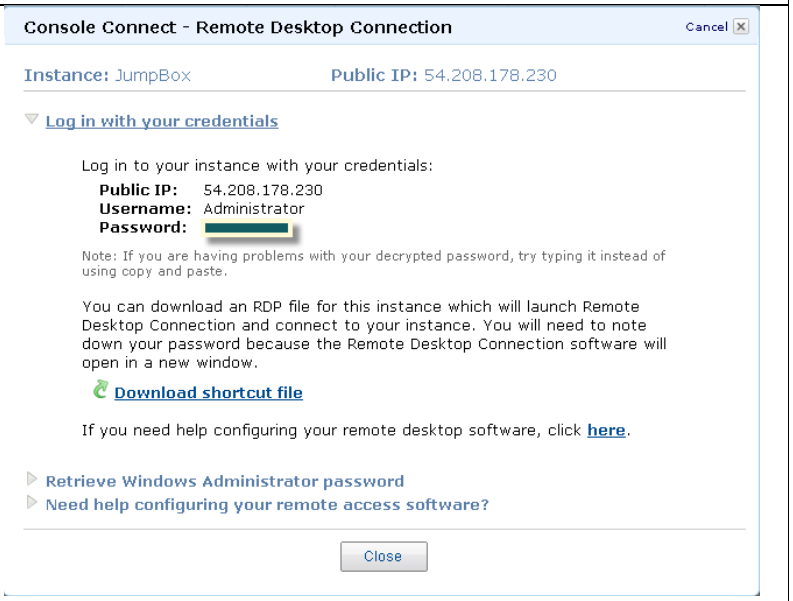
Instance: i-60345d05 (JumpBox) Public DNS: ec2-54-209-15-251.compute-1.amazonaws.com

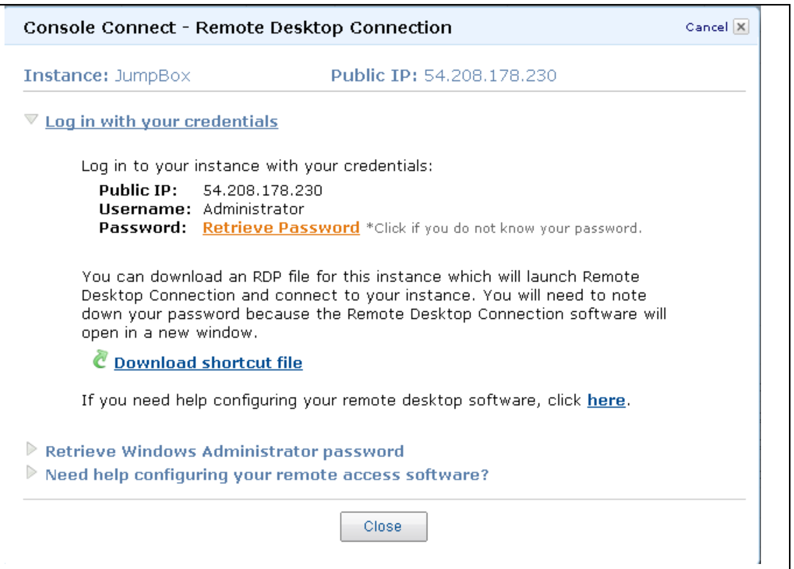
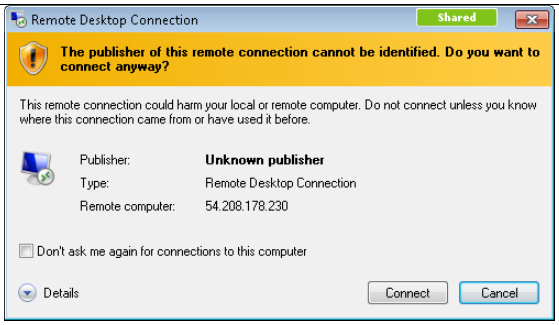
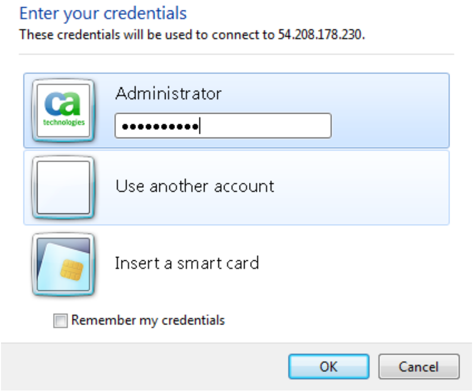
Instance ID	i-60345d05	Public DNS	ec2-54-209-15-251.compute-1.amazonaws.com
Instance state	running	Elastic IP	-
Instance type	m1.medium	Private DNS	ip-10-0-0-183.ec2.internal
Availability zone	us-east-1a	Private IPs	10.0.0.183
Security groups	JumpBox. view rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-a117ebc0
AMI ID	Loading ami-90c4b8f9...	Subnet ID	subnet-aa17ebcb
Platform	windows	Network interfaces	eth0
IAM role	-	Source/dest. check	True
Key pair name	ControlMinder		
Owner	362472105971	EBS-optimized	False
Launch time	2013-11-05T11:28:45.000Z (3 hours)	Root device type	ebs
Termination protection	False	Root device	/dev/sda1
Lifecycle	normal	Block devices	/dev/sda1 xvdf

Click “Connect”.



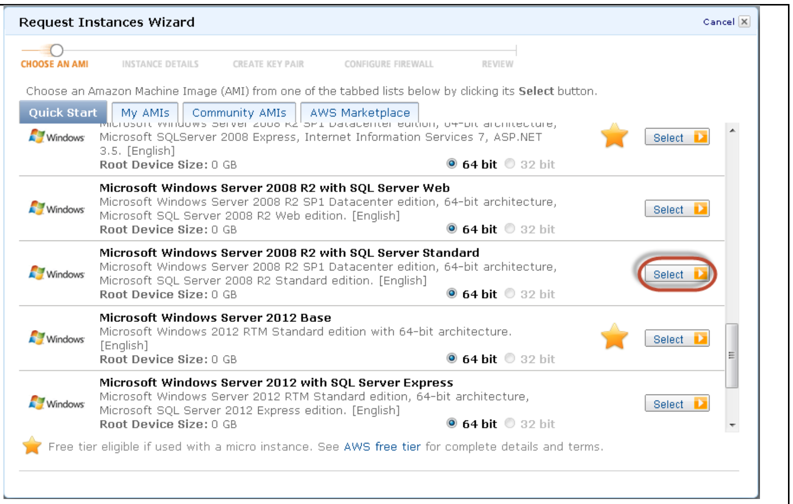
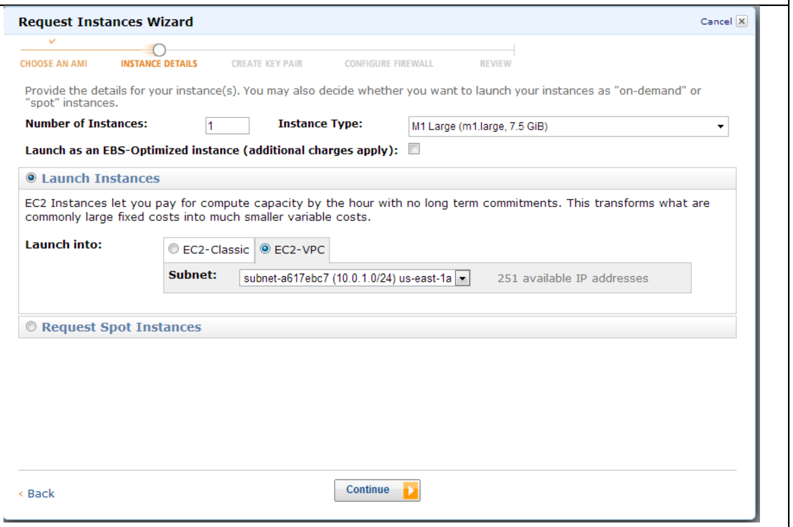
☐	Name	Instance ID
☐	MSSQL Server	i-06355c63
☐	Apache Reverse Proxy	i-1ce45878
■	JumpBox	i-60345d05
☐	DS_Public	i-6e3ae615
☐	VPC NAT	i-886aadeb
☐	AuthMinder S3	i-981c6ee5
☐	ubuntu-ac-12.8	i-a94f44ce
☐	ENTM	i-d2c69db1
☐	AmLinuxBox	i-e756739f

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 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----- MIIEpQIBAAKCAQEAtpY8K0l2+7ibvc0nXlhEso6tRV00sq03oioE6KEVjBpijjg0k0ZUSGS3ol0I GT/FPqrHtjTYKLHl4Bhdl7/MRlGKMQK37EF6JgPCxplnnt65nDrrMhlhwIisYJbtrMK2FRZWFzjk UW0XyFqQVIlVbQ5KfAJQgJ6Cgt/x0luI/LrIBNAxhBybpKU6M97kuIHISKgnBa7EKXgDwJsQtH/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 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:** [redacted] 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?

Click “Download shortcut file”	 Console Connect - Remote Desktop Connection Cancel ☒ 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:** Retrieve Password *Click if you do not know your password. 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? Close
Click the Connect button on the Remote Desktop Connection form.	 Remote Desktop Connection Shared **The publisher of this remote connection cannot be identified. Do you want to connect anyway?** This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before. Publisher: **Unknown publisher** Type: Remote Desktop Connection Remote computer: 54.208.178.230 □ Don't ask me again for connections to this computer Details Connect Cancel
Enter the credentials that will be used to connect to 54.208.178.230. From the JumpBox server you may connect to the ENTM server the Microsoft SQL server by starting RPD on the JumpBox server.	 Enter your credentials These credentials will be used to connect to 54.208.178.230. Administrator •••••••••• Use another account Insert a smart card □ Remember my credentials OK Cancel

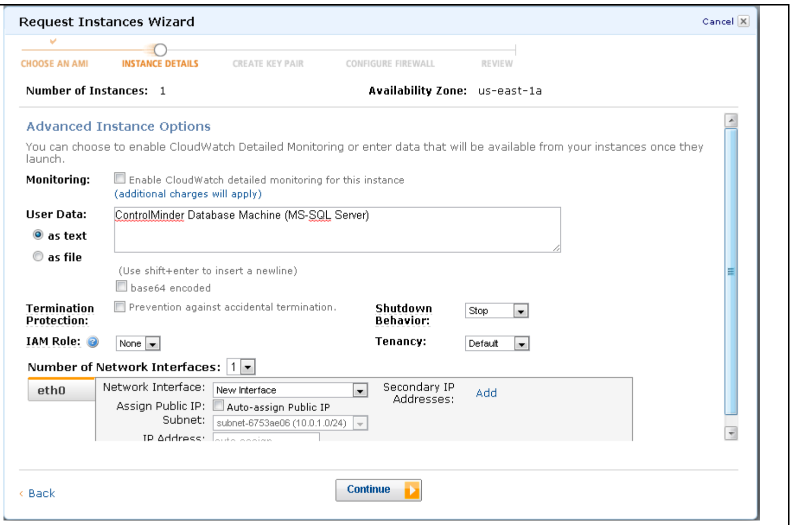
Deploying the RDBMS Using Microsoft SQL Server

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".	 Request Instances Wizard Cancel ☒ CHOOSE AN AMI · INSTANCE DETAILS · CREATE KEY PAIR · CONFIGURE FIREWALL · REVIEW Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its **Select** button. Quick Start · My AMIs · Community AMIs · AWS Marketplace Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQLServer 2008 Express, Internet Information Services 7, ASP.NET 3.5. [English] **Root Device Size:** 0 GB ● 64 bit ○ 32 bit — Select **Microsoft Windows Server 2008 R2 with SQL Server Web** Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQL Server 2008 R2 Web edition. [English] **Root Device Size:** 0 GB ● 64 bit ○ 32 bit — Select **Microsoft Windows Server 2008 R2 with SQL Server Standard** Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQL Server 2008 R2 Standard edition. [English] **Root Device Size:** 0 GB ● 64 bit ○ 32 bit — Select **Microsoft Windows Server 2012 Base** Microsoft Windows 2012 RTM Standard edition with 64-bit architecture. [English] **Root Device Size:** 0 GB ● 64 bit ○ 32 bit — Select **Microsoft Windows Server 2012 with SQL Server Express** Microsoft Windows Server 2012 RTM Standard edition, 64-bit architecture, Microsoft SQL Server 2012 Express edition. [English] **Root Device Size:** 0 GB ● 64 bit ○ 32 bit — Select Free tier eligible if used with a micro instance. See AWS free tier for complete details and terms.
Deploy the instance on the private subnet.	 Request Instances Wizard Cancel ☒ CHOOSE AN AMI · INSTANCE DETAILS · CREATE KEY PAIR · CONFIGURE FIREWALL · REVIEW Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances. **Number of Instances:** 1 **Instance Type:** M1 Large (m1.large, 7.5 GiB) **Launch as an EBS-Optimized instance (additional charges apply):** □ ● **Launch Instances** EC2 Instances let you pay for compute capacity by the hour with no long term commitments. This transforms what are commonly large fixed costs into much smaller variable costs. **Launch into:** ○ EC2-Classic ● EC2-VPC **Subnet:** subnet-a617ebc7 (10.0.1.0/24) us-east-1a 251 available IP addresses ○ **Request Spot Instances** ‹ Back · Continue

Provide “User data” to identify your instance.

Click the Continue button.



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

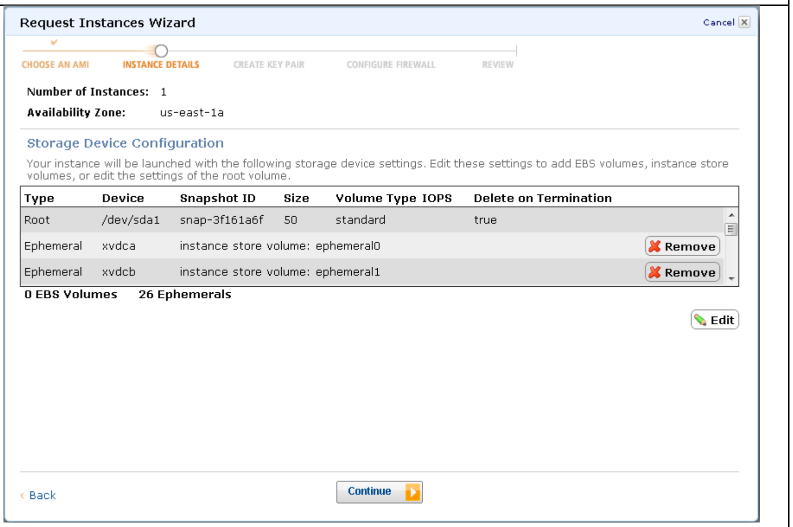
Assign Public IP: □ Auto-assign Public IP

Subnet: subnet-6753ae06 (10.0.1.0/24)

IP Address: auto-assign

Secondary IP Addresses: Add

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



Number of Instances: 1

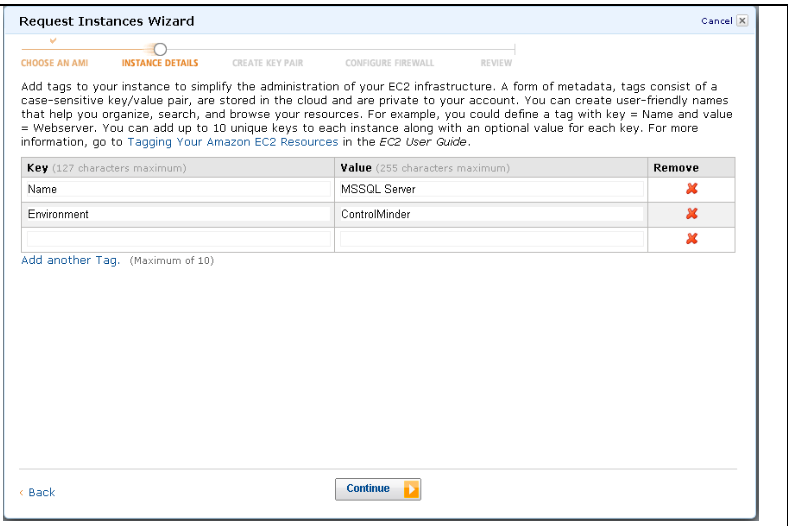
Availability Zone: us-east-1a

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	xvdca	instance store volume: ephemeral0					Remove
Ephemeral	xvdcb	instance store volume: ephemeral1					Remove

0 EBS Volumes   26 Ephemerals

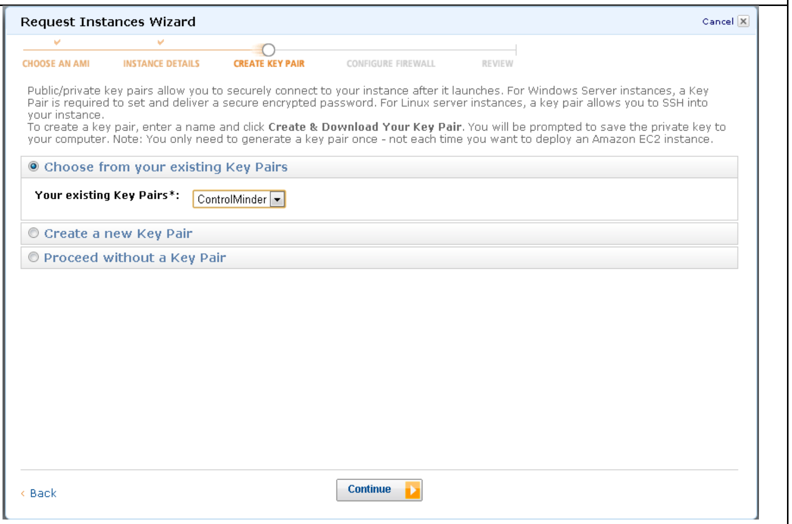
<table>
<tr>
<td>Name your instance and provide any additional tags as required.</td>
<td>


Request Instances Wizard

Add tags to your instance to simplify the administration of your EC2 infrastructure. A form of metadata, tags consist of a case-sensitive key/value pair, are stored in the cloud and are private to your account. You can create user-friendly names that help you organize, search, and browse your resources. For example, you could define a tag with key = Name and value = Webserver. You can add up to 10 unique keys to each instance along with an optional value for each key. For more information, go to Tagging Your Amazon EC2 Resources in the *EC2 User Guide*.

<table>
<tr><th>Key (127 characters maximum)</th><th>Value (255 characters maximum)</th><th>Remove</th></tr>
<tr><td>Name</td><td>MSSQL Server</td><td>✗</td></tr>
<tr><td>Environment</td><td>ControlMinder</td><td>✗</td></tr>
<tr><td></td><td></td><td>✗</td></tr>
</table>

Add another Tag. (Maximum of 10)

</td>
</tr>
<tr>
<td>Use the key pair associated you're your AWS ECS Account.</td>
<td>


Request Instances Wizard

Public/private key pairs allow you to securely connect to your instance after it launches. For Windows Server instances, a Key Pair is required to set and deliver a secure encrypted password. For Linux server instances, a key pair allows you to SSH into your instance.
To create a key pair, enter a name and click **Create & Download Your Key Pair**. You will be prompted to save the private key to your computer. Note: You only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.

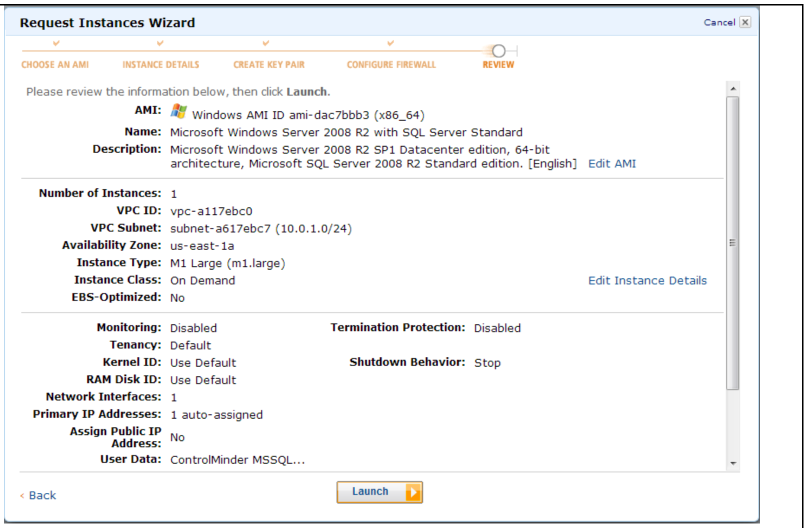
● Choose from your existing Key Pairs

Your existing Key Pairs*: ControlMinder

○ Create a new Key Pair

○ Proceed without a Key Pair

</td>
</tr>
<tr>
<td>Add the Default_Private Security Group to this instance.</td>
<td></td>
</tr>
</table>

Launch the instance by clicking the Launch button.	

Request Instances Wizard

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)
Instance Class: On Demand
EBS-Optimized: No
Edit Instance Details

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...

Preparing the Database

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

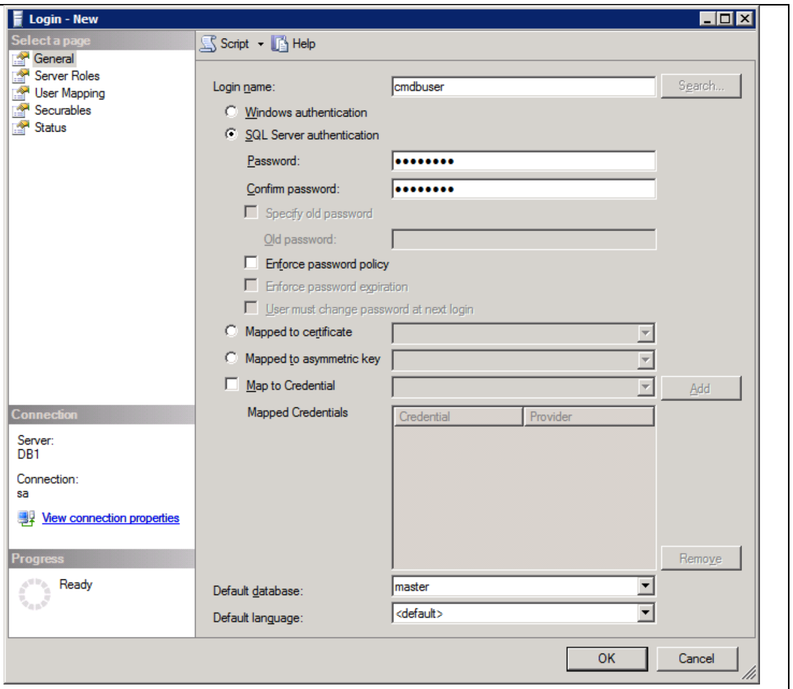
You can obtain the IP address of the Microsoft SQL Server from its instance properties.

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.



Login name: cmdbuser

○ Windows authentication

● SQL Server authentication

Password: ••••••••

Confirm password: ••••••••

☐ Specify old password

Old password:

☐ Enforce password policy

☐ Enforce password expiration

☐ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

☐ Map to Credential

Mapped Credentials

Credential	Provider

Default database: master

Default language: <default>

Server: DB1

Connection: sa

Ready

Create the database

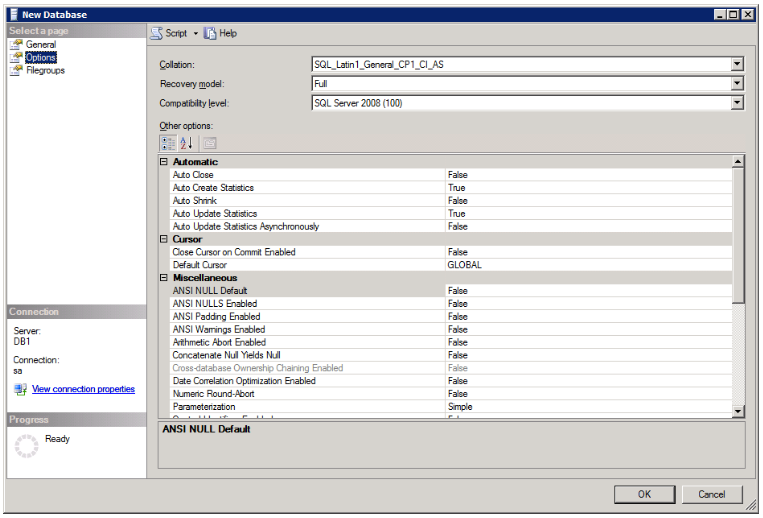
When creating the database, set Collation to:

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.



Collation: SQL_Latin1_General_CP1_CI_AS

Recovery model: Full

Compatibility level: SQL Server 2008 (100)

Other options:

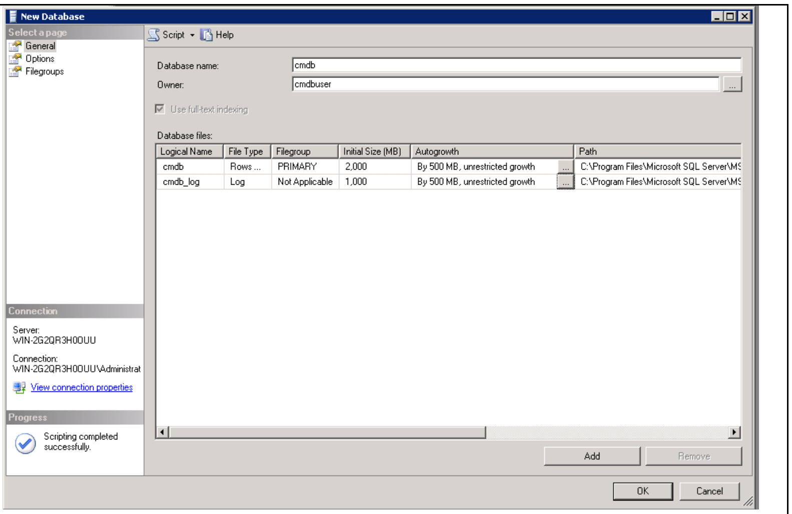
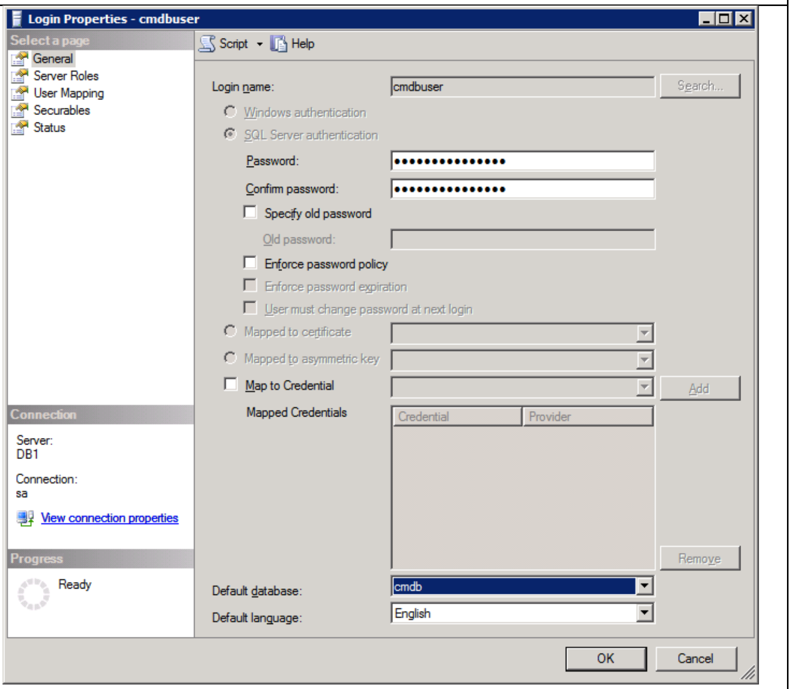
Automatic	
Auto Close	False
Auto Create Statistics	True
Auto Shrink	False
Auto Update Statistics	True
Auto Update Statistics Asynchronously	False
Cursor	
Close Cursor on Commit Enabled	False
Default Cursor	GLOBAL
Miscellaneous	
ANSI NULL Default	False
ANSI NULLS Enabled	False
ANSI Padding Enabled	False
ANSI Warnings Enabled	False
Arithmetic Abort Enabled	False
Concatenate Null Yields Null	False
Cross-database Ownership Chaining Enabled	False
Date Correlation Optimization Enabled	False
Numeric Round-Abort	False
Parameterization	Simple

ANSI NULL Default

Server: DB1

Connection: sa

Ready

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.	

New Database

Database name: cmdb

Owner: cmdbuser

☑ Use full-text indexing

Database files:

Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth	Path
cmdb	Rows ...	PRIMARY	2,000	By 500 MB, unrestricted growth	C:\Program Files\Microsoft SQL Server\MS
cmdb_log	Log	Not Applicable	1,000	By 500 MB, unrestricted growth	C:\Program Files\Microsoft SQL Server\MS

Server: WIN-2G2QR3H00UU

Connection: WIN-2G2QR3H00UU\Administrat

Scripting completed successfully.

Login Properties - cmdbuser

Login name: cmdbuser

○ Windows authentication

● SQL Server authentication

Password: •••••••••••••••

Confirm password: •••••••••••••••

☐ Specify old password

Old password:

☐ Enforce password policy

☐ Enforce password expiration

☐ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

☐ Map to Credential

Mapped Credentials

Credential	Provider

Default database: cmdb

Default language: English

Server: DB1

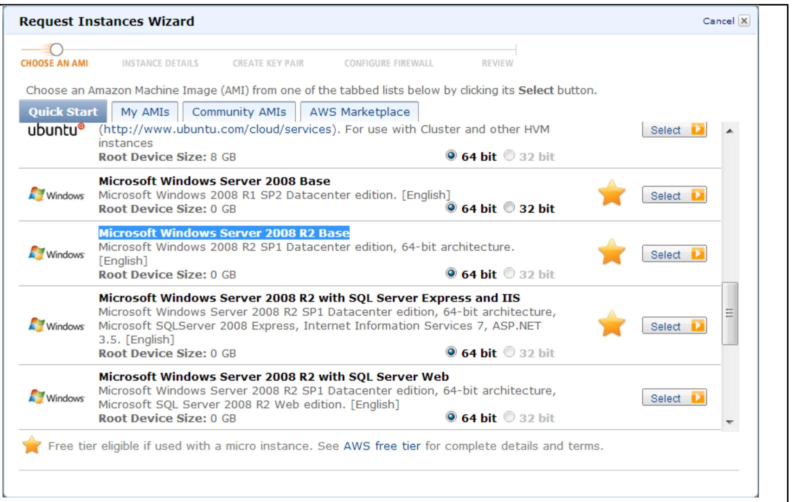
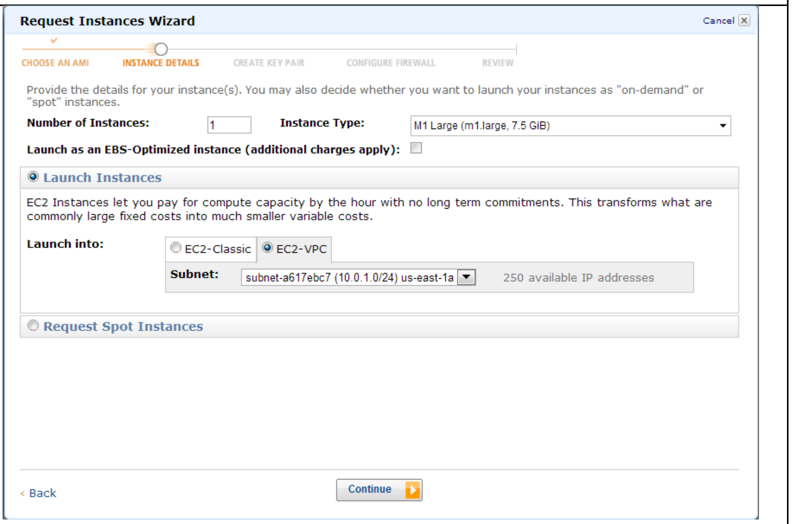
Connection: sa

Ready

Deploying Enterprise Management

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

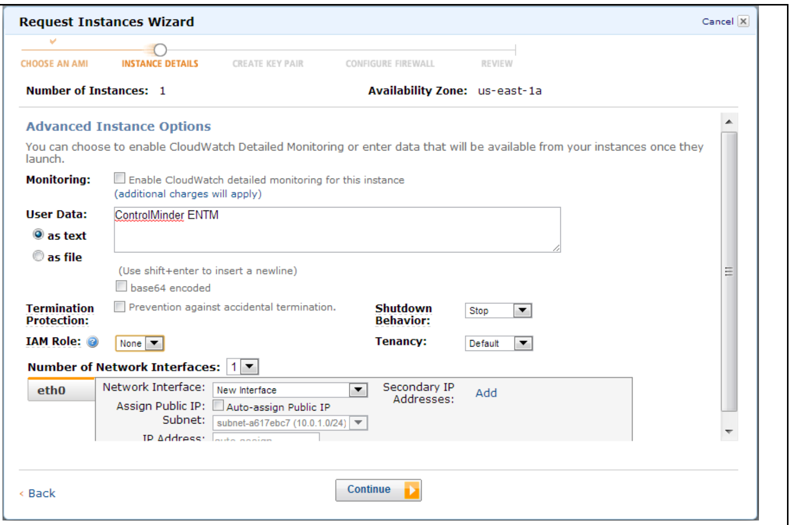
Create ENTM Instance

Create another instance using the Classic Wizard. Select "Microsoft Windows Server 2008 R2 Base" 64 bit.	 Request Instances Wizard Cancel CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW Quick Start My AMIs Community AMIs AWS Marketplace Select Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its **Select** button. ubuntu (http://www.ubuntu.com/cloud/services). For use with Cluster and other HVM instances **Root Device Size:** 8 GB ● 64 bit ○ 32 bit **Microsoft Windows Server 2008 Base** Microsoft Windows 2008 R1 SP2 Datacenter edition. [English] **Root Device Size:** 0 GB ● 64 bit ○ 32 bit **Microsoft Windows Server 2008 R2 Base** Microsoft Windows 2008 R2 SP1 Datacenter edition, 64-bit architecture. [English] **Root Device Size:** 0 GB ● 64 bit ○ 32 bit **Microsoft Windows Server 2008 R2 with SQL Server Express and IIS** Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQLServer 2008 Express, Internet Information Services 7, ASP.NET 3.5. [English] **Root Device Size:** 0 GB ● 64 bit ○ 32 bit **Microsoft Windows Server 2008 R2 with SQL Server Web** Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQL Server 2008 R2 Web edition. [English] **Root Device Size:** 0 GB ● 64 bit ○ 32 bit Free tier eligible if used with a micro instance. See AWS free tier for complete details and terms.
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.	 Request Instances Wizard Cancel CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW Back Continue Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances. **Number of Instances:** 1 **Instance Type:** M1 Large (m1.large, 7.5 GiB) **Launch as an EBS-Optimized instance (additional charges apply):** □ ● **Launch Instances** EC2 Instances let you pay for compute capacity by the hour with no long term commitments. This transforms what are commonly large fixed costs into much smaller variable costs. **Launch into:** ○ EC2-Classic ● EC2-VPC **Subnet:** subnet-a617ebc7 (10.0.1.0/24) us-east-1a 250 available IP addresses ○ **Request Spot Instances**

Provide User Data to identify your instance.

Keep default values for all other Settings.

Click the Continue button.



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 ENTM

● 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

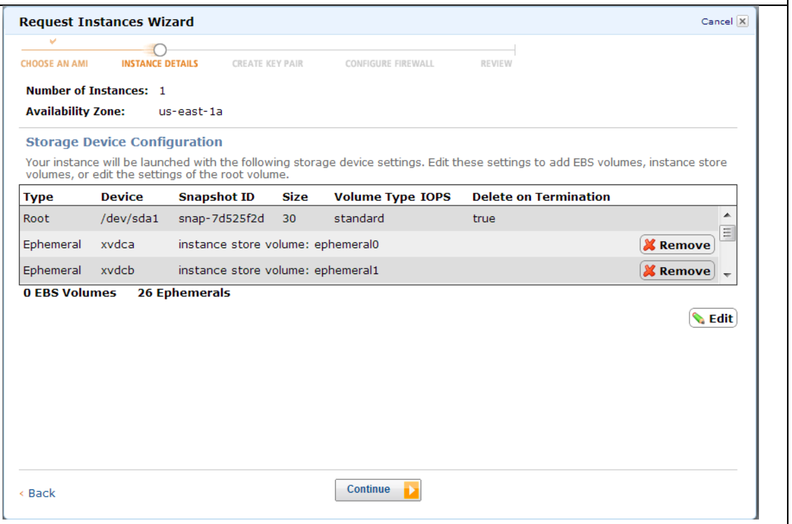
Number of Network Interfaces: 1

eth0

Network Interface: New Interface
Assign Public IP: □ Auto-assign Public IP
Subnet: subnet-a617ebc7 (10.0.1.0/24)
IP Address: auto assign
Secondary IP Addresses: Add

Click the Continue button.

30 gigabytes of disk storage is sufficient for the ENTM Server.



Number of Instances: 1

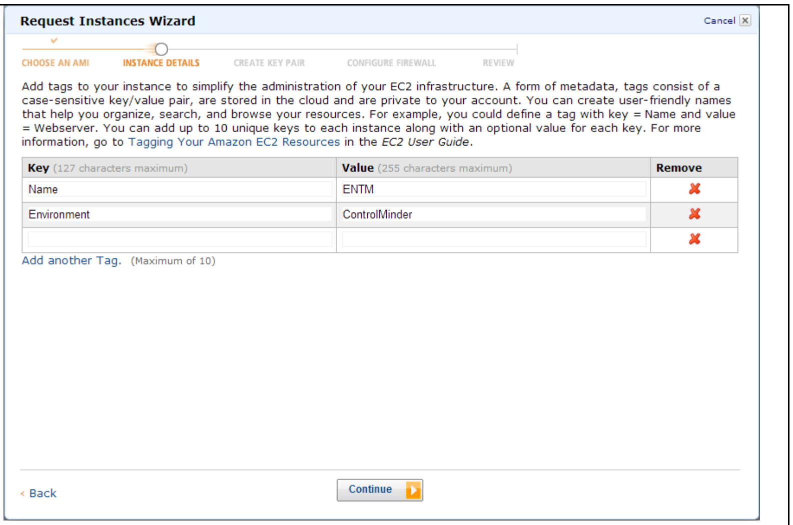
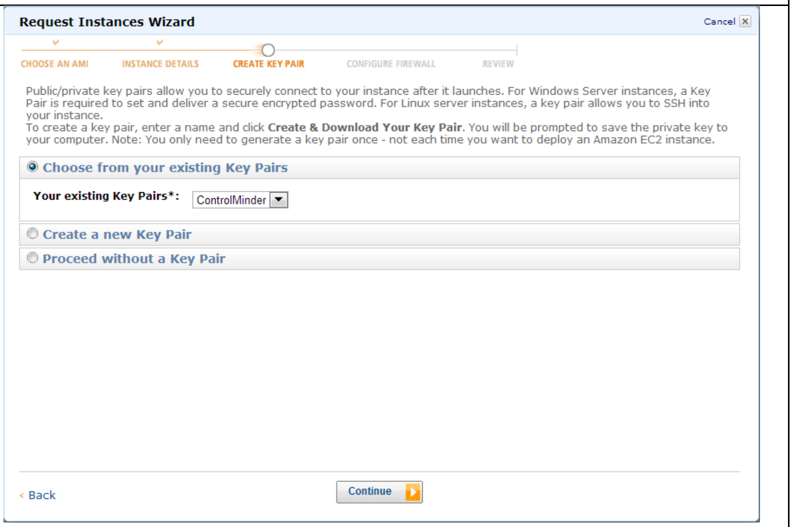
Availability Zone: us-east-1a

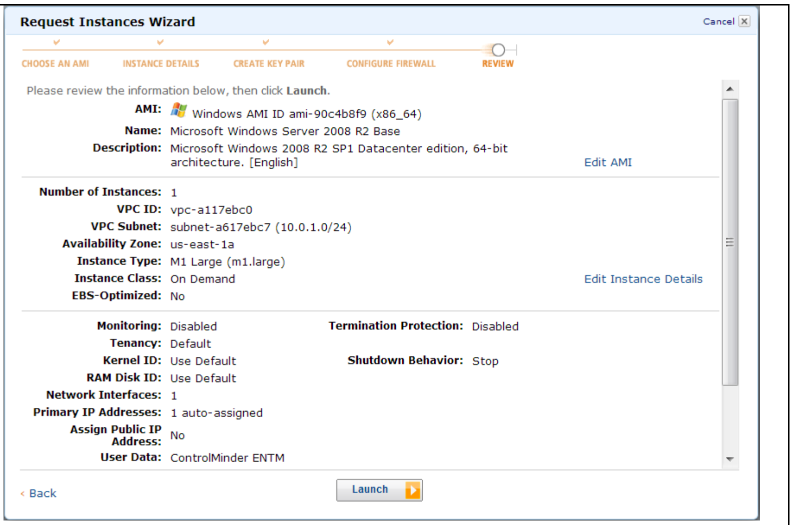
Storage Device Configuration

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-7d525f2d	30	standard		true	
Ephemeral	xvdca	instance store volume: ephemeral0					Remove
Ephemeral	xvdcb	instance store volume: ephemeral1					Remove

0 EBS Volumes **26 Ephemerals**

Name your instance and provide any additional tags as required.	 **Request Instances Wizard** Cancel ☒ CHOOSE AN AMI ✓ INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW Add tags to your instance to simplify the administration of your EC2 infrastructure. A form of metadata, tags consist of a case-sensitive key/value pair, are stored in the cloud and are private to your account. You can create user-friendly names that help you organize, search, and browse your resources. For example, you could define a tag with key = Name and value = Webserver. You can add up to 10 unique keys to each instance along with an optional value for each key. For more information, go to Tagging Your Amazon EC2 Resources in the *EC2 User Guide*. **Key** (127 characters maximum) | **Value** (255 characters maximum) | **Remove** Name | ENTM | ✗ Environment | ControlMinder | ✗ | | ✗ Add another Tag. (Maximum of 10)
Use the key pair associated you're your AWS ECS Account.	 **Request Instances Wizard** Cancel ☒ CHOOSE AN AMI ✓ INSTANCE DETAILS ✓ CREATE KEY PAIR CONFIGURE FIREWALL REVIEW Public/private key pairs allow you to securely connect to your instance after it launches. For Windows Server instances, a Key Pair is required to set and deliver a secure encrypted password. For Linux server instances, a key pair allows you to SSH into your instance. To create a key pair, enter a name and click **Create & Download Your Key Pair**. You will be prompted to save the private key to your computer. Note: You only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance. ● Choose from your existing Key Pairs **Your existing Key Pairs*:** ControlMinder ▼ ○ Create a new Key Pair ○ Proceed without a Key Pair
Add the Default_Private Security Group to this instance	

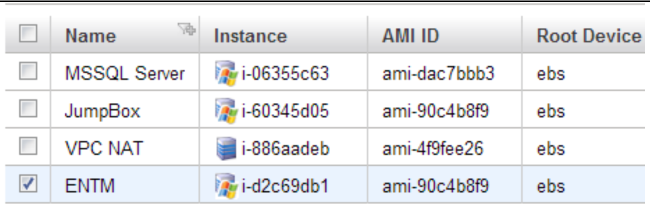
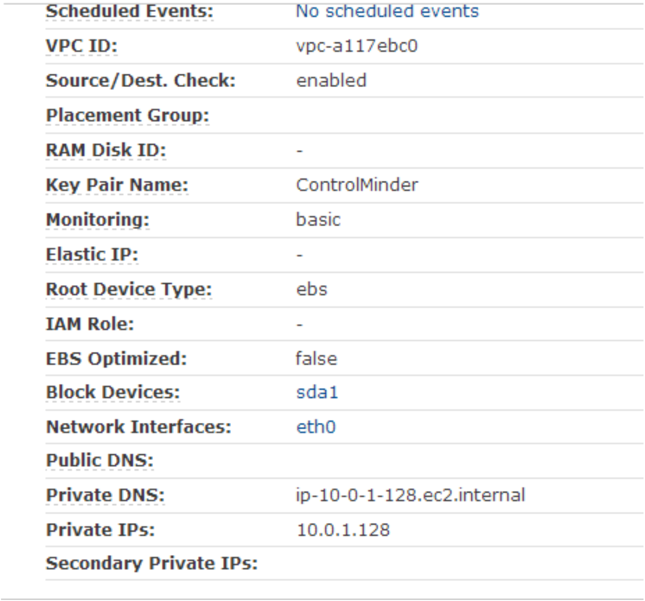
Launch the instance by clicking the Launch button.	 **Request Instances Wizard** Cancel ☒ CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW Please review the information below, then click **Launch**. **AMI:** Windows AMI ID ami-90c4b8f9 (x86_64) **Name:** Microsoft Windows Server 2008 R2 Base **Description:** Microsoft Windows 2008 R2 SP1 Datacenter edition, 64-bit architecture. [English] **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 **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

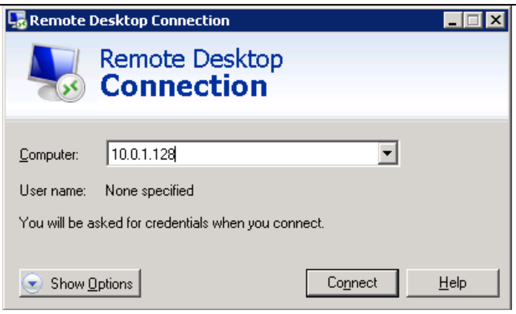
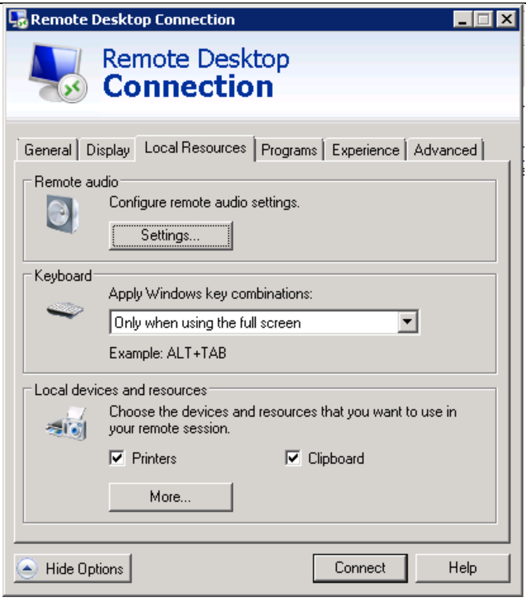
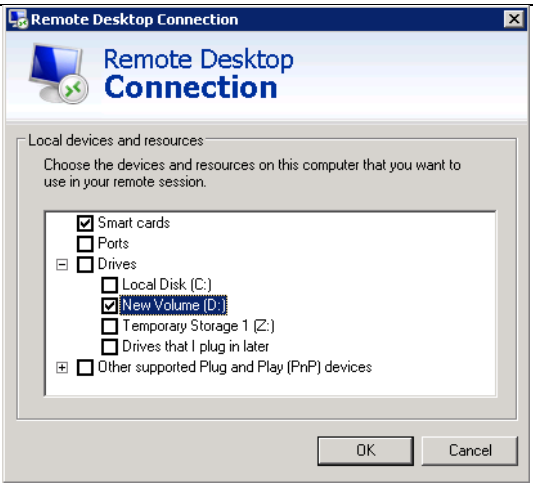
Transferring the Software

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

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

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

Go to the list of running instances on the EC2 dashboard and select the ENTM instance. Note the IP address of the ENTM server.	 □ Name | Instance | AMI ID | Root Device □ MSSQL Server | i-06355c63 | ami-dac7bbb3 | ebs □ JumpBox | i-60345d05 | ami-90c4b8f9 | ebs □ VPC NAT | i-886aadeb | ami-4f9fee26 | ebs ☑ ENTM | i-d2c69db1 | ami-90c4b8f9 | ebs  Scheduled Events: No scheduled events VPC ID: vpc-a117ebc0 Source/Dest. Check: enabled Placement Group: RAM Disk ID: - Key Pair Name: ControlMinder Monitoring: basic Elastic IP: - Root Device Type: ebs IAM Role: - EBS Optimized: false Block Devices: sda1 Network Interfaces: eth0 Public DNS: Private DNS: ip-10-0-1-128.ec2.internal Private IPs: 10.0.1.128 Secondary Private IPs:

From the JumpBox server, use Remote Desktop to connect to the ENTM Server. Before clicking the Connect button, click the Show Options button.	 Remote Desktop Connection Remote Desktop Connection Show Options Connect Help Computer: 10.0.1.128 User name: None specified You will be asked for credentials when you connect.
Click the Local Resources tab. Click the More button.	 Remote Desktop Connection Remote Desktop Connection General Display Local Resources Programs Experience Advanced Settings... More... Hide Options Connect Help Remote audio Configure remote audio settings. Keyboard Apply Windows key combinations: Only when using the full screen Example: ALT+TAB Local devices and resources Choose the devices and resources that you want to use in your remote session. ☑ Printers ☑ Clipboard
Select the local drive to the JumpBox server where you already downloaded the ControlMinder software. Click the OK button and then click the Connect button. To obtain the Windows Administrator password for the ENTM Server follow the same steps described as described for the JumpBox server. Copy the software to the Temporary Storage available on the ENTM Server.	 Remote Desktop Connection Remote Desktop Connection OK Cancel Local devices and resources Choose the devices and resources on this computer that you want to use in your remote session. ☑ Smart cards ☐ Ports ☐ Drives ☐ Local Disk (C:) ☑ New Volume (D:) ☐ Temporary Storage 1 (Z:) ☐ Drives that I plug in later ☐ Other supported Plug and Play (PnP) devices

ENTM Installation

Steps to install Enterprise Management include:

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

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

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

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

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

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

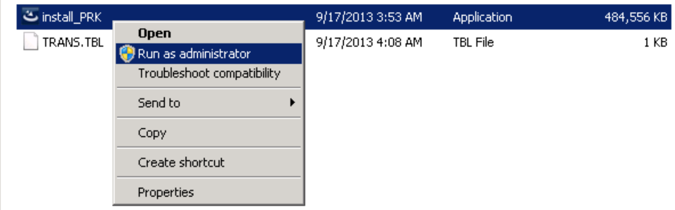
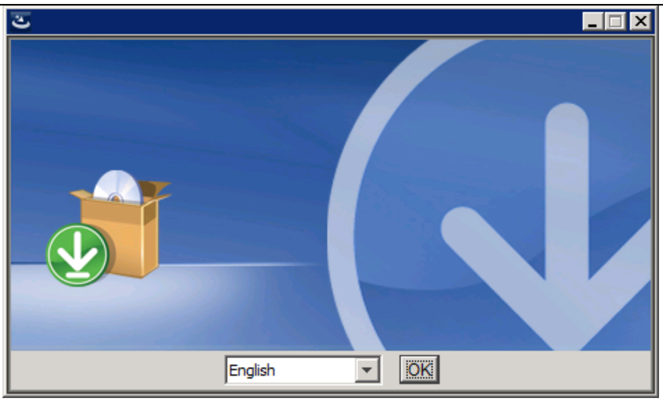
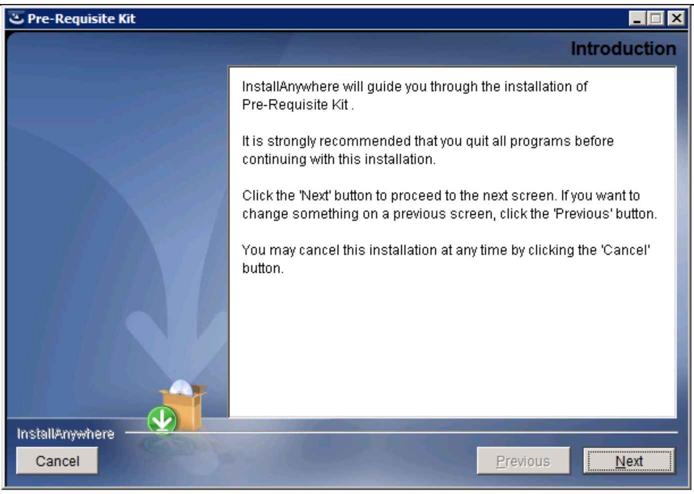
▪ JDK (from the Third-Party Components)	200 MB
▪ JBoss (from the Third-Party Components)	850 MB
▪ Enterprise Management	1.10 GB

Install Third-Party Components

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

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

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

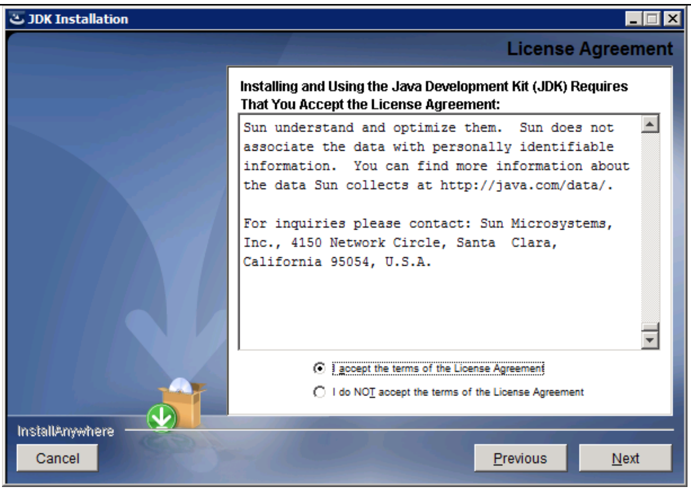
Locate install_PRK.exe found in the PrereqInstaller directory of the Third-Party Components ISO image. Start the installation by right-clicking **Install_PRK.exe** and selecting Run as administrator from the menu. This will install the Java Development Kit and JBoss.	 install_PRK 9/17/2013 3:53 AM Application 484,556 KB TRANS.TBL 9/17/2013 4:08 AM TBL File 1 KB Open Run as administrator Troubleshoot compatibility Send to Copy Create shortcut Properties
Click the OK button to accept English as the installation language.	
Click the Next button.	 InstallAnywhere will guide you through the installation of Pre-Requisite Kit . It is strongly recommended that you quit all programs before continuing with this installation. Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button. You may cancel this installation at any time by clicking the 'Cancel' button.

JDK Installation

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

Click the radial button noting I accept the terms of the License Agreement.

Click the Next button.



Installing and Using the Java Development Kit (JDK) Requires That You Accept the License Agreement:

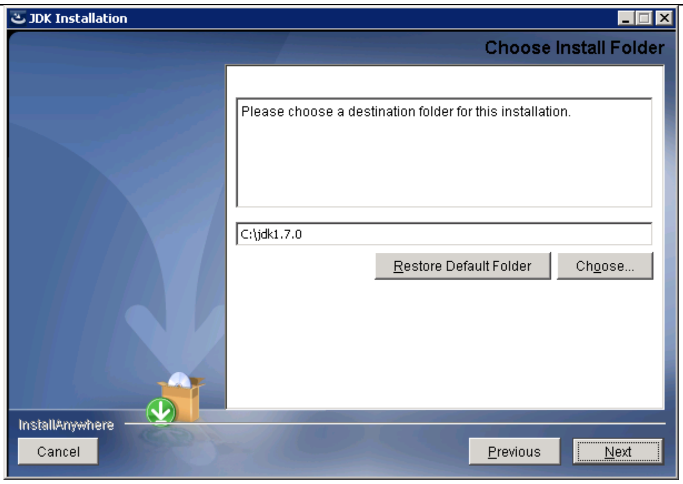
```
Sun understand and optimize them.  Sun does not
associate the data with personally identifiable
information.  You can find more information about
the data Sun collects at http://java.com/data/.

For inquiries please contact: Sun Microsystems,
Inc., 4150 Network Circle, Santa  Clara,
California 95054, U.S.A.
```

● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

Select the destination folder.

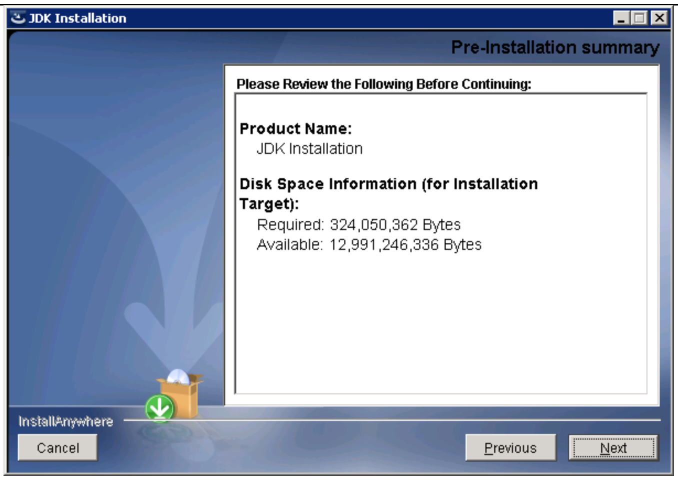
Click the Next button.



Please choose a destination folder for this installation.

C:\jdk1.7.0

Click the Next button.



Please Review the Following Before Continuing:

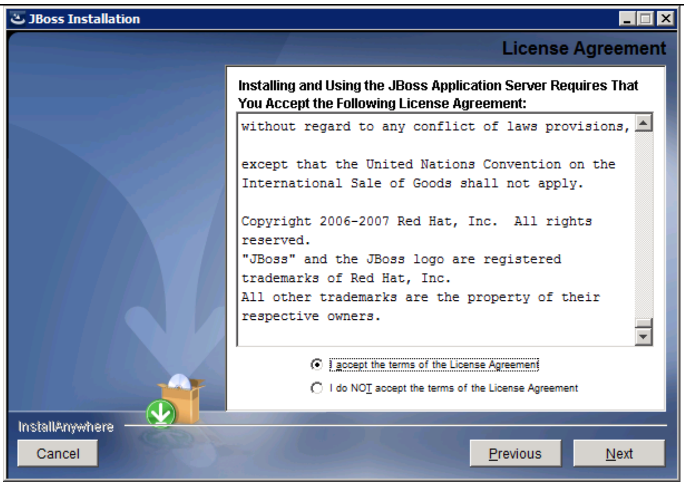
Product Name:
JDK Installation

Disk Space Information (for Installation Target):
Required: 324,050,362 Bytes
Available: 12,991,246,336 Bytes

JBoss Installation

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

Click the Next button.



Installing and Using the JBoss Application Server Requires That You Accept the Following License Agreement:

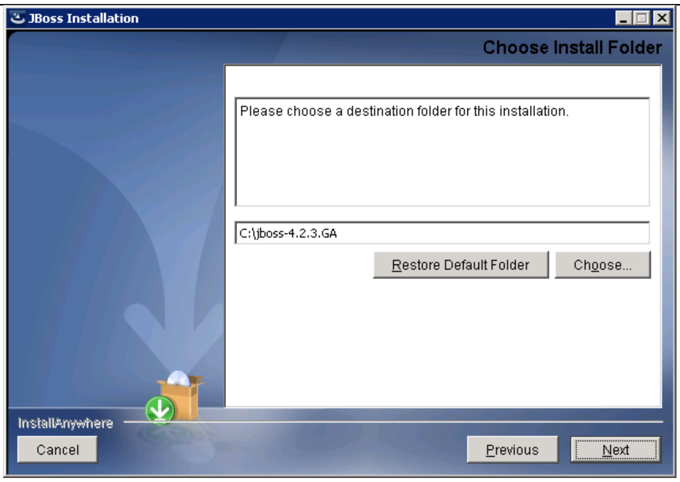
```
without regard to any conflict of laws provisions,

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.
```

● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

Select the destination folder.

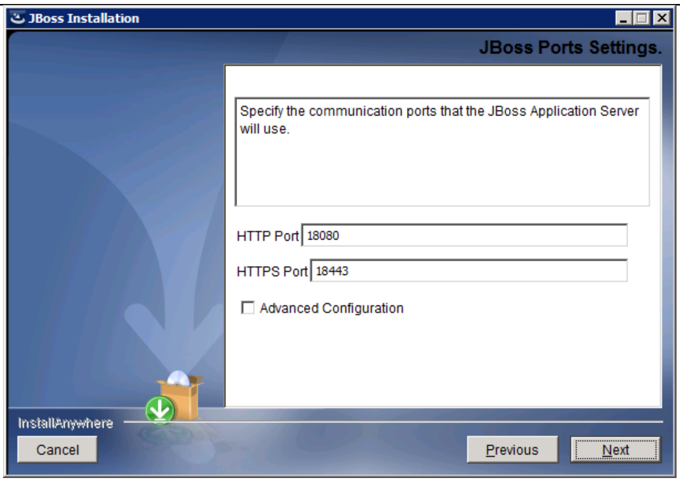
Click the Next button.



Please choose a destination folder for this installation.

C:\jboss-4.2.3.GA

Click the Next button.

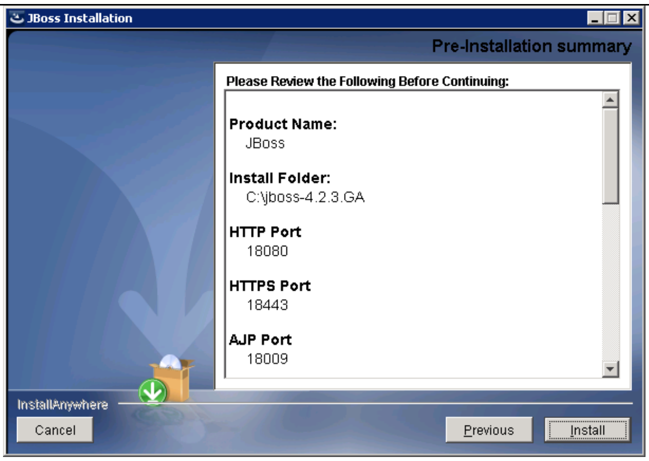
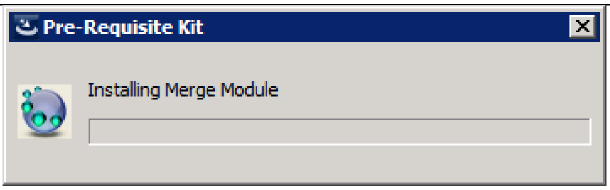


Specify the communication ports that the JBoss Application Server will use.

HTTP Port 18080

HTTPS Port 18443

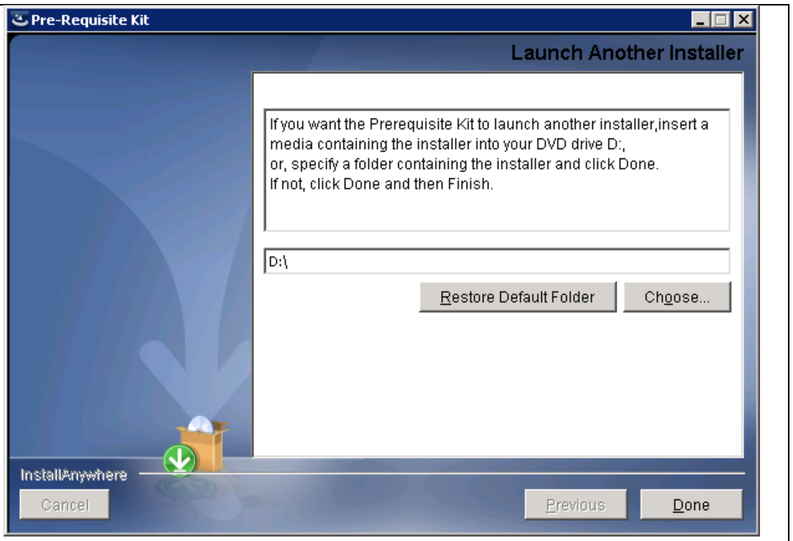
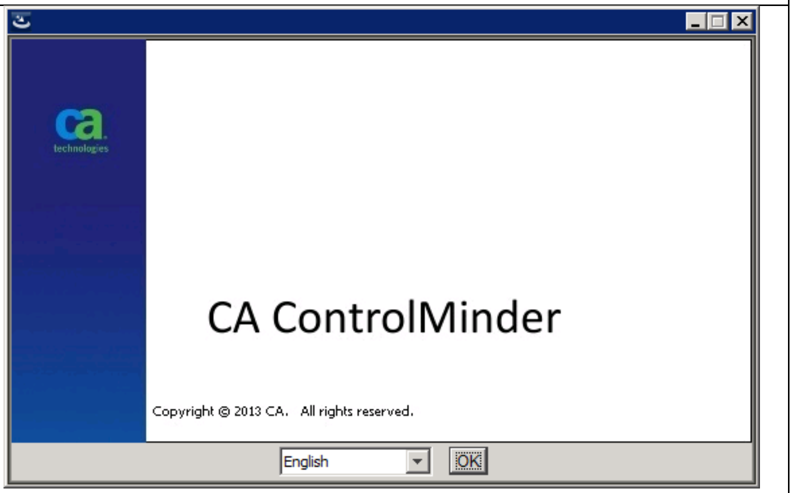
□ Advanced Configuration

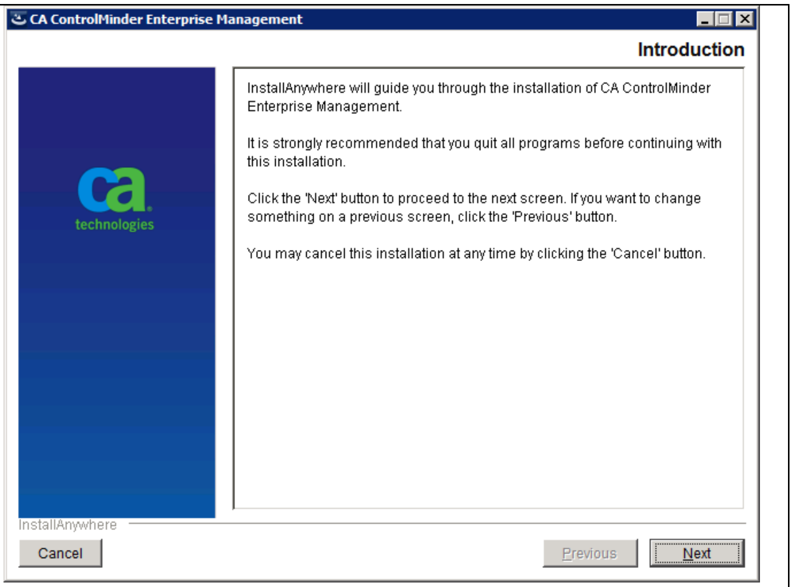
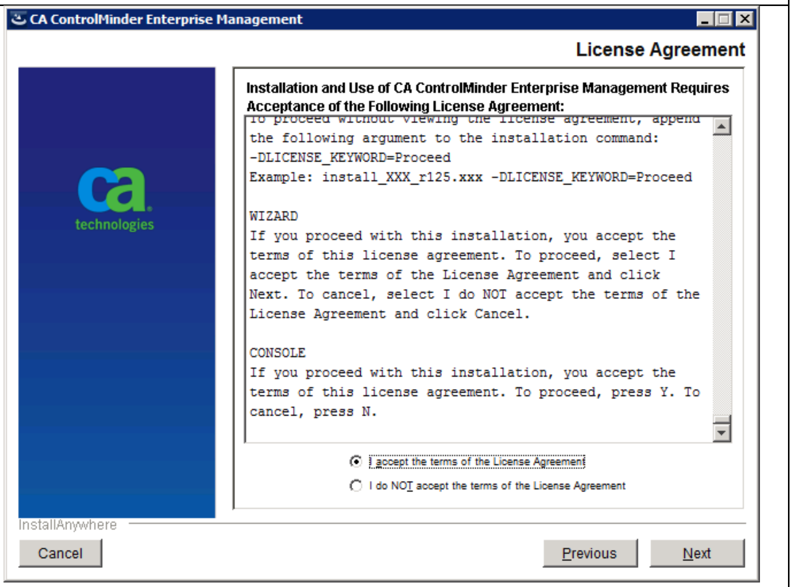
Click the Install button.	 JBoss Installation Pre-Installation summary Please Review the Following Before Continuing: Product Name: JBoss Install Folder: C:\jboss-4.2.3.GA HTTP Port 18080 HTTPS Port 18443 AJP Port 18009
Wait for installation to complete	 Installing Merge Module

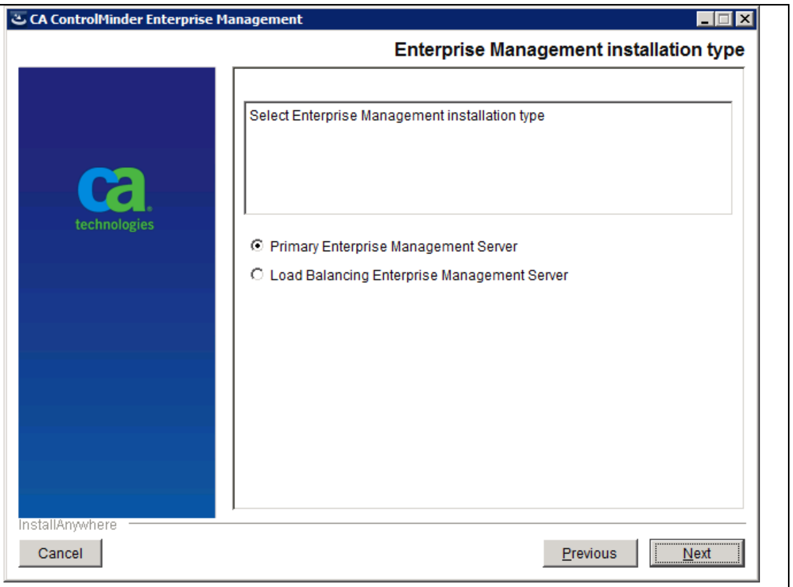
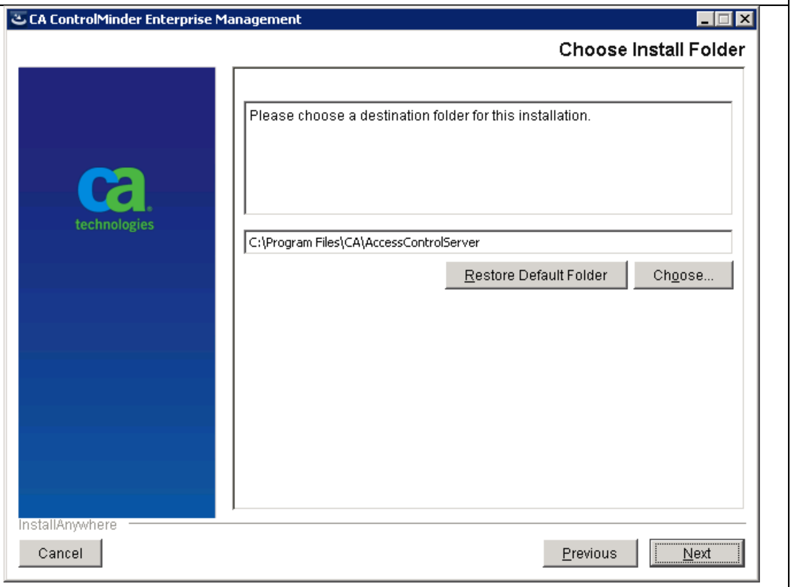
Install Enterprise Management

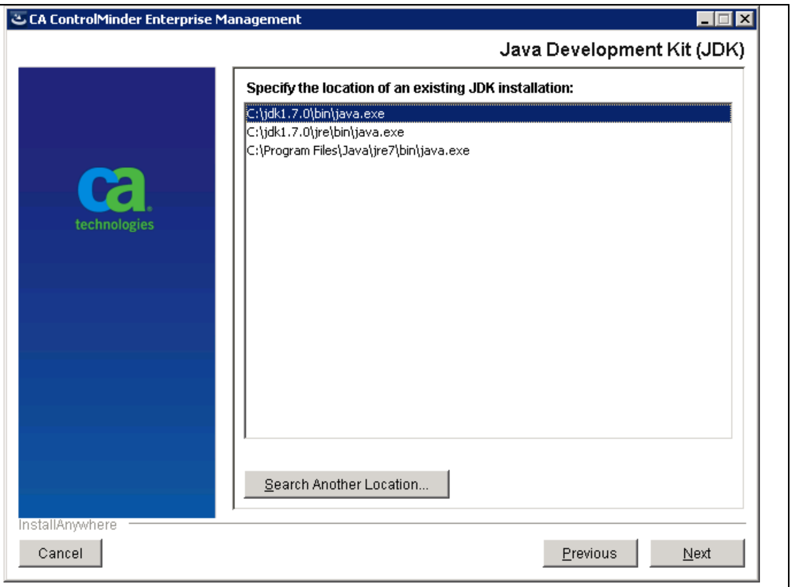
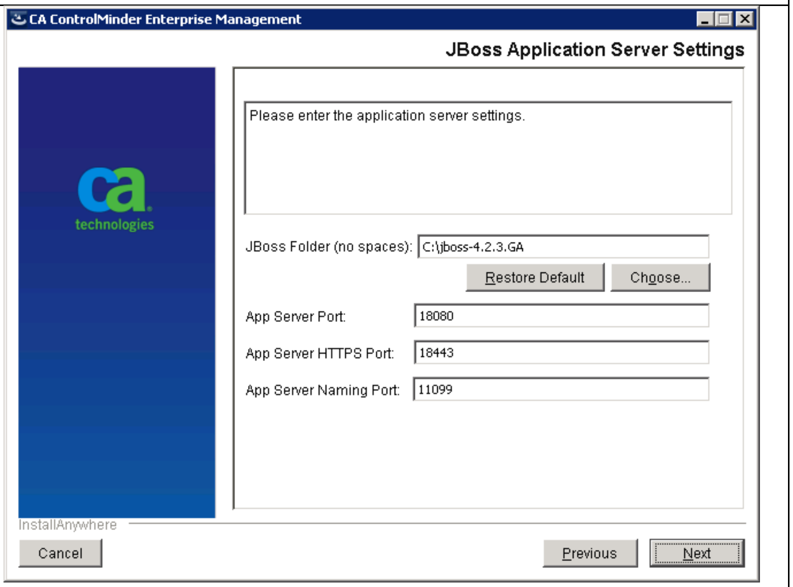
Either the Third-Party Components installer can launch the Enterprise Management installation, or you can manually start the installer by running ProductExplorer from the CA ControlMinder Server Components ISO image.

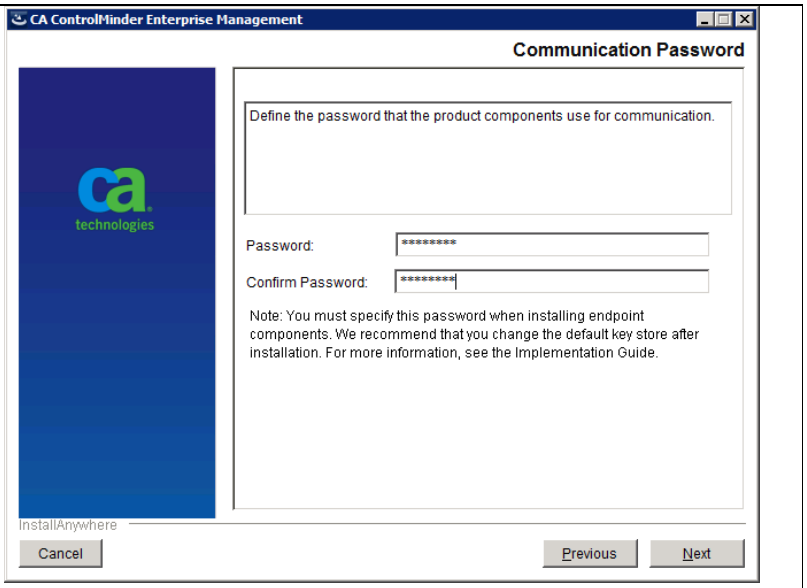
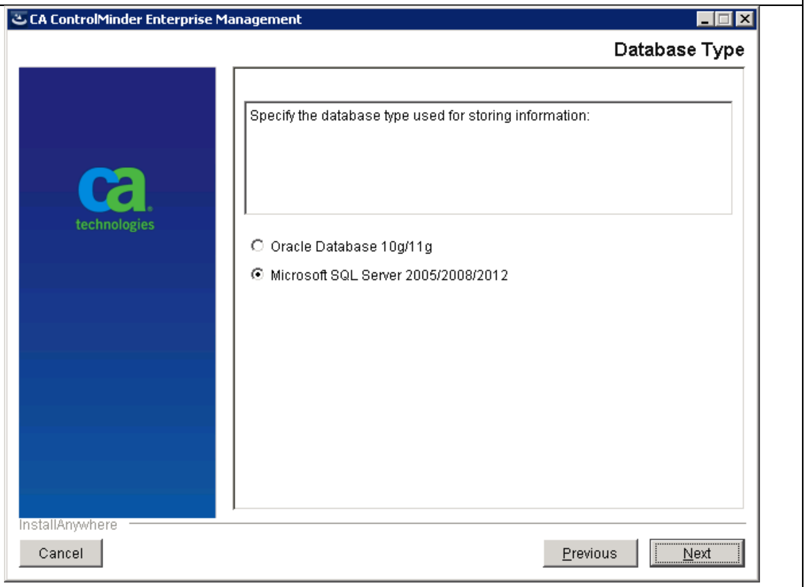
The following example has the Third-Party Components installer start the Enterprise Management installation.

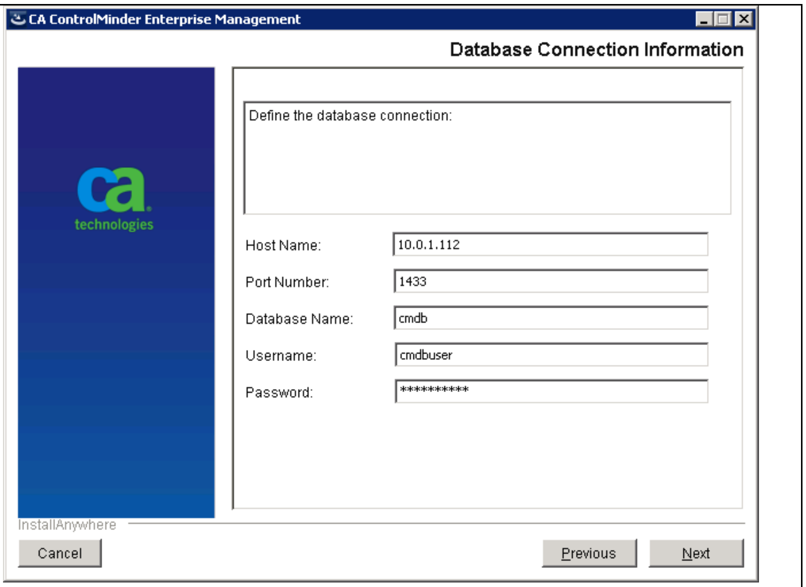
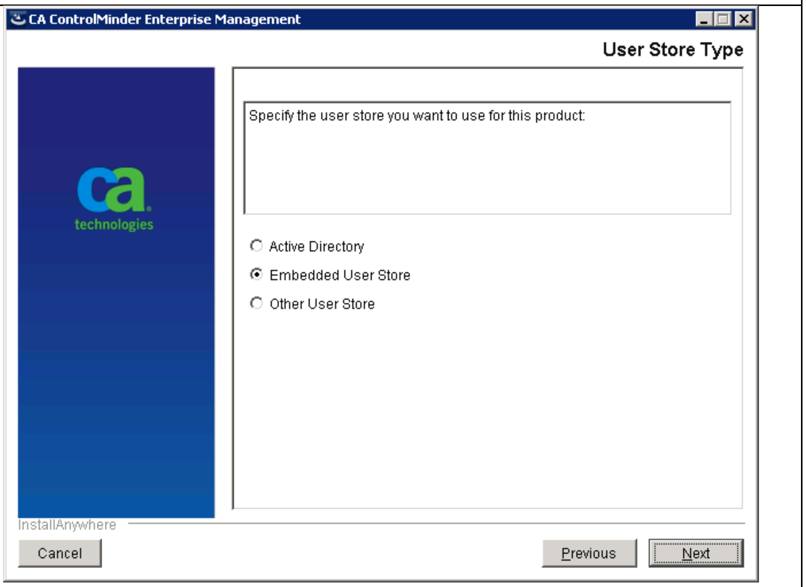
Mount the CA ControlMinder Server Components ISO image in the same virtual DVD drive where the Third-Party Components ISO image was installed. Click the Done button.	 Pre-Requisite Kit Launch Another Installer If you want the Prerequisite Kit to launch another installer,insert a media containing the installer into your DVD drive D:, or, specify a folder containing the installer and click Done. If not, click Done and then Finish. D:\ Restore Default Folder Choose... InstallAnywhere Cancel Previous Done
If ProductExplorer is started manually, select Enterprise Management from the available choices.	
Click the OK button to accept English as the installation language.	 CA ControlMinder Copyright © 2013 CA. All rights reserved. English

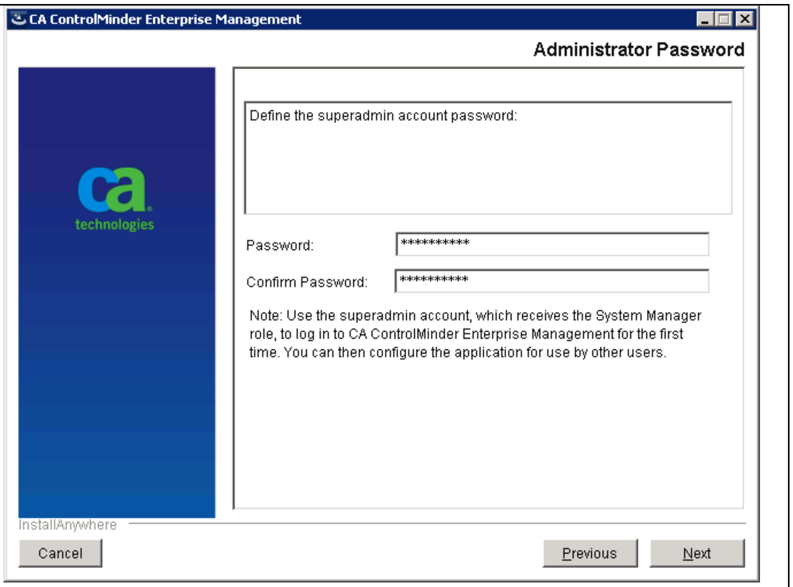
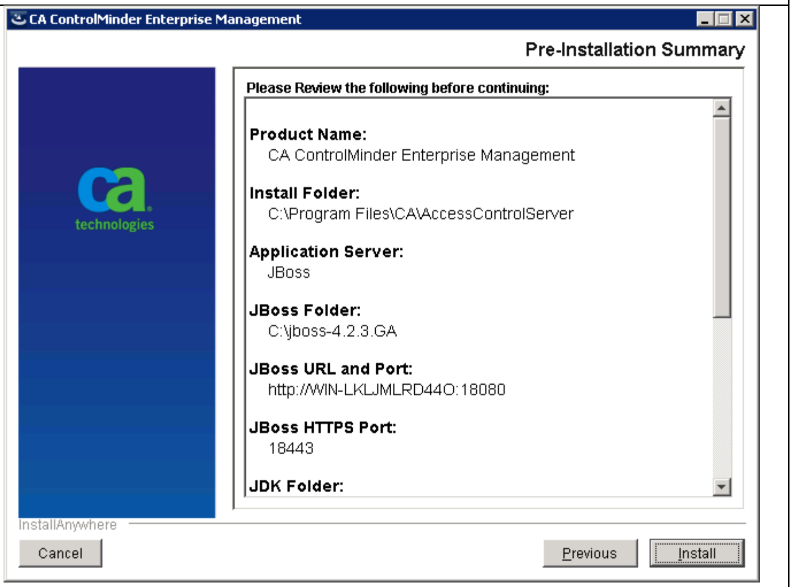
Click the Next button.	 CA ControlMinder Enterprise Management **Introduction** InstallAnywhere will guide you through the installation of CA ControlMinder Enterprise Management. It is strongly recommended that you quit all programs before continuing with this installation. Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button. You may cancel this installation at any time by clicking the 'Cancel' button. InstallAnywhere Cancel Previous Next
Read the License Agreement as you use the scrollbar to advance through the document. Click the Next button.	 CA ControlMinder Enterprise Management **License Agreement** **Installation and Use of CA ControlMinder Enterprise Management Requires Acceptance of the Following License Agreement:** To proceed without viewing the license agreement, append the following argument to the installation command: -DLICENSE_KEYWORD=Proceed Example: install_XXX_r125.xxx -DLICENSE_KEYWORD=Proceed WIZARD If you proceed with this installation, you accept the terms of this license agreement. To proceed, select I accept the terms of the License Agreement and click Next. To cancel, select I do NOT accept the terms of the License Agreement and click Cancel. CONSOLE If you proceed with this installation, you accept the terms of this license agreement. To proceed, press Y. To cancel, press N. ● I accept the terms of the License Agreement ○ I do NOT accept the terms of the License Agreement InstallAnywhere Cancel Previous Next

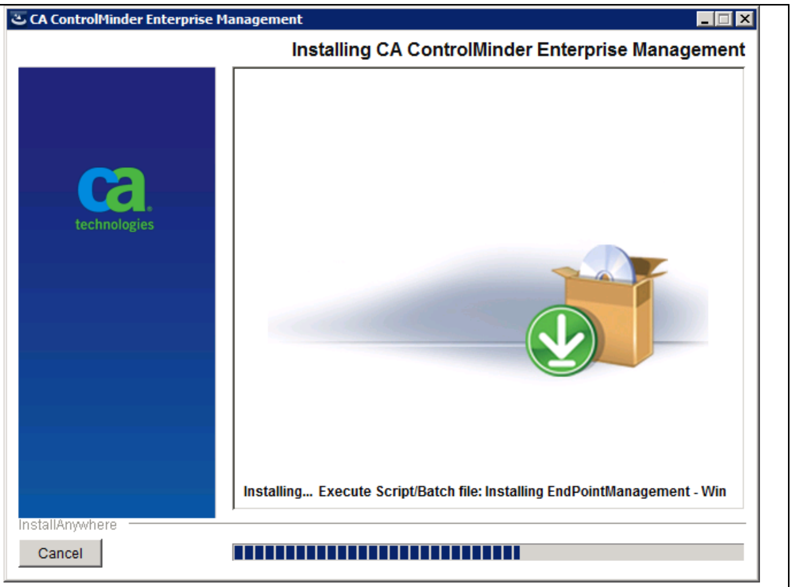
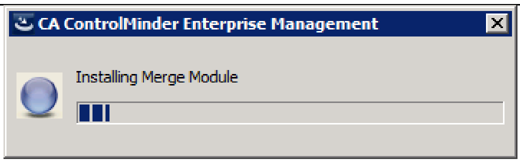
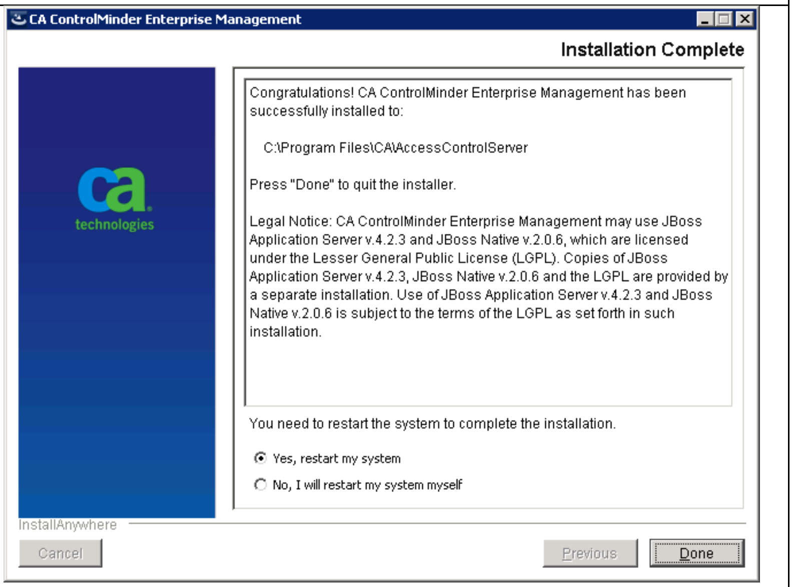
Select the radial button next to Primary Enterprise Management Server Click the Next button.	 CA ControlMinder Enterprise Management Enterprise Management installation type Select Enterprise Management installation type ● Primary Enterprise Management Server ○ Load Balancing Enterprise Management Server
Select the destination folder. Click the Next button.	 CA ControlMinder Enterprise Management Choose Install Folder Please choose a destination folder for this installation. C:\Program Files\CA\AccessControlServer Restore Default Folder Choose... InstallAnywhere Cancel Previous Next

Specify the location where you installed the Java JDK from the Third-Party Components ISO image. **Note**: This page will only appear if you started the installation manually from ProductExplorer.	 CA ControlMinder Enterprise Management Java Development Kit (JDK) Specify the location of an existing JDK installation: C:\jdk1.7.0\bin\java.exe C:\jdk1.7.0\jre\bin\java.exe C:\Program Files\Java\jre7\bin\java.exe technologies Search Another Location... InstallAnywhere Cancel Previous Next
Verify the JBoss settings. NOTE: The JBoss service must NOT be running at this time. Click the Next button.	 CA ControlMinder Enterprise Management JBoss Application Server Settings Please enter the application server settings. JBoss Folder (no spaces): C:\jboss-4.2.3.GA App Server Port: 18080 App Server HTTPS Port: 18443 App Server Naming Port: 11099 technologies Restore Default Choose... InstallAnywhere Cancel Previous Next

Provide the communication password. **NOTE**: This password Is used internally by Enterprise Management components. Click the Next button.	 CA ControlMinder Enterprise Management Communication Password Define the password that the product components use for communication. Password: ******** Confirm Password: ******** 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.
Select the radial button for Microsoft SQL Server as the Database Type. Click the Next button.	 CA ControlMinder Enterprise Management Database Type Specify the database type used for storing information: ○ Oracle Database 10g/11g ● Microsoft SQL Server 2005/2008/2012

Enter the connection information for the Microsoft SQL Server database. Click the Next button.	 CA ControlMinder Enterprise Management InstallAnywhere Cancel Previous Next Database Connection Information Define the database connection: Host Name: 10.0.1.112 Port Number: 1433 Database Name: cmdb Username: cmdbuser Password: ***********
Select the radial button for Embedded User Store as the User Store Type. Account information for all Enterprise Management users will be stored in the Microsoft SQL Server database. Click the Next button.	 CA ControlMinder Enterprise Management InstallAnywhere Cancel Previous Next User Store Type Specify the user store you want to use for this product: ○ Active Directory ● Embedded User Store ○ Other User Store

Provide the password for the superadmin account. This will be the only user available after the installation. The superadmin account is assigned the System Manager role. Click the Next button.	 CA ControlMinder Enterprise Management InstallAnywhere Cancel Previous Next Administrator Password Define the superadmin account password: Password: *********** Confirm Password: *********** 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.
Review the installation details. Click the Install button.	 CA ControlMinder Enterprise Management InstallAnywhere Cancel Previous Install Pre-Installation Summary Please Review the following before continuing: **Product Name:** CA ControlMinder Enterprise Management **Install Folder:** C:\Program Files\CA\AccessControlServer **Application Server:** JBoss **JBoss Folder:** C:\jboss-4.2.3.GA **JBoss URL and Port:** http://WIN-LKLJMLRD44O:18080 **JBoss HTTPS Port:** 18443 **JDK Folder:**

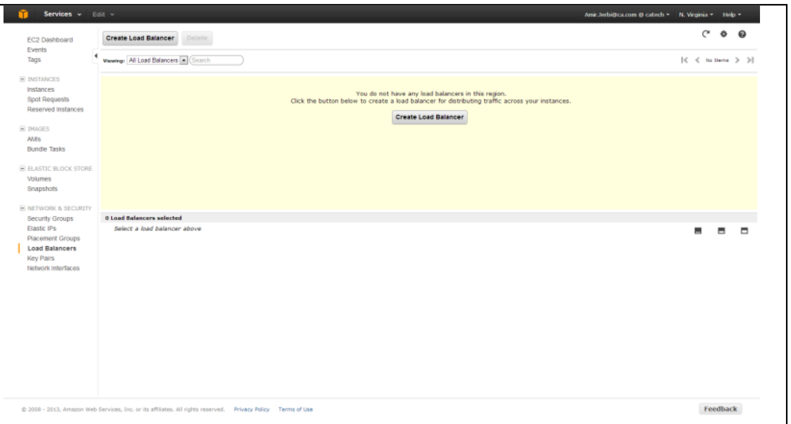
Wait for the installation to complete Important: If the installation does not appear to start, an installation confirmation window may be hiding under the current window. Move the top window and check for an underlying window.	 CA ControlMinder Enterprise Management Installing CA ControlMinder Enterprise Management Installing... Execute Script/Batch file: Installing EndPointManagement - Win InstallAnywhere Cancel
The installation is expected to take from 15 to 60 minutes to complete	 CA ControlMinder Enterprise Management Installing Merge Module
After the installation successfully completes, click the Done button to reboot the server and finalize the installation.	 CA ControlMinder Enterprise Management Installation Complete Congratulations! CA ControlMinder Enterprise Management has been successfully installed to: C:\Program Files\CA\AccessControlServer Press "Done" to quit the installer. 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. You need to restart the system to complete the installation. ● Yes, restart my system ○ No, I will restart my system myself InstallAnywhere Cancel Previous Done

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.

<table>
<tr>
<td>Choose “Load Balancers” option on the Amazon EC2 left side menu. Click on the “Create Load Balancer” button.</td>
<td>


You do not have any load balancers in this region.
Click the button below to create a load balancer for distributing traffic across your instances.

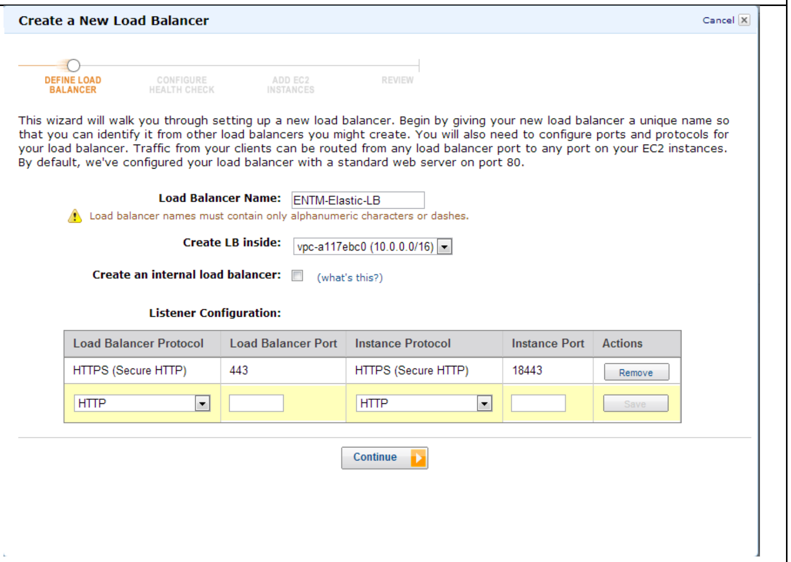
Create Load Balancer

0 Load Balancers selected

Select a load balancer above

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use
</td>
</tr>
<tr>
<td>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
</td>
<td>


Create a New Load Balancer

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: ENTM-Elastic-LB

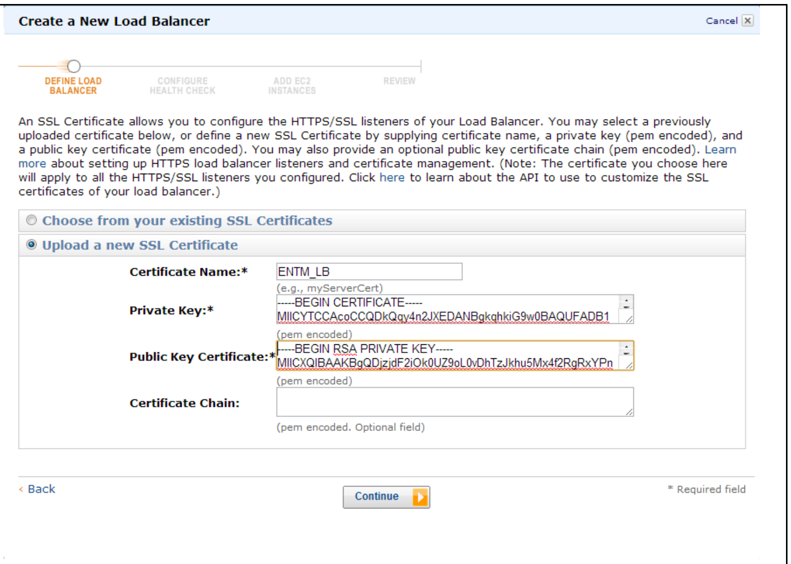
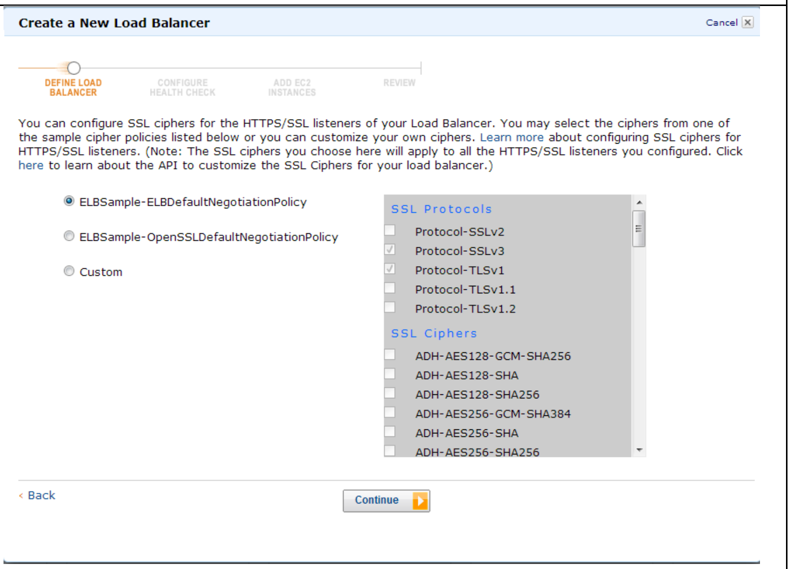
Load balancer names must contain only alphanumeric characters or dashes.

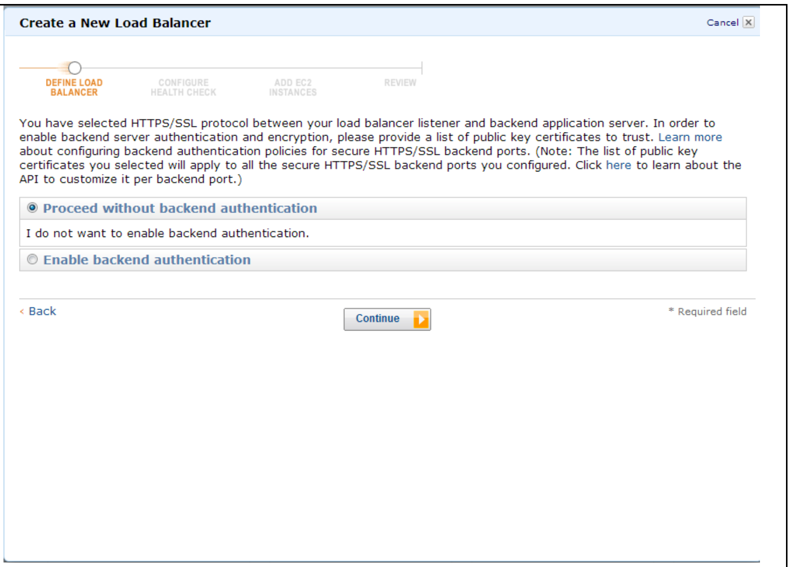
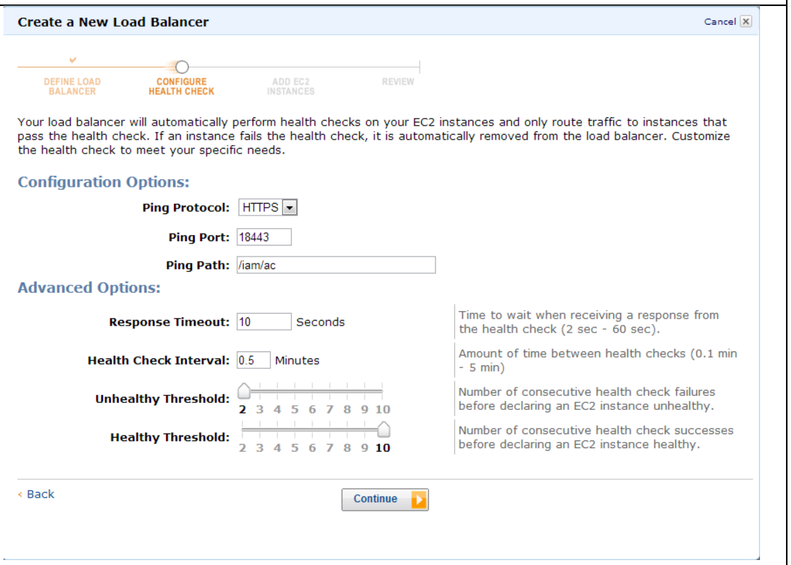
Create LB inside: vpc-a117ebc0 (10.0.0.0/16)

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

Listener Configuration:

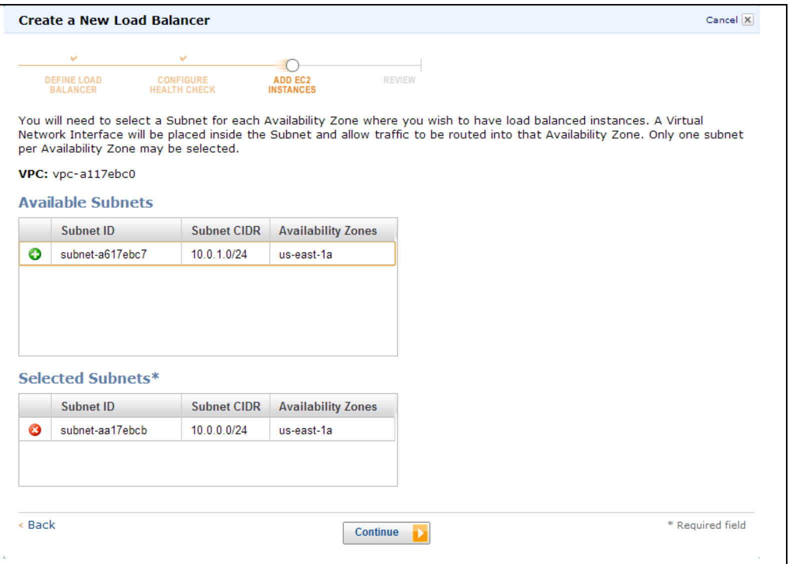
<table>
<tr><th>Load Balancer Protocol</th><th>Load Balancer Port</th><th>Instance Protocol</th><th>Instance Port</th><th>Actions</th></tr>
<tr><td>HTTPS (Secure HTTP)</td><td>443</td><td>HTTPS (Secure HTTP)</td><td>18443</td><td>Remove</td></tr>
<tr><td>HTTP</td><td></td><td>HTTP</td><td></td><td>Save</td></tr>
</table>
</td>
</tr>
</table>

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	 **Create a New Load Balancer** Cancel ☒ 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:*** ENTM_LB (e.g., myServerCert) **Private Key:*** -----BEGIN CERTIFICATE----- MIICYTCCAcoCCQDkQqy4n2JXEDANBgkqhkiG9w0BAQUFADB1 (pem encoded) **Public Key Certificate:*** -----BEGIN RSA PRIVATE KEY----- MIICXQIBAAKBgQDjzjdF2iOk0UZ9oL0vDhTzJkhu5Mx4f2RgRxYPn (pem encoded) **Certificate Chain:** (pem encoded. Optional field) ‹ Back · Continue · * Required field
Select ELBSample-ELBDefaultNegotionPolicy that includes SSLv3 and TLSv1.	 **Create a New Load Balancer** Cancel ☒ 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

Select "Proceed without backend authentication" and click Continue.	 **Create a New Load Balancer** Cancel ☒ DEFINE LOAD BALANCER CONFIGURE HEALTH CHECK ADD EC2 INSTANCES REVIEW 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. Learn more 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 here to learn about the API to customize it per backend port.) ● **Proceed without backend authentication** I do not want to enable backend authentication. ○ **Enable backend authentication**
Configure the URL that will be used by the Load Balancer for health monitoring. Specify port 18433 and path "/iam/ac".	 **Create a New Load Balancer** Cancel ☒ DEFINE LOAD BALANCER CONFIGURE HEALTH CHECK ADD EC2 INSTANCES REVIEW 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. **Configuration Options:** Ping Protocol: HTTPS Ping Port: 18443 Ping Path: /iam/ac **Advanced Options:** Response Timeout: 10 Seconds — Time to wait when receiving a response from the health check (2 sec - 60 sec). Health Check Interval: 0.5 Minutes — Amount of time between health checks (0.1 min - 5 min) Unhealthy Threshold: 2 (2 3 4 5 6 7 8 9 10) — Number of consecutive health check failures before declaring an EC2 instance unhealthy. Healthy Threshold: 10 (2 3 4 5 6 7 8 9 10) — Number of consecutive health check successes before declaring an EC2 instance healthy.

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

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

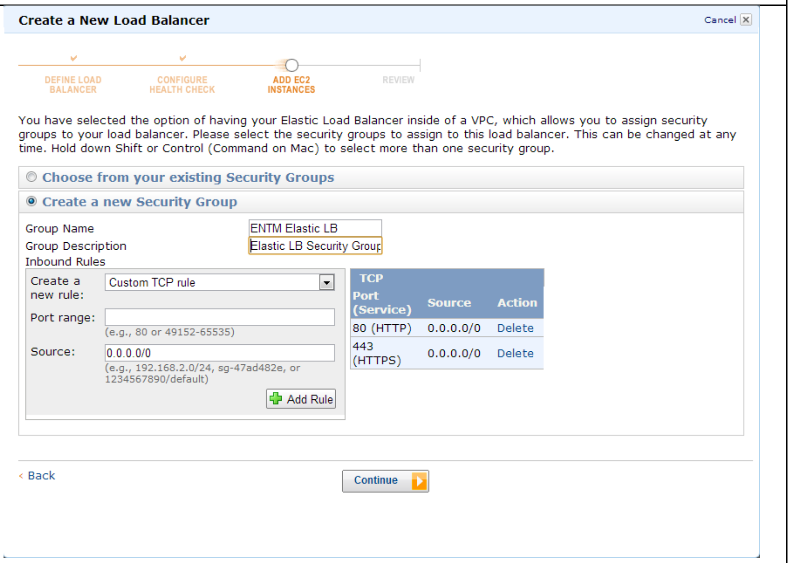
Available Subnets

	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

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



Create a New Load Balancer

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:

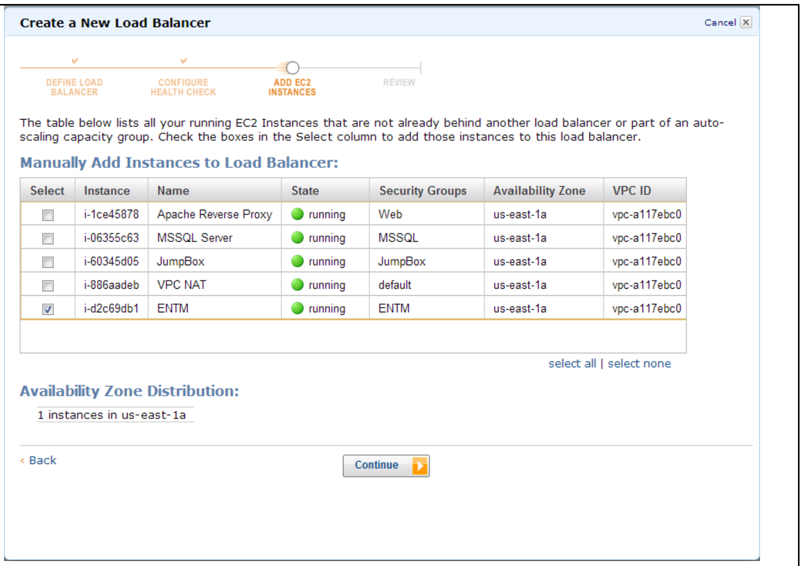
(e.g., 80 or 49152-65535)

Source: 0.0.0.0/0

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

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

Add the ENTM Server instance to the load balancer.



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.

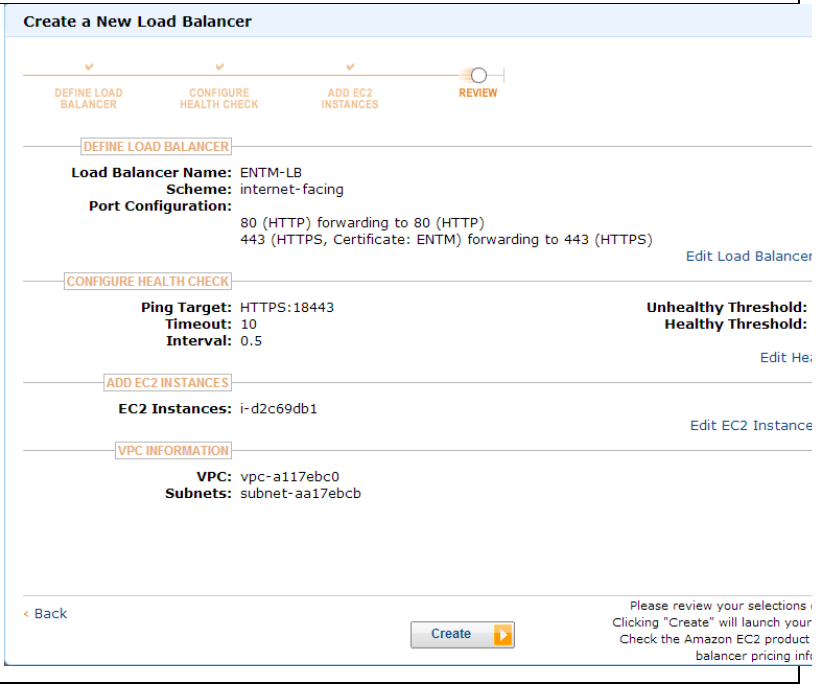
Manually Add Instances to Load Balancer:

Select	Instance	Name	State	Security Groups	Availability Zone	VPC ID
□	i-1ce45878	Apache Reverse Proxy	● running	Web	us-east-1a	vpc-a117ebc0
□	i-06355c63	MSSQL Server	● running	MSSQL	us-east-1a	vpc-a117ebc0
□	i-60345d05	JumpBox	● running	JumpBox	us-east-1a	vpc-a117ebc0
□	i-886aadeb	VPC NAT	● running	default	us-east-1a	vpc-a117ebc0
☑	i-d2c69db1	ENTM	● running	ENTM	us-east-1a	vpc-a117ebc0

Availability Zone Distribution:

1 instances in us-east-1a

Click the Create button to create the new load balancer.



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)

CONFIGURE HEALTH CHECK

Ping Target: HTTPS:18443
Timeout: 10
Interval: 0.5
Unhealthy Threshold:
Healthy Threshold:

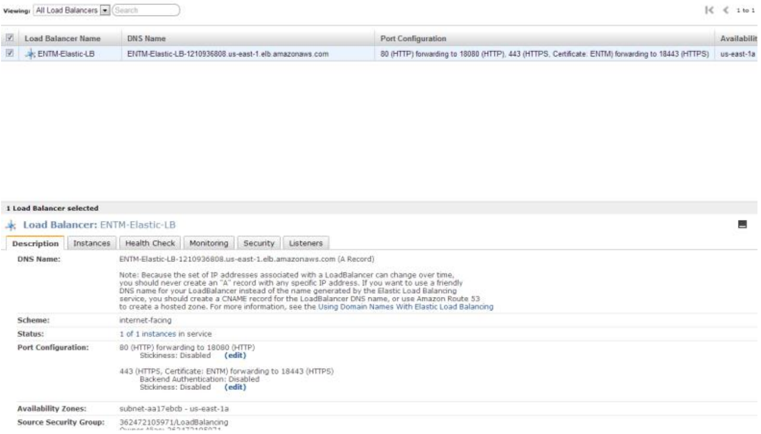
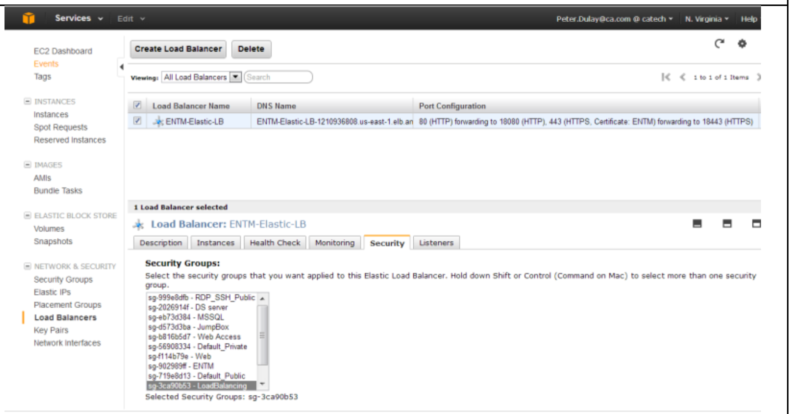
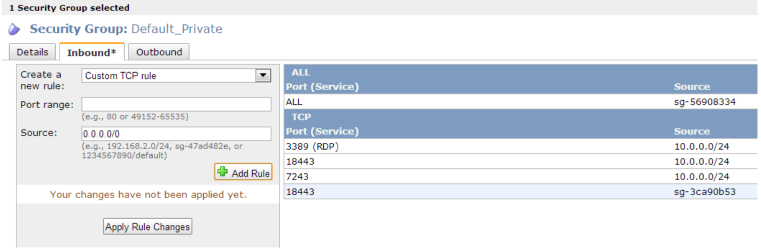
ADD EC2 INSTANCES

EC2 Instances: i-d2c69db1

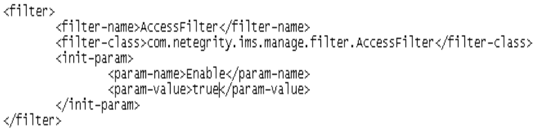
VPC INFORMATION

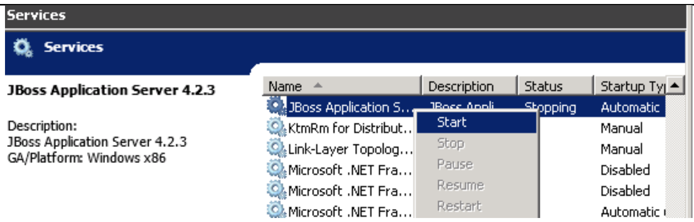
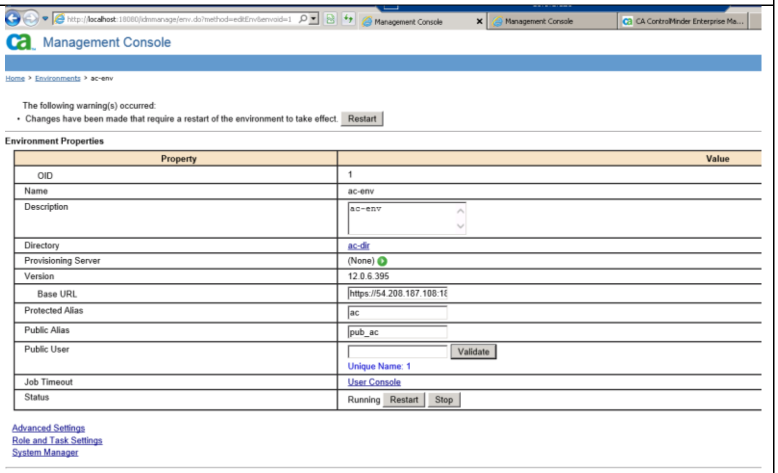
VPC: vpc-a117ebc0
Subnets: subnet-aa17ebcb

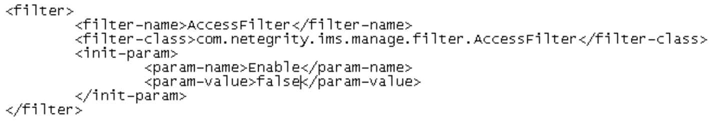
Please review your selections
Clicking "Create" will launch your
Check the Amazon EC2 product
balancer pricing inf

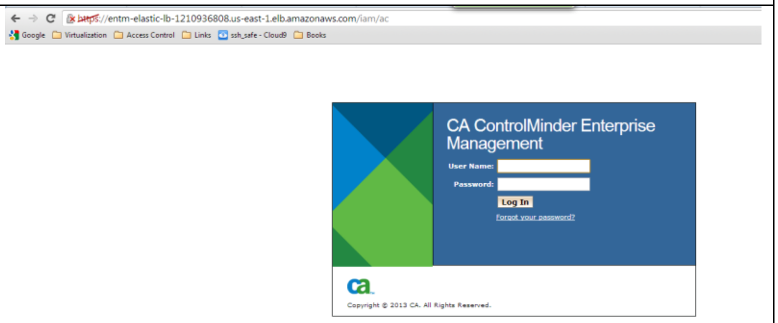
The newly created load balancer will be displayed in the list.	 Viewing: All Load Balancers 1 to 1 ☑ Load Balancer Name | DNS Name | Port Configuration | Availabilit ☑ ENTM-Elastic-LB | ENTM-Elastic-LB-1210936808.us-east-1.elb.amazonaws.com | 80 (HTTP) forwarding to 18080 (HTTP), 443 (HTTPS, Certificate: 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) Stickiness: Disabled (edit) 443 (HTTPS, Certificate: ENTM) forwarding to 18443 (HTTPS) Backend Authentication: Disabled Stickiness: Disabled (edit) Availability Zones: subnet-aa17ebcb - us-east-1a Source Security Group: 362472105971/LoadBalancing
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 @ catech | 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 1 to 1 of 1 Items ☑ Load Balancer Name | DNS Name | Port Configuration ☑ ENTM-Elastic-LB | ENTM-Elastic-LB-1210936808.us-east-1.elb.an | 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-999e8dfb - RDP_SSH_Public sg-2026914f - DS server sg-eb73d384 - MSSQL sg-d573d3ba - JumpBox sg-b816b5d7 - Web Access sg-56908334 - Default_Private sg-f114b79e - Web sg-902989ff - ENTM sg-719e8d13 - Default_Public sg-3ca90b53 - LoadBalancing 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 | 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 18443 | sg-3ca90b53

Configure ENTM to Use Amazon Elastic Load Balancer

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

Restart JBoss to effect the change.	 JBoss Application Server 4.2.3 Description: JBoss Application Server 4.2.3 GA/Platform: Windows x86 Name / Description / Status / Startup Type JBoss Application S... / JBoss Appli... / Stopping / Automatic KtmRm for Distribut... / Manual Link-Layer Topolog... / Manual Microsoft .NET Fra... / Disabled Microsoft .NET Fra... / Disabled Microsoft .NET Fra... / Automatic
From your Remote Desktop session to the ENTM Server, browse to the idmmanage URL: http://localhost:18080/idmmanage Choose “Environments” -> “ac-env”. Change the “Base URL” property to point to the public address of the Amazon Elastic Load Balancer (e.g. https://<ip address>) Click the Save button.	 http://localhost:18080/idmmanage/env.do?method=editEnv&envoid=1 Management Console Home > Environments > ac-env The following warning(s) occurred: • Changes have been made that require a restart of the environment to take effect. Restart Environment Properties 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: Validate Unique Name: 1 Job Timeout: User Console Status: Running Restart Stop Advanced Settings Role and Task Settings System Manager

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

You can now access Enterprise Management via the Amazon Elastic Load Balancer.	 ~~https~~://entm-elastic-lb-1210936808.us-east-1.elb.amazonaws.com/iam/ac Google Virtualization Access Control Links ssh_safe - Cloud9 Books CA ControlMinder Enterprise Management User Name: Password: Log In Forgot your password? Copyright © 2013 CA. All Rights Reserved.

Deploying Distribution Server

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

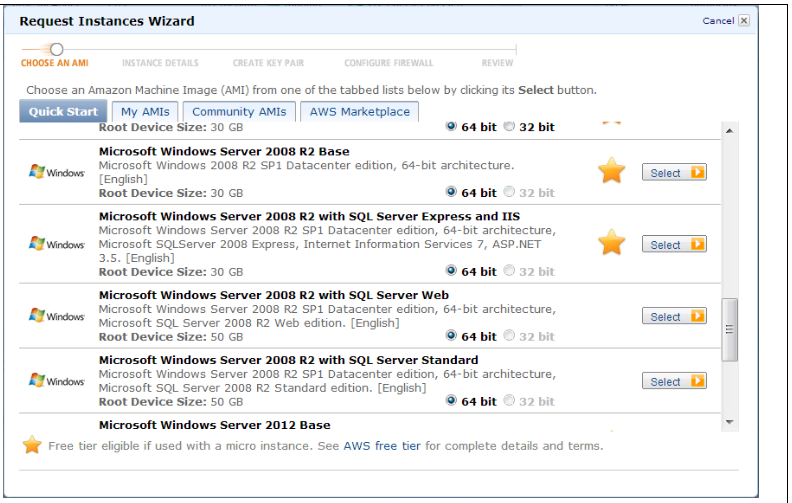
The Distribution Server provides communication services and scalability between the endpoints and the ENTM Server while limiting direct access to the ENTM Server.

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



Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its **Select** button.

Root Device Size: 30 GB ● 64 bit ○ 32 bit

Microsoft Windows Server 2008 R2 Base
Microsoft Windows 2008 R2 SP1 Datacenter edition, 64-bit architecture. [English]
Root Device Size: 30 GB ● 64 bit ○ 32 bit

Microsoft Windows Server 2008 R2 with SQL Server Express and IIS
Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQLServer 2008 Express, Internet Information Services 7, ASP.NET 3.5. [English]
Root Device Size: 30 GB ● 64 bit ○ 32 bit

Microsoft Windows Server 2008 R2 with SQL Server Web
Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQL Server 2008 R2 Web edition. [English]
Root Device Size: 50 GB ● 64 bit ○ 32 bit

Microsoft Windows Server 2008 R2 with SQL Server Standard
Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQL Server 2008 R2 Standard edition. [English]
Root Device Size: 50 GB ● 64 bit ○ 32 bit

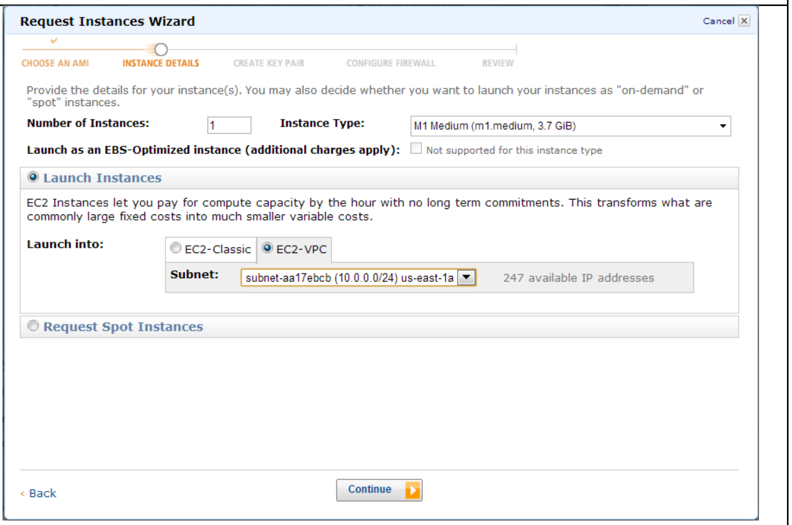
Microsoft Windows Server 2012 Base

Free tier eligible if used with a micro instance. See AWS free tier for complete details and terms.

Set Instance Type to M1 Large.

For the Launch into information, select the radial button for EC2-VPC and set the subnet to the public subnet (10.0.0.0/24).

Click the Continue button.



Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.

Number of Instances: 1 **Instance Type:** M1 Medium (m1.medium, 3.7 GiB)

Launch as an EBS-Optimized instance (additional charges apply): □ Not supported for this instance type

● Launch Instances

EC2 Instances let you pay for compute capacity by the hour with no long term commitments. This transforms what are commonly large fixed costs into much smaller variable costs.

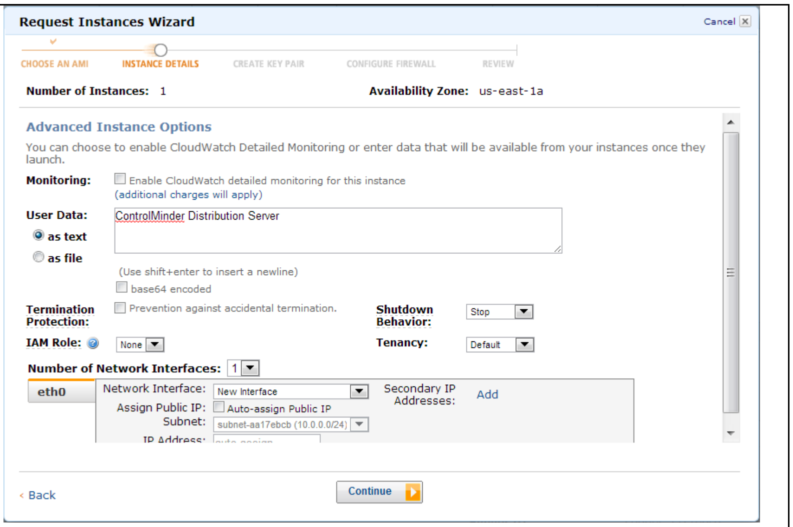
Launch into: ○ EC2-Classic ● EC2-VPC

Subnet: subnet-aa17ebcb (10.0.0.0/24) us-east-1a 247 available IP addresses

○ Request Spot Instances

Provide User Data to identify your instance.

Click the Continue button.



Request Instances Wizard

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 Distribution 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

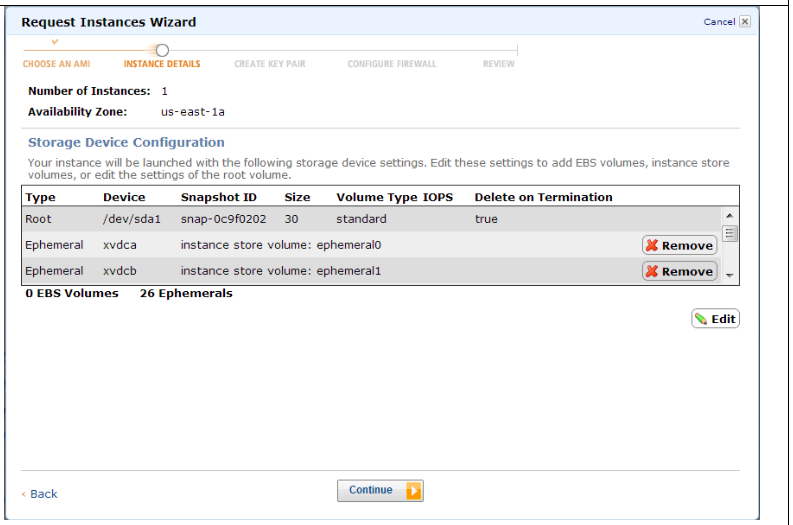
Subnet: subnet-aa17ebcb (10.0.0.0/24)

IP Address: auto-assign

Secondary IP Addresses: Add

Keep the default storage configuration.

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



Request Instances Wizard

Number of Instances: 1

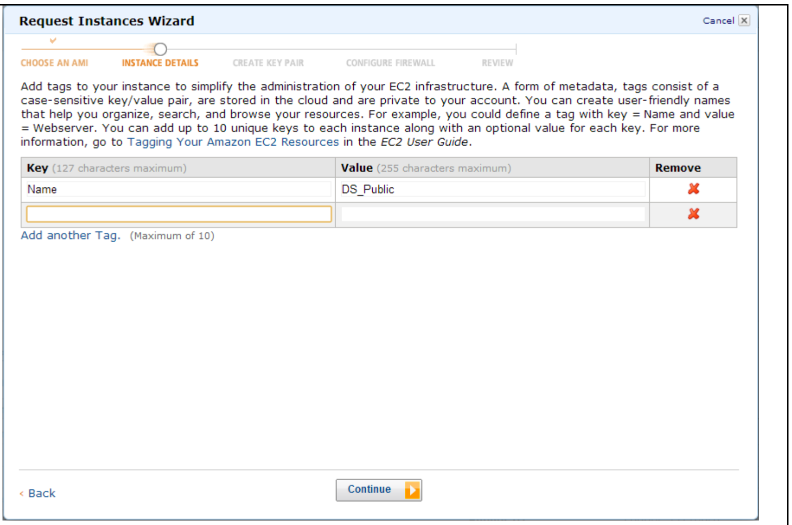
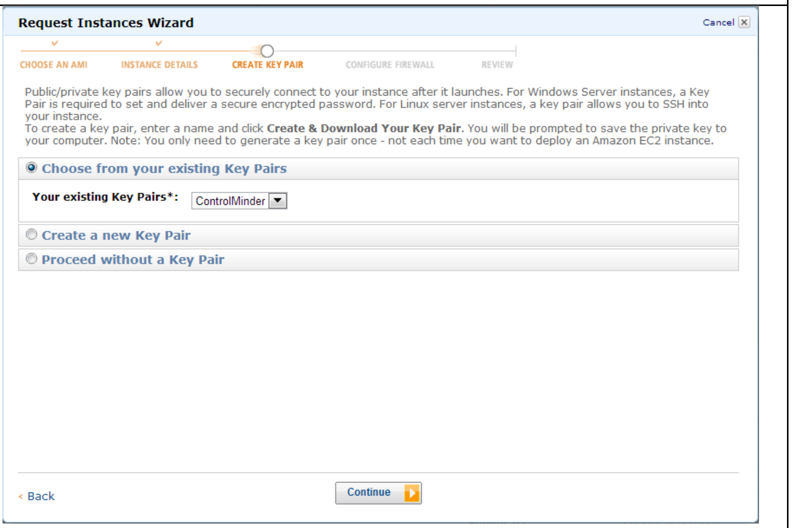
Availability Zone: us-east-1a

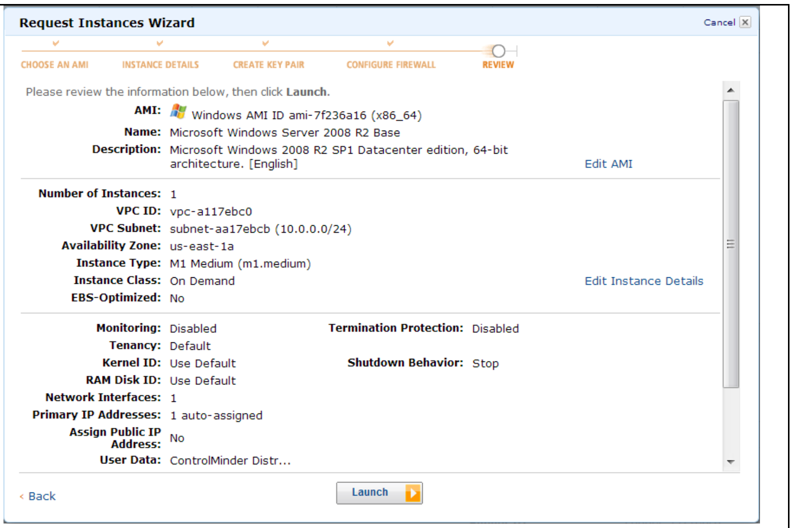
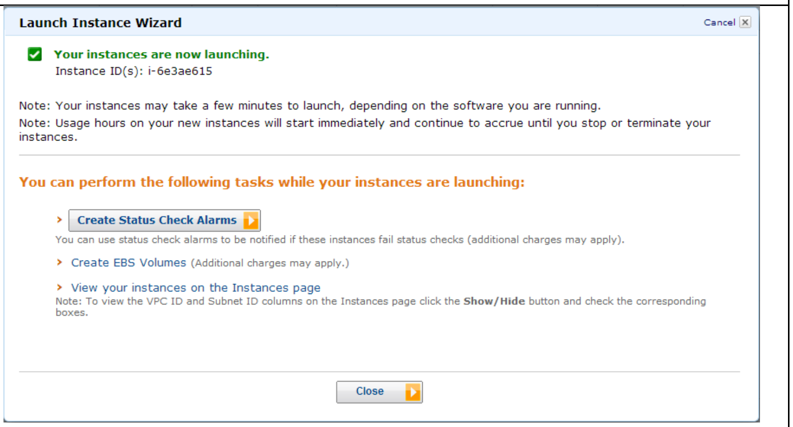
Storage Device Configuration

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-0c9f0202	30	standard		true	
Ephemeral	xvdca	instance store volume: ephemeral0					Remove
Ephemeral	xvdcb	instance store volume: ephemeral1					Remove

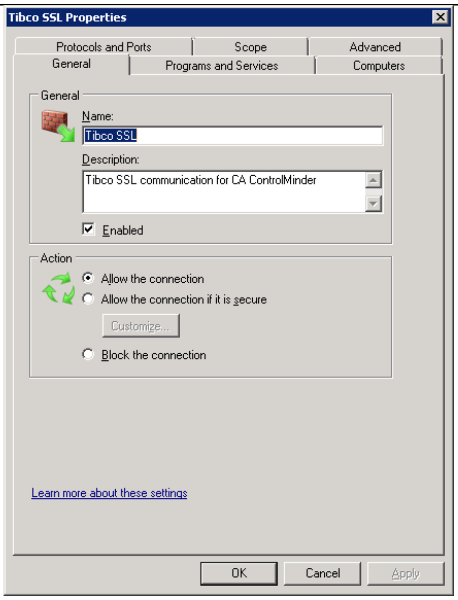
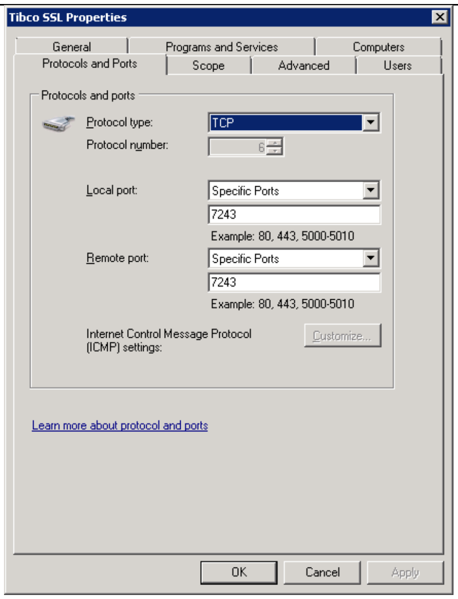
0 EBS Volumes **26 Ephemerals**

Name your instance and provide any additional tags as required.	 **Request Instances Wizard** Add tags to your instance to simplify the administration of your EC2 infrastructure. A form of metadata, tags consist of a case-sensitive key/value pair, are stored in the cloud and are private to your account. You can create user-friendly names that help you organize, search, and browse your resources. For example, you could define a tag with key = Name and value = Webserver. You can add up to 10 unique keys to each instance along with an optional value for each key. For more information, go to Tagging Your Amazon EC2 Resources in the *EC2 User Guide*. **Key** (127 characters maximum) | **Value** (255 characters maximum) | **Remove** Name | DS_Public | ✘ Add another Tag. (Maximum of 10)
Use the key pair associated you're your AWS ECS Account.	 **Request Instances Wizard** Public/private key pairs allow you to securely connect to your instance after it launches. For Windows Server instances, a Key Pair is required to set and deliver a secure encrypted password. For Linux server instances, a key pair allows you to SSH into your instance. To create a key pair, enter a name and click **Create & Download Your Key Pair**. You will be prompted to save the private key to your computer. Note: You only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance. ● Choose from your existing Key Pairs **Your existing Key Pairs*:** ControlMinder ○ Create a new Key Pair ○ Proceed without a Key Pair
Add the Default_Public Security Group to the Distribution Server instance	

Click 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-7f236a16 (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-aa17ebcb (10.0.0.0/24) **Availability Zone:** us-east-1a **Instance Type:** M1 Medium (m1.medium) **Instance Class:** On Demand **EBS-Optimized:** No Edit Instance Details **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 Distr...
Click the Close button.	 **Launch Instance Wizard** Cancel ☒ ☑ **Your instances are now launching.** Instance ID(s): i-6e3ae615 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. **You can perform the following tasks while your instances are launching:** › Create Status Check Alarms You can use status check alarms to be notified if these instances fail status checks (additional charges may apply). › Create EBS Volumes (Additional charges may apply.) › View your instances on the Instances page Note: To view the VPC ID and Subnet ID columns on the Instances page click the **Show/Hide** button and check the corresponding boxes.

Prepare to Install the Distribution Server

Tibco Communication Configuration

Ensure there are Microsoft Windows Firewall rules on both the ENTM Server and the Distribution Server to allow incoming and outgoing communication on the Tibco SSL Port (7243).	 Tibco SSL Properties Protocols and Ports Scope Advanced General Programs and Services Computers Customize... Learn more about these settings OK Cancel Apply General Name: Tibco SSL Description: Tibco SSL communication for CA ControlMinder ☑ Enabled Action ● Allow the connection ○ Allow the connection if it is secure ○ Block the connection
	 Tibco SSL Properties General Programs and Services Computers Protocols and Ports Scope Advanced Users Customize... Learn more about protocol and ports OK Cancel Apply Protocols and ports Protocol type: TCP Protocol number: 6 Local port: Specific Ports 7243 Example: 80, 443, 5000-5010 Remote port: Specific Ports 7243 Example: 80, 443, 5000-5010 Internet Control Message Protocol (ICMP) settings:

Configure Name Resolution

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

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

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

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

```
10.0.1.128       WIN-LKLJMLRD44O       WIN-LKLJMLRD44O.ec2.internal
```

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

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

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

Steps to install Distribution Server include:

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

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

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

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

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

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

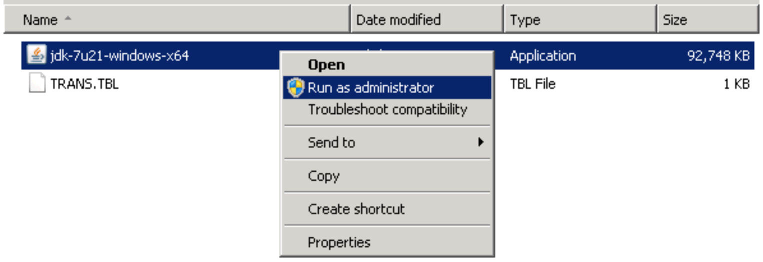
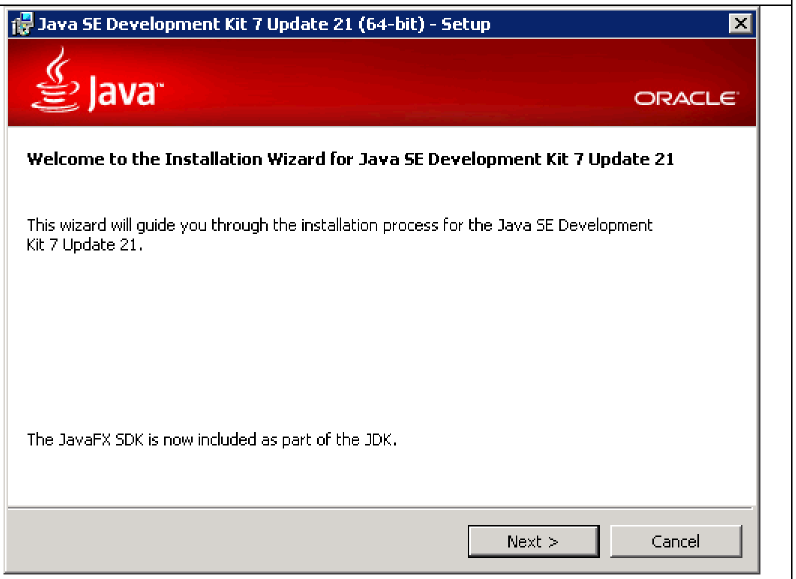
▪ JDK (from the Third-Party Components)	200 MB
▪ JBoss (from the Third-Party Components)	850 MB
▪ Enterprise Management	??? GB

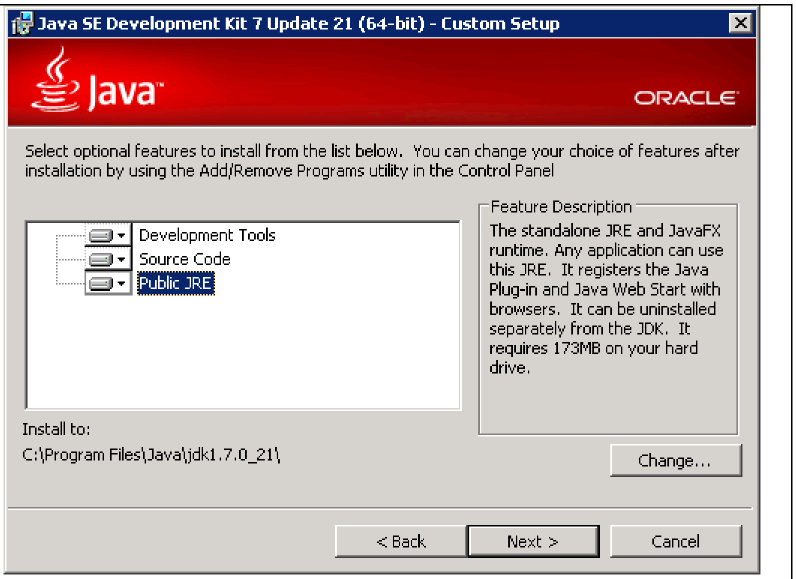
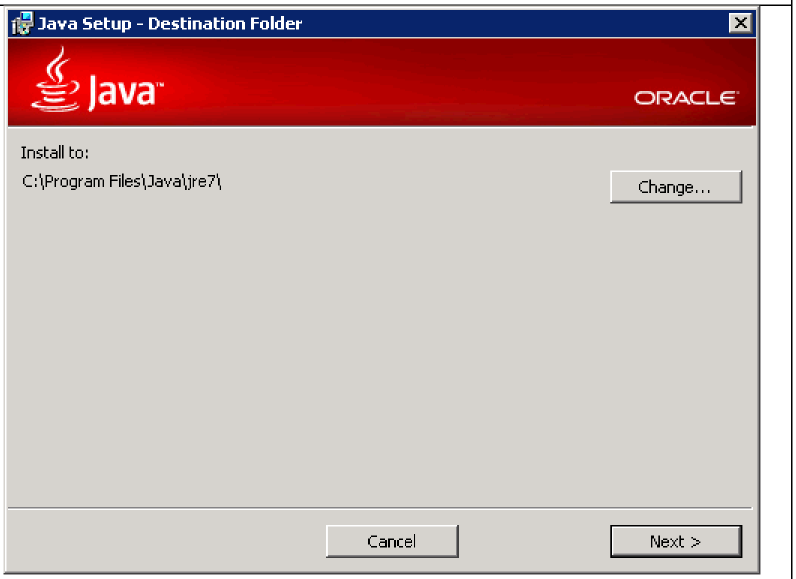
Install Third-Party Components

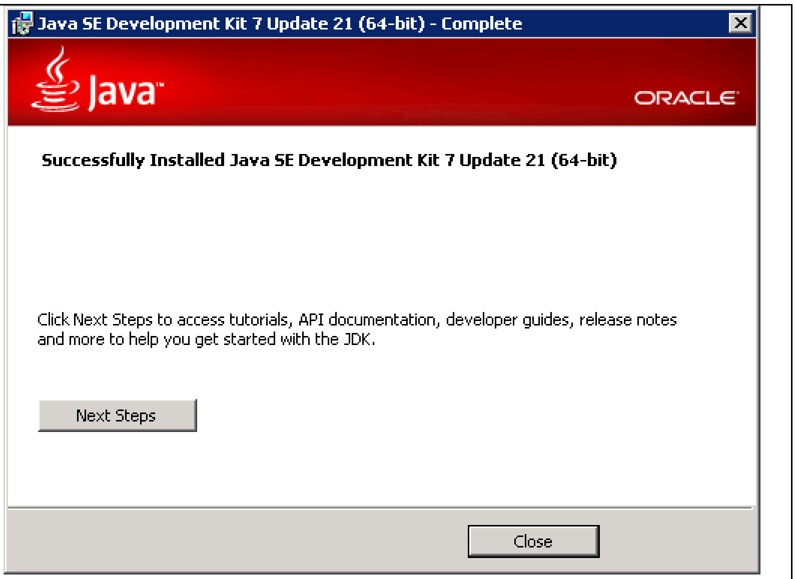
Login to the Distribution Server as a member of the local Administrators group.

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

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

Locate the Java SDK installer, **jdk-7u21-windows-x64.exe,** from the JDK-1.7.21_x64 directory on the DVD drive. Right click **jdk-7u21-windows-x64.exe** and choose Run as administrator.	 Name · Date modified · Type · Size jdk-7u21-windows-x64 · Application · 92,748 KB TRANS.TBL · TBL File · 1 KB Open Run as administrator Troubleshoot compatibility Send to Copy Create shortcut Properties
Click the Next button to start the Java SDK installation.	 Java SE Development Kit 7 Update 21 (64-bit) - Setup **Welcome to the Installation Wizard for Java SE Development Kit 7 Update 21** This wizard will guide you through the installation process for the Java SE Development Kit 7 Update 21. The JavaFX SDK is now included as part of the JDK.

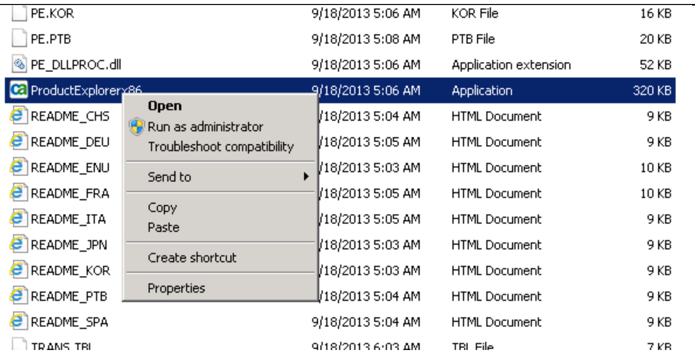
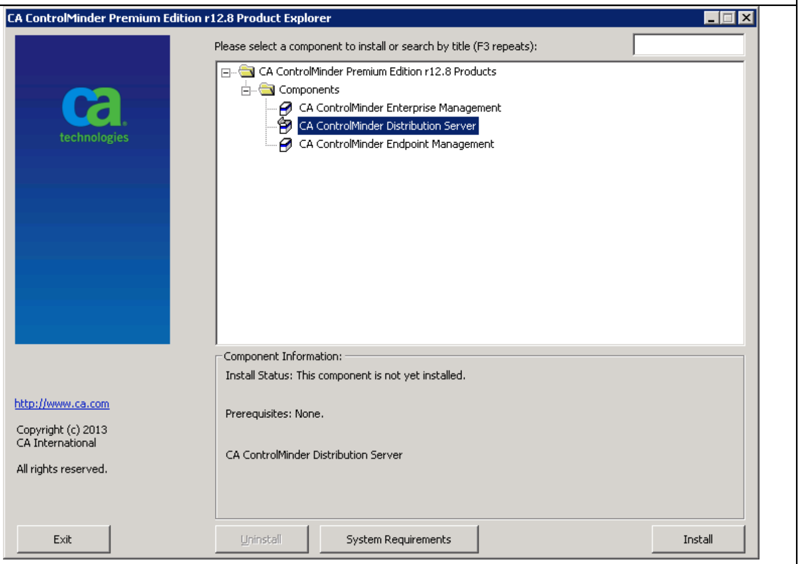
Click the Next button.	 Java SE Development Kit 7 Update 21 (64-bit) - Custom Setup Select optional features to install from the list below. You can change your choice of features after installation by using the Add/Remove Programs utility in the Control Panel Development Tools Source Code Public JRE Feature Description The standalone JRE and JavaFX runtime. Any application can use this JRE. It registers the Java Plug-in and Java Web Start with browsers. It can be uninstalled separately from the JDK. It requires 173MB on your hard drive. Install to: C:\Program Files\Java\jdk1.7.0_21\
Click the Next button.	 Java Setup - Destination Folder Install to: C:\Program Files\Java\jre7\

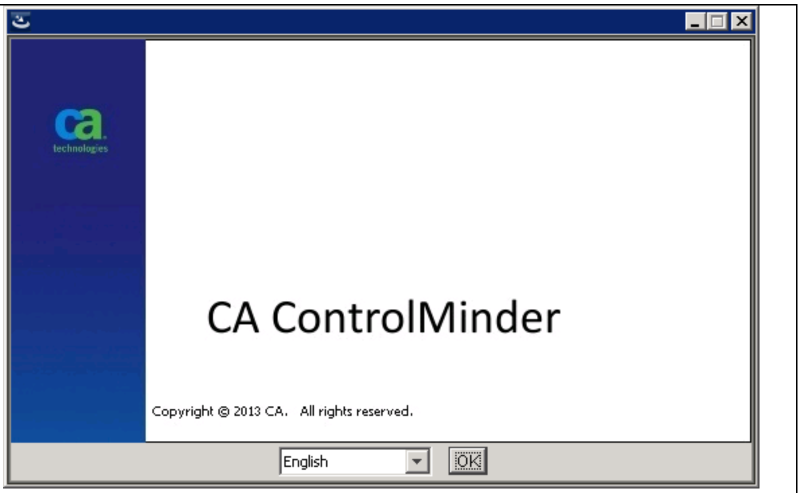
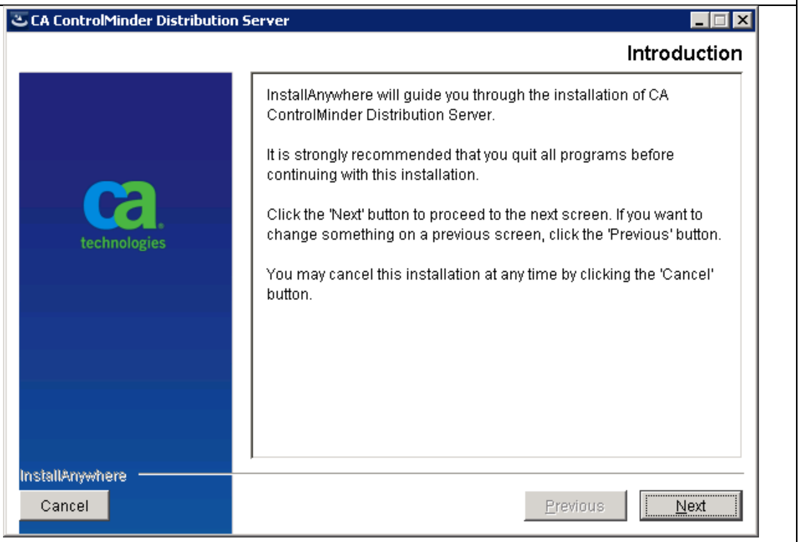
Click the Close button to finish the installation.	 Java SE Development Kit 7 Update 21 (64-bit) - Complete Successfully Installed Java SE Development Kit 7 Update 21 (64-bit) Click Next Steps to access tutorials, API documentation, developer guides, release notes and more to help you get started with the JDK.

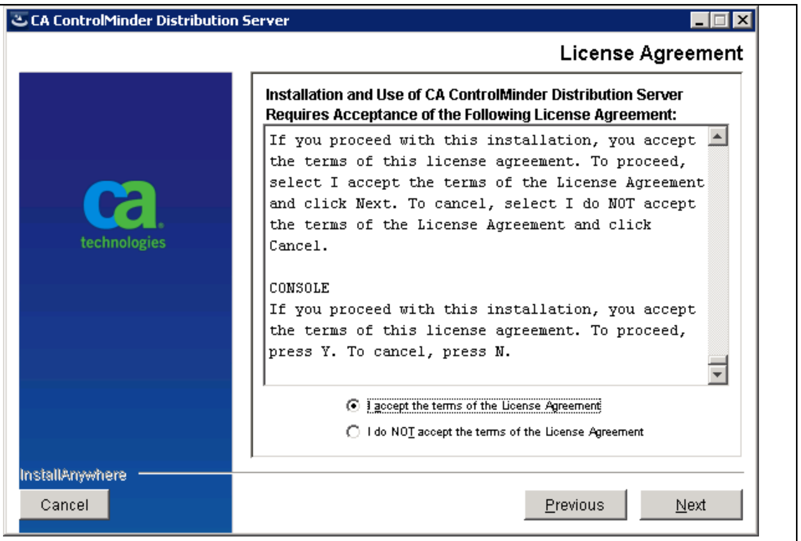
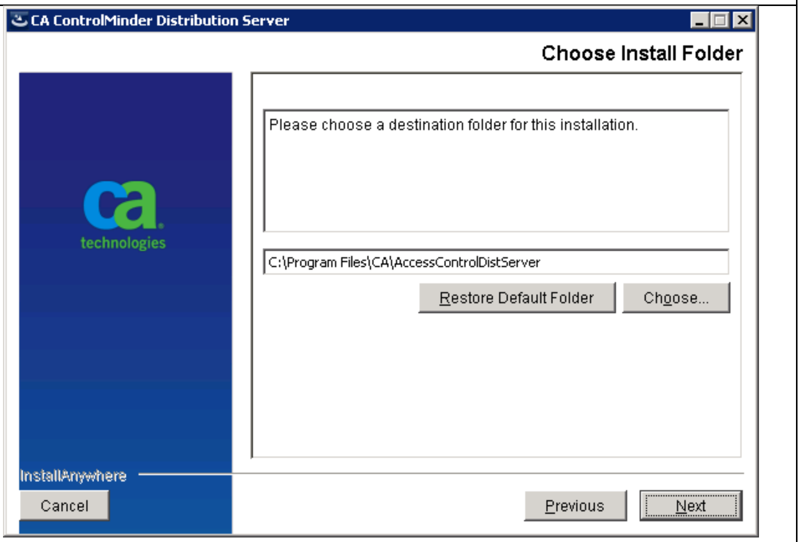
Install the Distribution Server

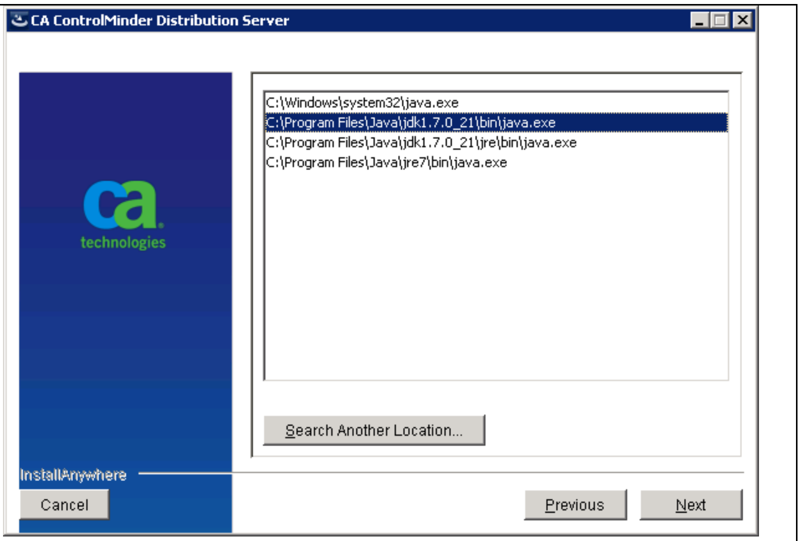
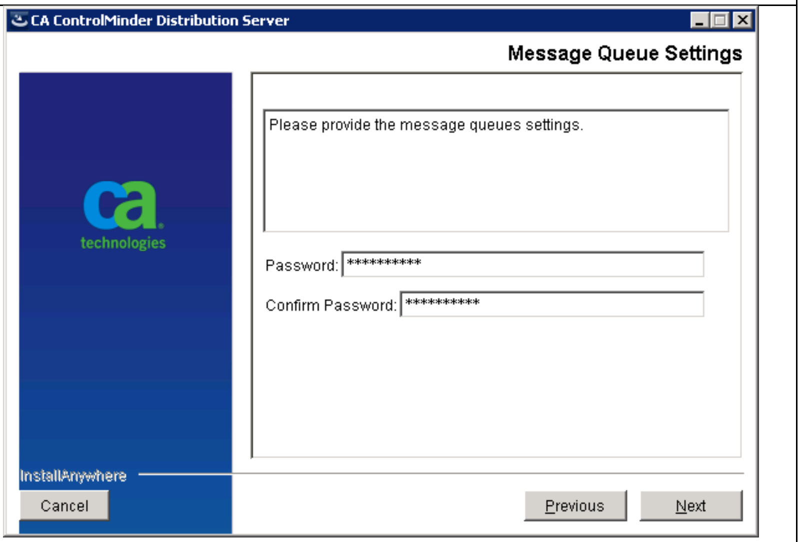
Mount the CA ControlMinder Server Components ISO image in the virtual DVD drive.

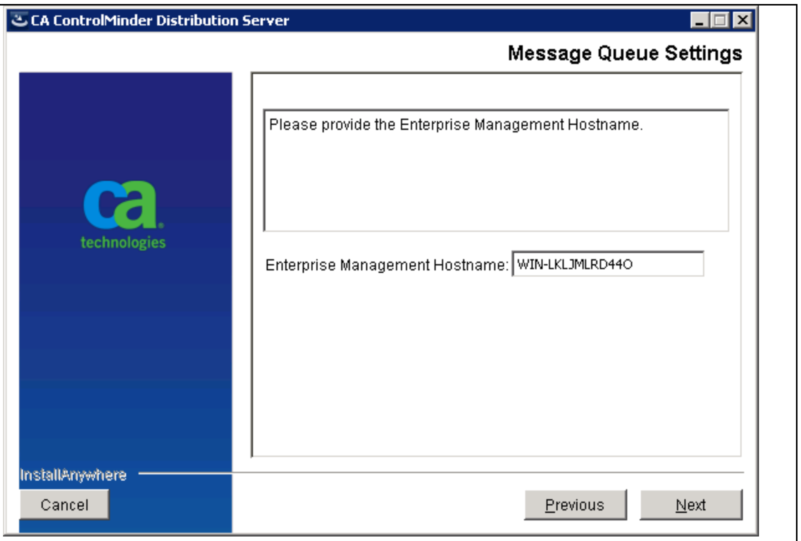
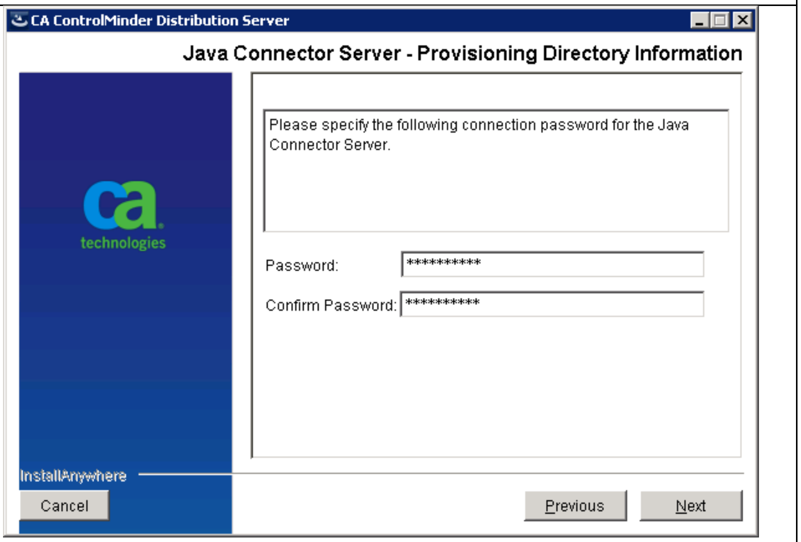
Important: Do not use a UNC path or remote share to specify the software location.

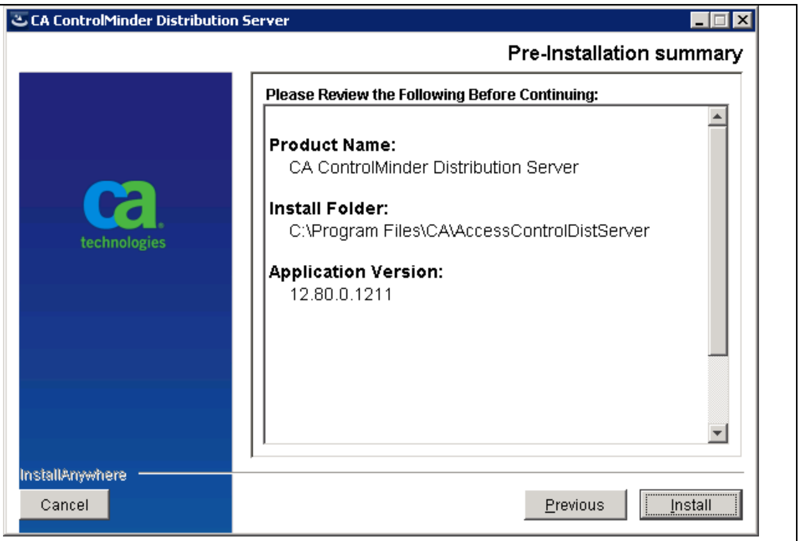
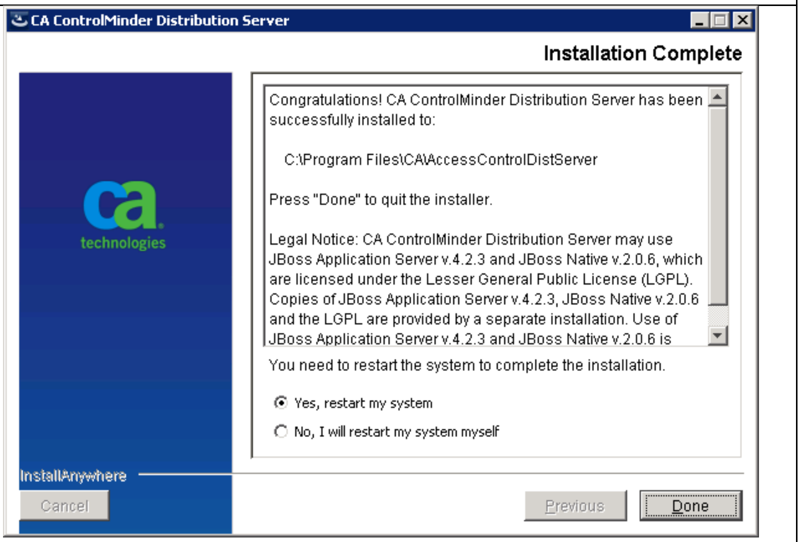
Start the Distribution Server installation by launching **ProductExplorer** from the virtual DVD drive. Remember to start **ProductExplorer** by right-clicking the executable and choosing Run as administrator.	 PE.KOR 9/18/2013 5:06 AM KOR File 16 KB PE.PTB 9/18/2013 5:08 AM PTB File 20 KB PE_DLLPROC.dll 9/18/2013 5:06 AM Application extension 52 KB ProductExplorerx86 9/18/2013 5:06 AM Application 320 KB README_CHS /18/2013 5:04 AM HTML Document 9 KB README_DEU /18/2013 5:05 AM HTML Document 9 KB README_ENU /18/2013 5:03 AM HTML Document 10 KB README_FRA /18/2013 5:05 AM HTML Document 10 KB README_ITA /18/2013 5:05 AM HTML Document 9 KB README_JPN /18/2013 5:03 AM HTML Document 9 KB README_KOR /18/2013 5:03 AM HTML Document 9 KB README_PTB /18/2013 5:04 AM HTML Document 9 KB README_SPA 9/18/2013 5:04 AM HTML Document 9 KB TRANS.TBL 9/18/2013 6:03 AM TBL File 7 KB Open Run as administrator Troubleshoot compatibility Send to Copy Paste Create shortcut Properties
From the Components folder of **ProductExplorer**, select CA ControlMinder Distribution Server. Click the Install button.	 CA ControlMinder Premium Edition r12.8 Product Explorer Please select a component to install or search by title (F3 repeats): CA ControlMinder Premium Edition r12.8 Products Components CA ControlMinder Enterprise Management CA ControlMinder Distribution Server CA ControlMinder Endpoint Management Component Information: Install Status: This component is not yet installed. Prerequisites: None. CA ControlMinder Distribution Server http://www.ca.com Copyright (c) 2013 CA International All rights reserved. ca technologies Exit Uninstall System Requirements Install

Click the OK button to accept English as the language for the installation.	 CA ControlMinder Copyright © 2013 CA. All rights reserved. English
Click the Next button.	 CA ControlMinder Distribution Server Introduction InstallAnywhere will guide you through the installation of CA ControlMinder Distribution Server. It is strongly recommended that you quit all programs before continuing with this installation. Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button. You may cancel this installation at any time by clicking the 'Cancel' button.

Read the License Agreement as you use the scrollbar to advance through the document. Click the radial button noting I accept the terms of the License Agreement. Click the Next button.	 CA ControlMinder Distribution Server License Agreement **Installation and Use of CA ControlMinder Distribution Server Requires Acceptance of the Following License Agreement:** If you proceed with this installation, you accept the terms of this license agreement. To proceed, select I accept the terms of the License Agreement and click Next. To cancel, select I do NOT accept the terms of the License Agreement and click Cancel. CONSOLE If you proceed with this installation, you accept the terms of this license agreement. To proceed, press Y. To cancel, press N. ● I accept the terms of the License Agreement ○ I do NOT accept the terms of the License Agreement technologies InstallAnywhere Cancel Previous Next
Select the installation directory. Click the Next button.	 CA ControlMinder Distribution Server Choose Install Folder Please choose a destination folder for this installation. C:\Program Files\CA\AccessControlDistServer Restore Default Folder Choose... technologies InstallAnywhere Cancel Previous Next

Select the location where you previously installed the Java JDK from the Third-Party Components ISO image. Click the Next button.	 CA ControlMinder Distribution Server C:\Windows\system32\java.exe C:\Program Files\Java\jdk1.7.0_21\bin\java.exe C:\Program Files\Java\jdk1.7.0_21\jre\bin\java.exe C:\Program Files\Java\jre7\bin\java.exe Search Another Location... InstallAnywhere Cancel Previous Next
Provide the message queue password. This is the communication password you specified during the ENTM Server installation. Click the Next button.	 CA ControlMinder Distribution Server Message Queue Settings Please provide the message queues settings. Password: *********** Confirm Password: ***********

Provide the ENTM Server hostname. Ensure this hostname can be resolved. Click the Next button.	 CA ControlMinder Distribution Server Message Queue Settings Please provide the Enterprise Management Hostname. Enterprise Management Hostname: WIN-LKLJMLRD44O
Provide a password for the Java Connector Server. Click the Next button.	 CA ControlMinder Distribution Server Java Connector Server - Provisioning Directory Information Please specify the following connection password for the Java Connector Server. Password: *********** Confirm Password: ***********

Click the Install button.	 CA ControlMinder Distribution Server **Pre-Installation summary** **Please Review the Following Before Continuing:** **Product Name:** CA ControlMinder Distribution Server **Install Folder:** C:\Program Files\CA\AccessControlDistServer **Application Version:** 12.80.0.1211
After the installation successfully completes, click the Done button to reboot the server and finalize the installation.	 CA ControlMinder Distribution Server **Installation Complete** Congratulations! CA ControlMinder Distribution Server has been successfully installed to: C:\Program Files\CA\AccessControlDistServer Press "Done" to quit the installer. Legal Notice: 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 You need to restart the system to complete the installation. ● Yes, restart my system ○ No, I will restart my system myself

Install ControlMinder Endpoints

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

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

Open Required Communication Ports

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

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

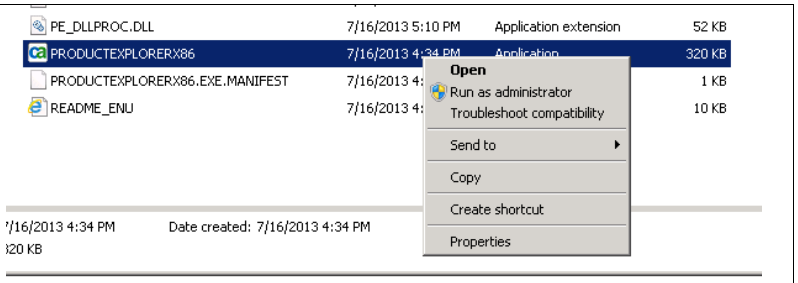
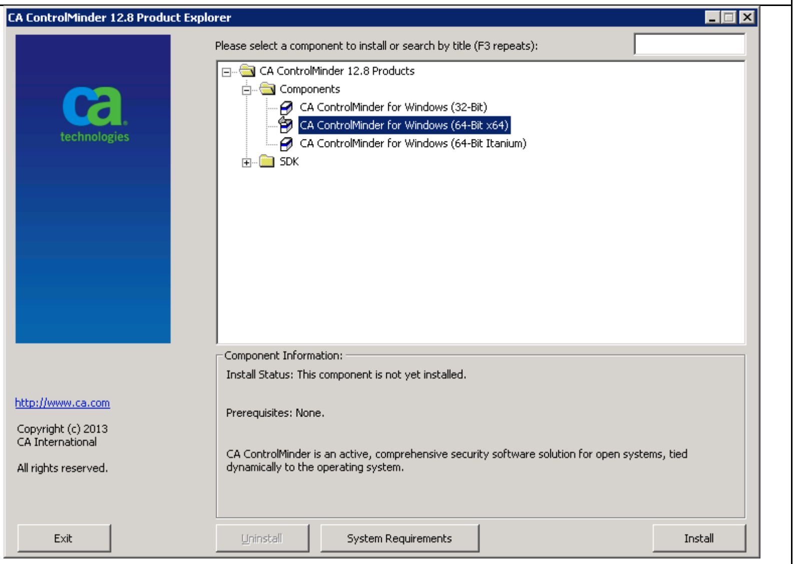
Microsoft Windows Installation

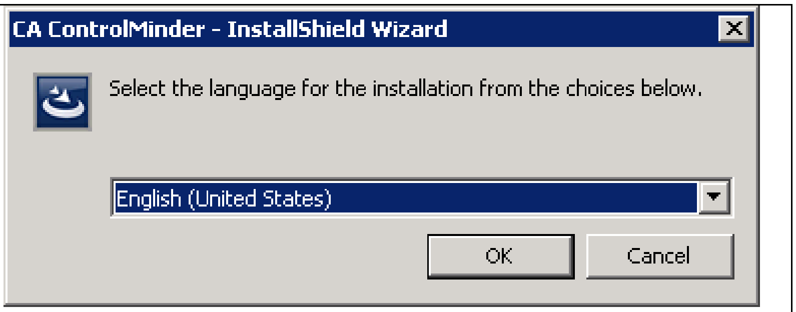
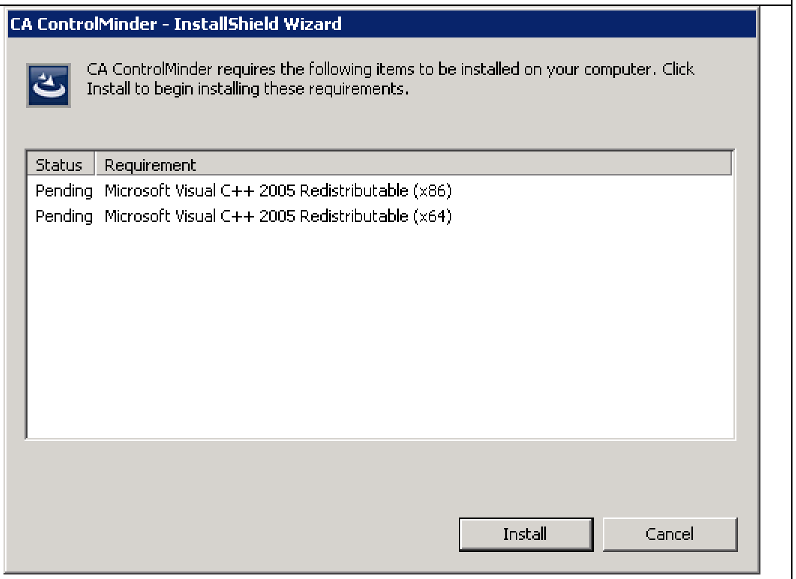
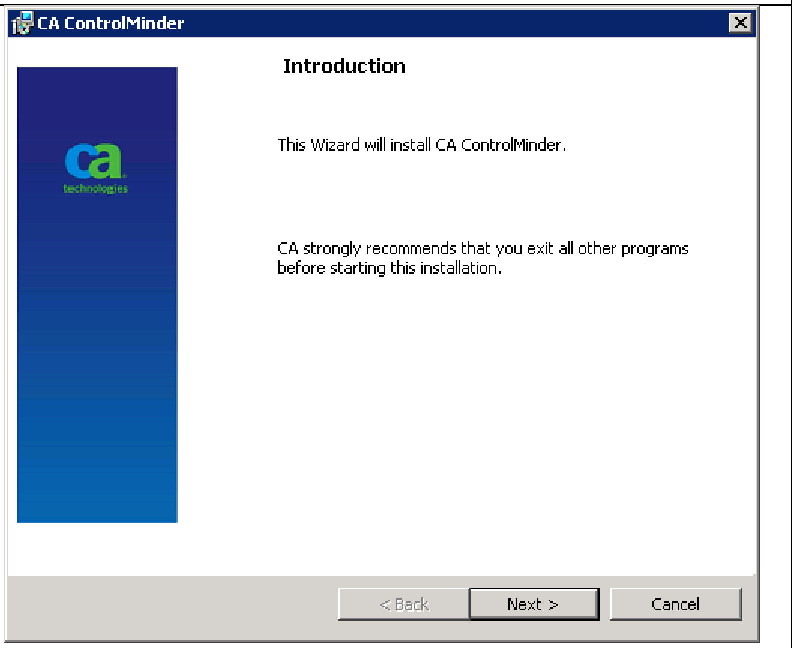
Transfer the CA ControlMinder Endpoint software to the instance.

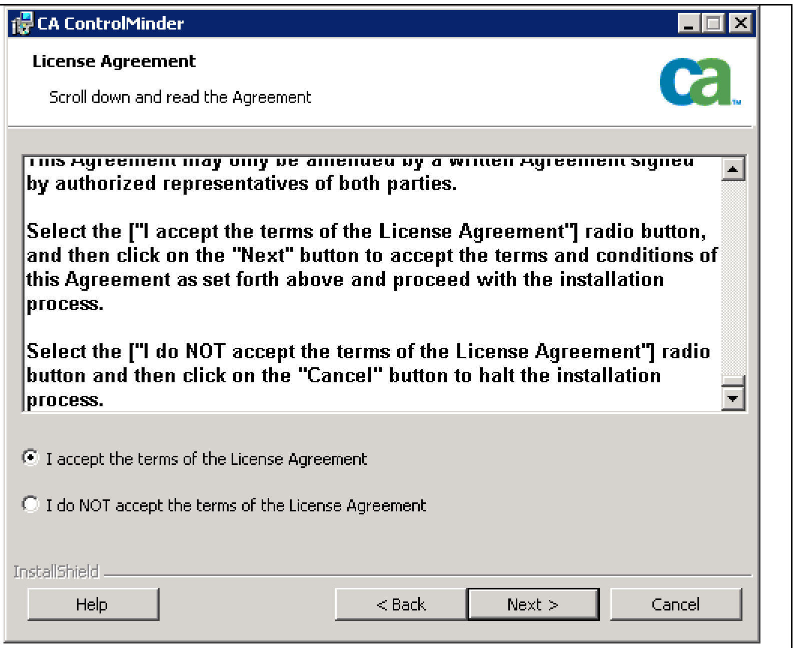
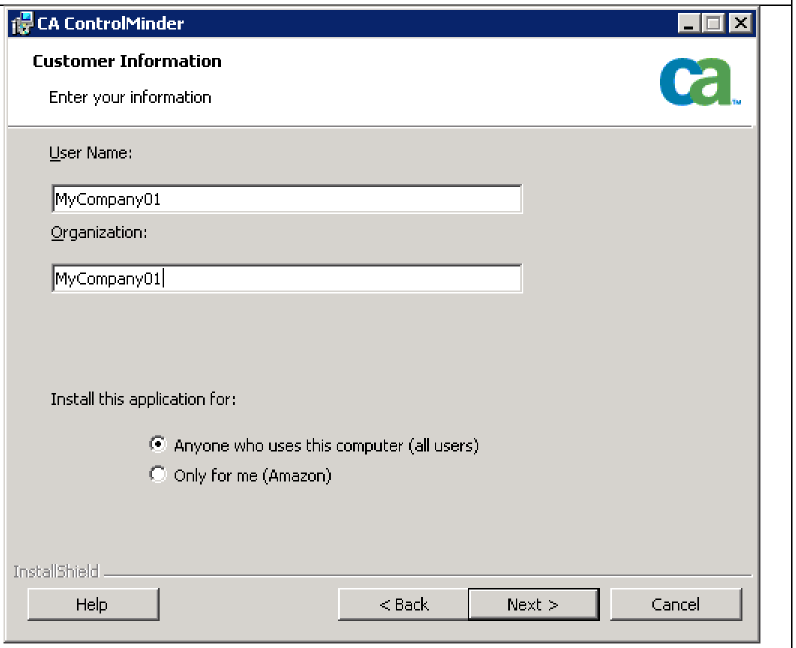
You can either mount the ISO image or extract all of the files from the ISO image.

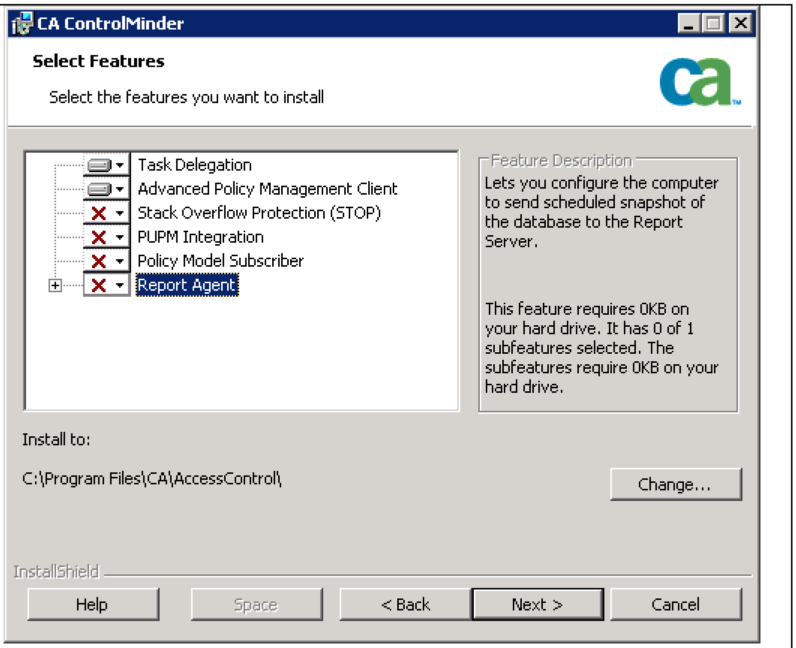
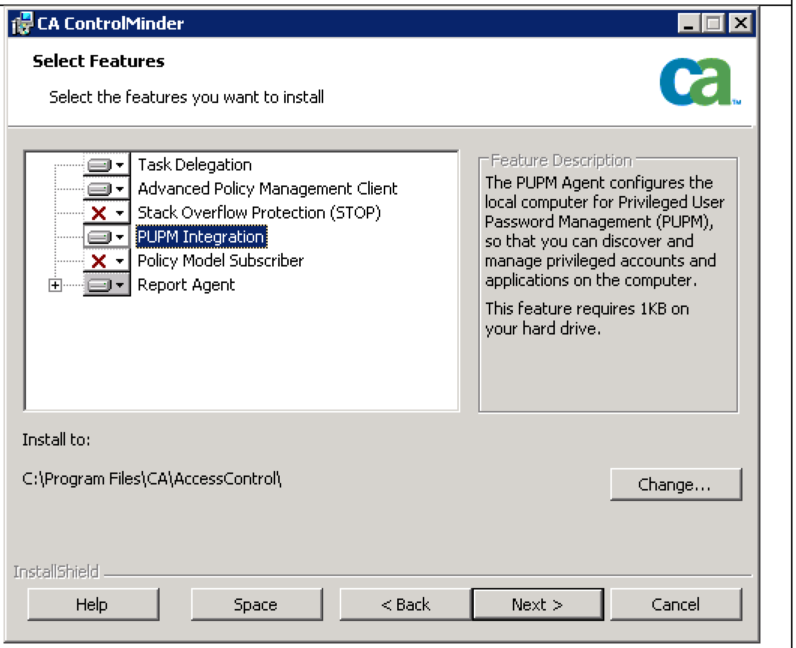
You must be a member of the local Administrators group to perform the installation.

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

Locate the PRODUCTEXPLORERX86.EXE executable. Right-click the executable and choose Run as administrator to start the installation.	 PE_DLLPROC.DLL 7/16/2013 5:10 PM Application extension 52 KB PRODUCTEXPLORERX86 7/16/2013 4:34 PM Application 320 KB PRODUCTEXPLORERX86.EXE.MANIFEST 7/16/2013 4: 1 KB README_ENU 7/16/2013 4: 10 KB 7/16/2013 4:34 PM Date created: 7/16/2013 4:34 PM 320 KB Open Run as administrator Troubleshoot compatibility Send to Copy Create shortcut Properties
This example assumes that the endpoint is a 64-bit Intel/AMD architecture. From the Components folder of the Product Explorer, select CA ControlMinder for Windows (64-Bit x64)Click the Install button.	 CA ControlMinder 12.8 Product Explorer Please select a component to install or search by title (F3 repeats): CA ControlMinder 12.8 Products Components CA ControlMinder for Windows (32-Bit) CA ControlMinder for Windows (64-Bit x64) CA ControlMinder for Windows (64-Bit Itanium) SDK Component Information: Install Status: This component is not yet installed. Prerequisites: None. CA ControlMinder is an active, comprehensive security software solution for open systems, tied dynamically to the operating system. http://www.ca.com Copyright (c) 2013 CA International All rights reserved. technologies Exit Uninstall System Requirements Install

Select the language for the installation and click the OK button.	 CA ControlMinder - InstallShield Wizard Select the language for the installation from the choices below. English (United States)
If prompted to install Microsoft Visual C++ Redistributable libraries, click the Install button.	 CA ControlMinder - InstallShield Wizard CA ControlMinder requires the following items to be installed on your computer. Click Install to begin installing these requirements. Status Requirement Pending Microsoft Visual C++ 2005 Redistributable (x86) Pending Microsoft Visual C++ 2005 Redistributable (x64)
Click the Next button to proceed with the ControlMinder endpoint software installation.	 CA ControlMinder Introduction This Wizard will install CA ControlMinder. CA strongly recommends that you exit all other programs before starting this installation.

Read the License Agreement as you use the scrollbar to advance through the document. Click the radial button noting I accept the terms of the License Agreement. Click the Next button.	 CA ControlMinder **License Agreement** Scroll down and read the Agreement **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.** ● I accept the terms of the License Agreement ○ I do NOT accept the terms of the License Agreement
Provide customer information. Click the Next button.	 CA ControlMinder **Customer Information** Enter your information User Name: MyCompany01 Organization: MyCompany01 Install this application for: ● Anyone who uses this computer (all users) ○ Only for me (Amazon)

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.	 CA ControlMinder **Select Features** Select the features you want to install Task Delegation Advanced Policy Management Client ✗ Stack Overflow Protection (STOP) ✗ PUPM Integration ✗ Policy Model Subscriber ✗ Report Agent Feature Description Lets you configure the computer to send scheduled snapshot of the database to the Report Server. This feature requires 0KB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive. Install to: C:\Program Files\CA\AccessControl\ Change... InstallShield Help Space < Back Next > Cancel
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 **Select Features** Select the features you want to install Task Delegation Advanced Policy Management Client ✗ Stack Overflow Protection (STOP) PUPM Integration ✗ Policy Model Subscriber Report Agent Feature Description The PUPM Agent configures the local computer for Privileged User Password Management (PUPM), so that you can discover and manage privileged accounts and applications on the computer. This feature requires 1KB on your hard drive. Install to: C:\Program Files\CA\AccessControl\ Change... InstallShield Help Space < Back Next > Cancel

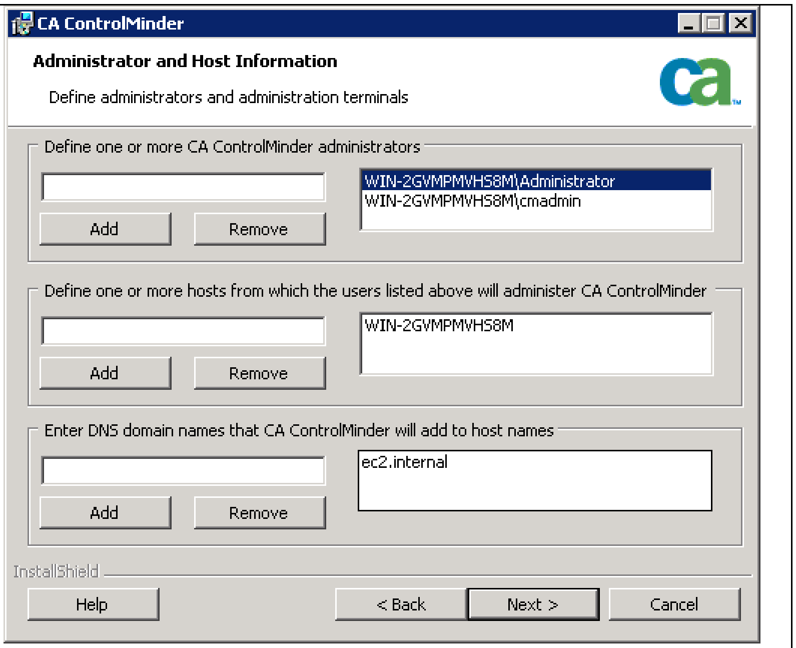
Provide the names of the ControlMinder administrators.

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

WIN-2GVMPMVHS8M\Administrator
WIN-2GVMPMVHS8M\cmadmin

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

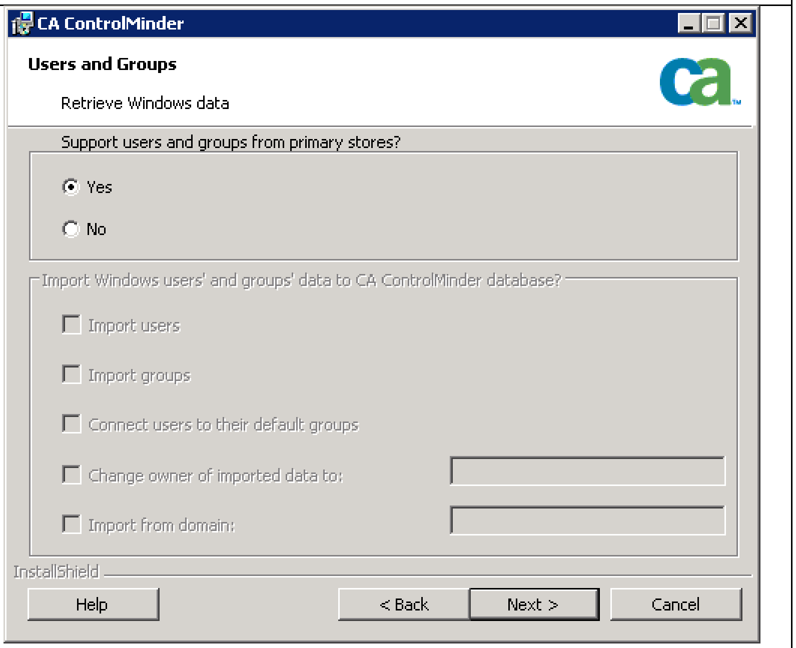
WIN-2GVMPMVHS8M

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

ec2.internal

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?

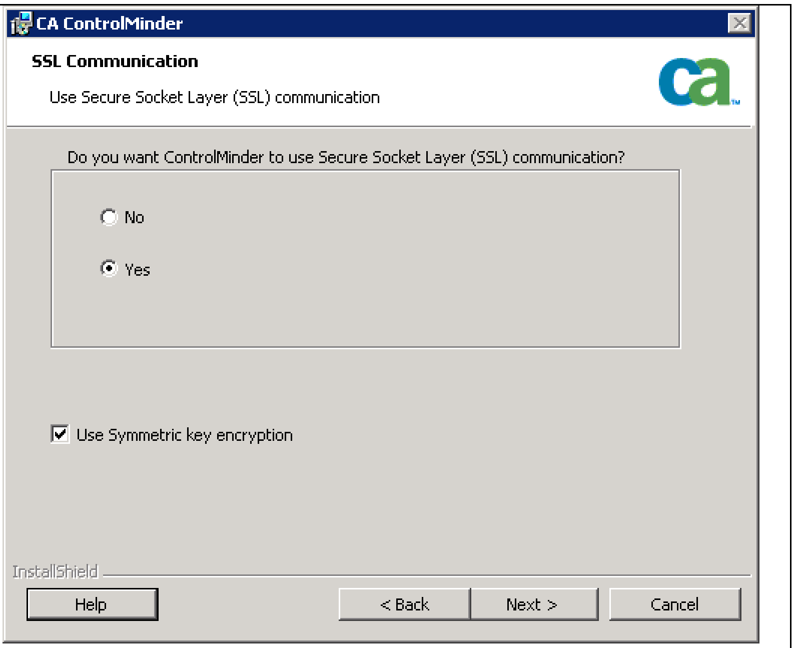
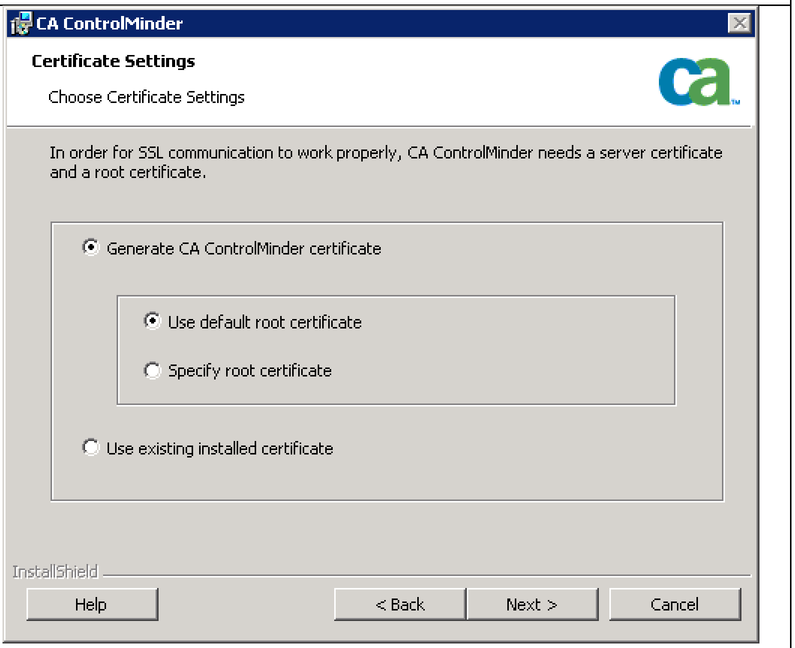
□ Import users

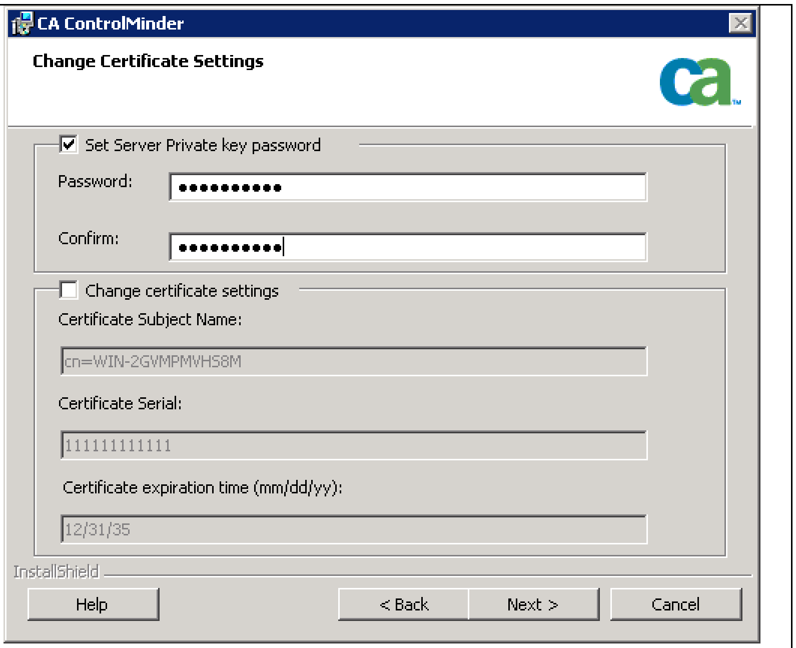
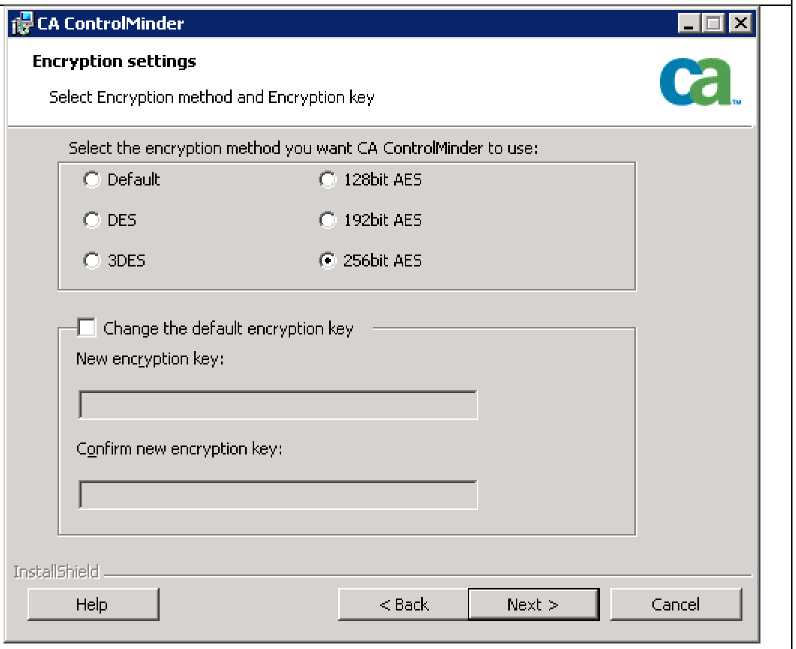
□ Import groups

□ Connect users to their default groups

□ Change owner of imported data to:

□ Import from domain:

Click the radial button for Yes to use Secure Socket Layer (SSL) communication. Leave the Use Symmetric key encryption checkbox checked. Click the Next button.	 CA ControlMinder **SSL Communication** Use Secure Socket Layer (SSL) communication Do you want ControlMinder to use Secure Socket Layer (SSL) communication? ○ No ● Yes ☑ Use Symmetric key encryption
Specify the certificate to use for SSL communication. The example in the screenshot uses a default root certificate to create a self-signed certificate. A consideration is whether or not to use a certificate generated by the Certificate Authority employed by your organization. Click the Next button.	 CA ControlMinder **Certificate Settings** Choose Certificate Settings In order for SSL communication to work properly, CA ControlMinder needs a server certificate and a root certificate. ● Generate CA ControlMinder certificate ● Use default root certificate ○ Specify root certificate ○ Use existing installed certificate

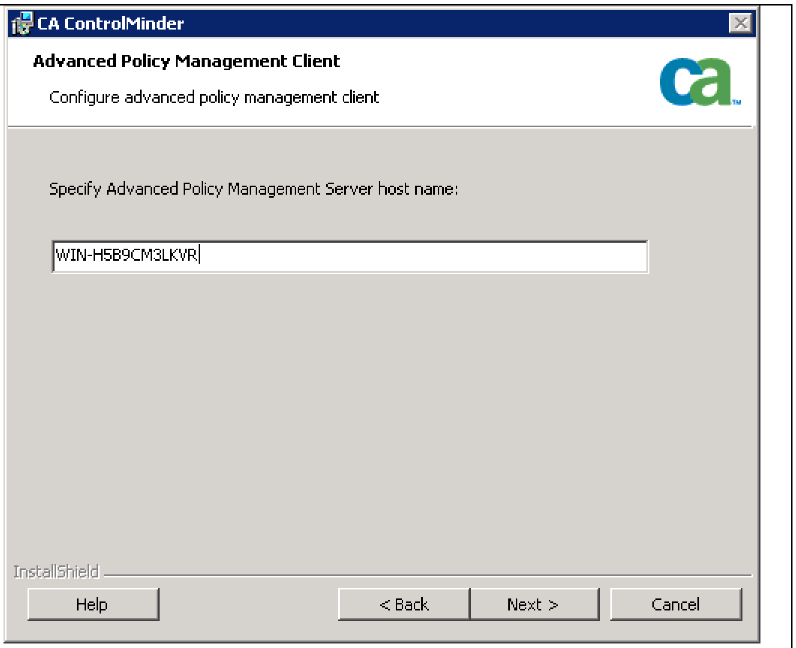
Provide the password of the certificate's private key. Click the Next button.	CA ControlMinder Change Certificate Settings ☑ Set Server Private key password Password: ●●●●●●●●●●● Confirm: ●●●●●●●●●●● ☐ Change certificate settings Certificate Subject Name: cn=WIN-2GVMPMVHS8M Certificate Serial: 111111111111 Certificate expiration time (mm/dd/yy): 12/31/35
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:

Provide the hostname of the Distribution Server.

All communication between the endpoint and the ENTM Server flows through the Distribution Server.

The endpoint must be able to resolve the hostname of the Distribution Server.

Click the Next button.



Advanced Policy Management Client

Configure advanced policy management client

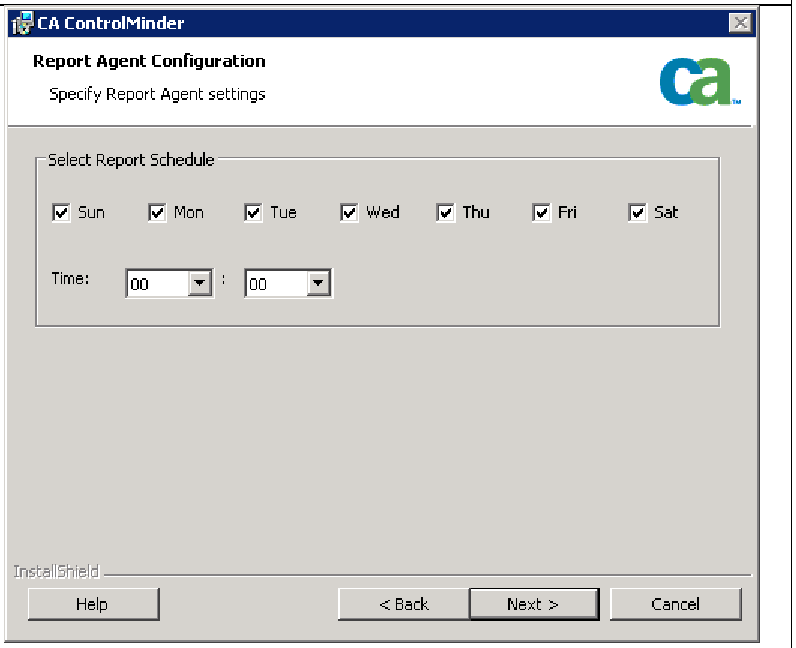
Specify Advanced Policy Management Server host name:

WIN-H5B9CM3LKVR

Specify when the Report Agent sends snapshots of the endpoint’s ControlMinder database to the ENTM Server (via the Distribution Server).

The snapshot data are used for reporting purposes.

Click the Next button.



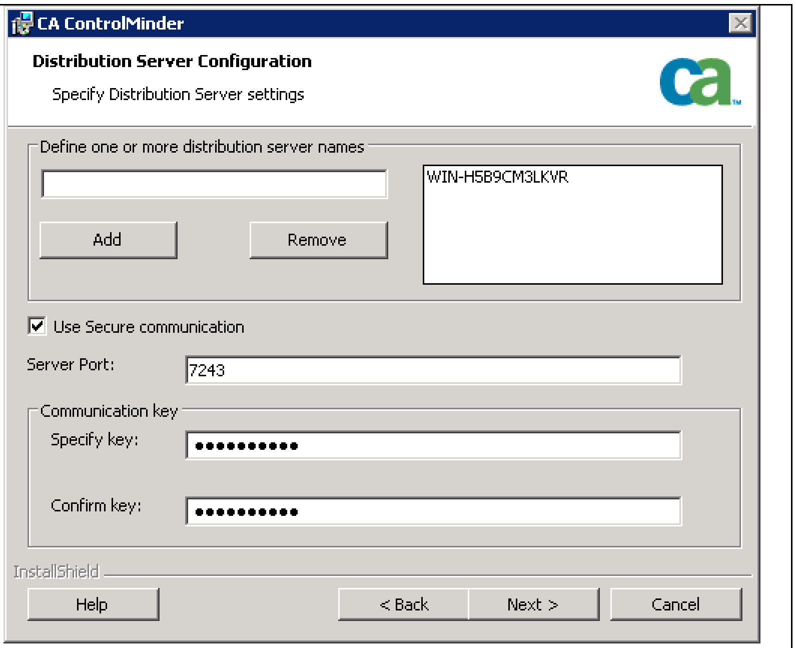
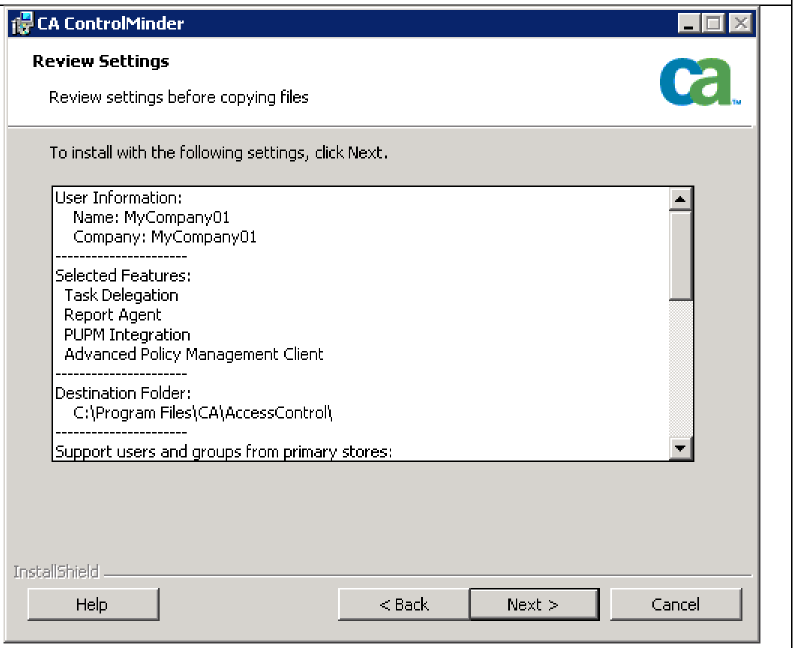
Report Agent Configuration

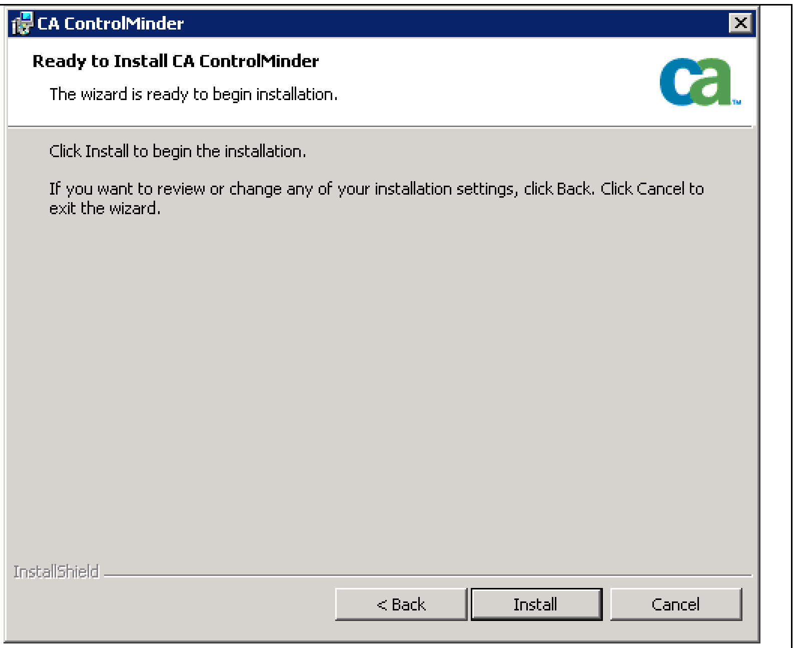
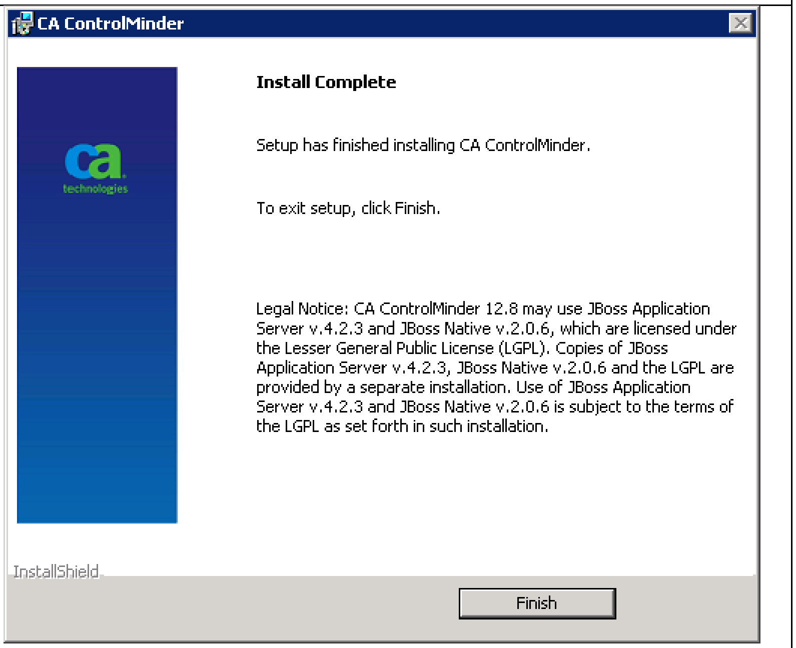
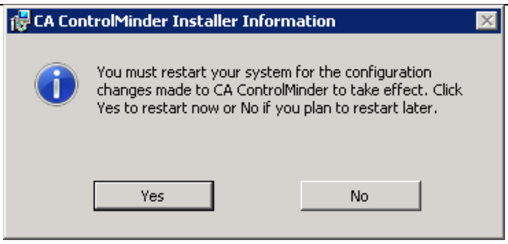
Specify Report Agent settings

Select Report Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time: 00 : 00

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

Click the Install button.	 CA ControlMinder **Ready to Install CA ControlMinder** The wizard is ready to begin installation. Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
After the installation has completed, click the Finish button.	 CA ControlMinder **Install Complete** Setup has finished installing CA ControlMinder. To exit setup, click Finish. Legal Notice: CA ControlMinder 12.8 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.
The installation may require a reboot to load ControlMinder kernel drivers. Click the Yes button to reboot now or click the No button to manually reboot at a later time.	 CA ControlMinder Installer Information 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.

Ubuntu Installation

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

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

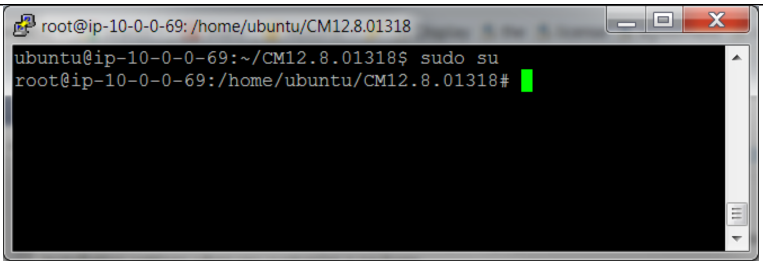
You need the following files from the CA ControlMinder UNIX Endpoint installation DVD:

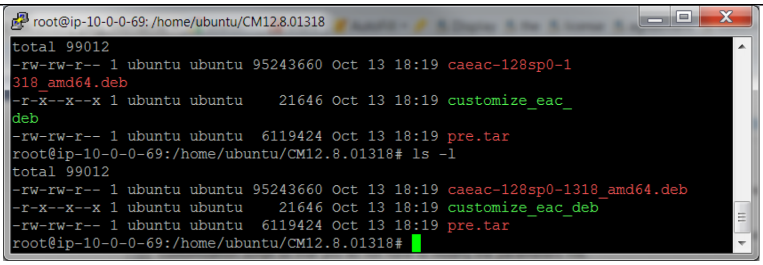
- caeac-xxxspx-xxx_amd64.deb
- customize_eac_deb
- pre.tar

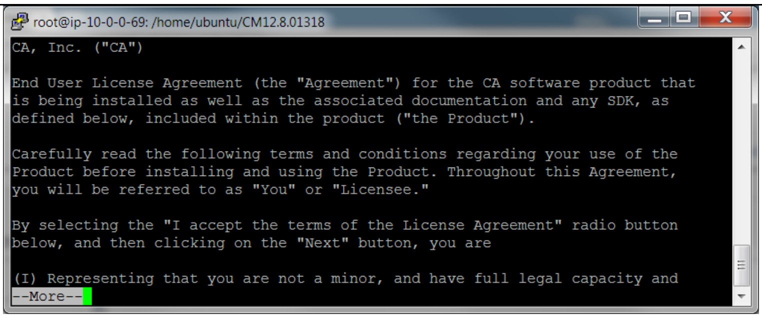
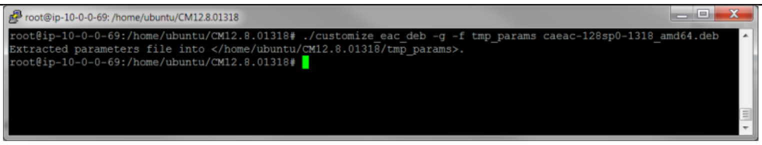
These are usually located under NativePackages\RPMPackages\DEBIAN directory.

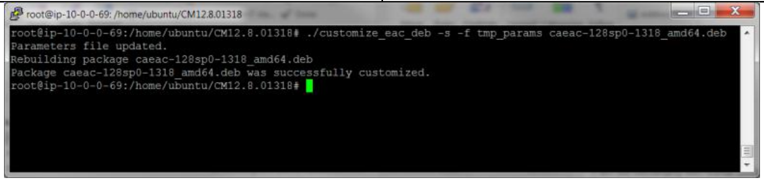
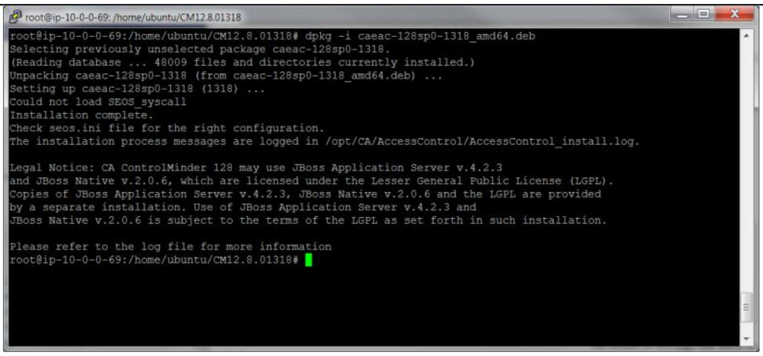
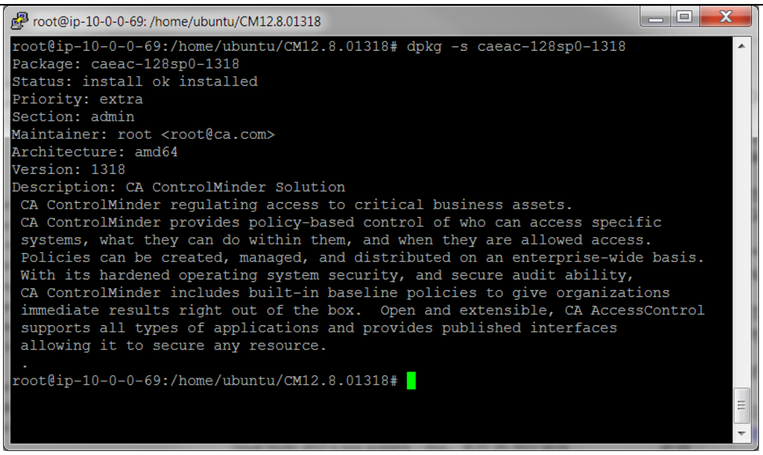
Before you can install CA ControlMinder using a native package, you must customize the CA ControlMinder package to specify that you accept the license agreement. You can also specify custom installation settings when you customize the package.

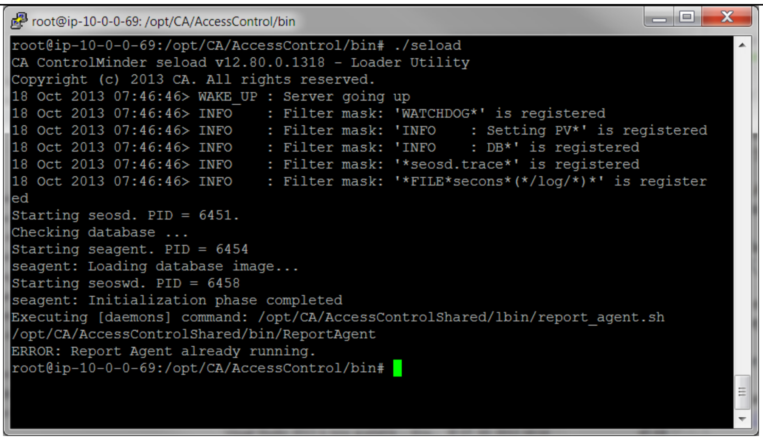
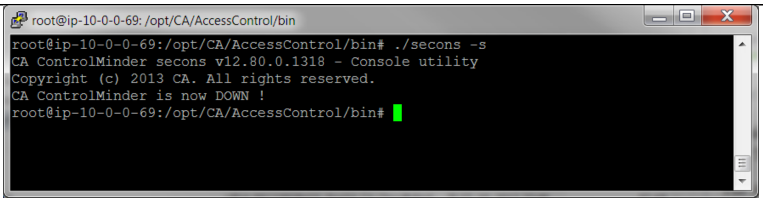
You customize a package by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

Change your identity to root by running:
sudo su
	
	`ubuntu@ip-10-0-0-69:~/CM12.8.01318$ sudo su`
	`root@ip-10-0-0-69:/home/ubuntu/CM12.8.01318#`

Change to the directory where the installation package is located.
Make sure that customize_eac_deb is executable.
	
	`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#`

Run: customize_eac_deb -a pkg_filename to display the license agreement. Take note of the keyword that appears at the end of the license agreement inside square brackets. You specify this keyword in the next step.	 root@ip-10-0-0-69: /home/ubuntu/CM12.8.01318 CA, Inc. ("CA") End User License Agreement (the "Agreement") for the CA software product that is being installed as well as the associated documentation and any SDK, as defined below, included within the product ("the Product"). Carefully read the following terms and conditions regarding your use of the Product before installing and using the Product. Throughout this Agreement, you will be referred to as "You" or "Licensee." By selecting the "I accept the terms of the License Agreement" radio button below, and then clicking on the "Next" button, you are (I) Representing that you are not a minor, and have full legal capacity and --More--	
Get the installation parameters file and save it as tmp_params by running: customize_eac_deb -g -f tmp_params pkg_filename	 root@ip-10-0-0-69: /home/ubuntu/CM12.8.01318 root@ip-10-0-0-69:/home/ubuntu/CM12.8.01318# ./customize_eac_deb -g -f tmp_params caeac-128sp0-1318_amd64.deb Extracted parameters file into </home/ubuntu/CM12.8.01318/tmp_params>. root@ip-10-0-0-69:/home/ubuntu/CM12.8.01318#	
Open the tmp_params file for editing and customize the parameters.	LIC_CMD=	Provide the keyword you extracted earlier noting that you accept the license agreement.
	ADMIN_USERS=”root,ubuntu”	Specifies the the root and ubuntu users are ControlMinder administrators of the endpoint.
	ENCRYPTION_METHOD_SET=3	Specifies that both SSL encryption and Symmectric key encryption are enabled.
	DH_NAME=”Distribution_Server_Hostname”	Hostname of the Distribution Server that manages the endpoint. NOTE: the endpoint must be able to resolve this hostname.
	DIST_SRV_HOST=”Distribution_Server_Hostname”	Use the same value as assigned to DH_NAME.
	INSTALL_RA=”yes”	Install the Report Agent for collecting endpoint snapshots and optionally to collect audit events.
	REPORT_SHARED_SECRET=My Secret	This is the communication password specified when Enterprise Management was installed. Report Agent uses it to communicate to the Message Queue.
	ENABLE_ELM=”no”	Determines whether or not audit events are collected. Set to “no”

		unless a UAR server is implemented.
	INSTALL_PUPM="yes"	Installs the PUPM Agent.
Save your customized settings in installation package. customize_eac_deb -s -f tmp_params pkg_filename The package will be updated with the customized settings.	 root@ip-10-0-0-69:/home/ubuntu/CM12.8.01318# ./customize_eac_deb -s -f tmp_params caeac-128sp0-1318_amd64.deb Parameters file updated. Rebuilding package caeac-128sp0-1318_amd64.deb Package caeac-128sp0-1318_amd64.deb was successfully customized. root@ip-10-0-0-69:/home/ubuntu/CM12.8.01318#	
Install the CA ControlMinder package: dpkg -i caeac-xxxspx-xxx_amd64.deb The package is installed into the /opt/CA/ directory by default. The installation directory can be modified in the parameter file.	 root@ip-10-0-0-69:/home/ubuntu/CM12.8.01318# dpkg -i caeac-128sp0-1318_amd64.deb Selecting previously unselected package caeac-128sp0-1318. (Reading database ... 48009 files and directories currently installed.) Unpacking caeac-128sp0-1318 (from caeac-128sp0-1318_amd64.deb) ... Setting up caeac-128sp0-1318 (1318) ... Could not load SEOS_syscall Installation complete. Check seos.ini file for the right configuration. The installation process messages are logged in /opt/CA/AccessControl/AccessControl_install.log. Legal Notice: CA ControlMinder 128 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. Please refer to the log file for more information root@ip-10-0-0-69:/home/ubuntu/CM12.8.01318#	
Verify that the package status is "OK installed". dpkg -s caeac-xxxspx-xxx	 root@ip-10-0-0-69:/home/ubuntu/CM12.8.01318# dpkg -s caeac-128sp0-1318 Package: caeac-128sp0-1318 Status: install ok installed Priority: extra Section: admin Maintainer: root <root@ca.com> Architecture: amd64 Version: 1318 Description: CA ControlMinder Solution CA ControlMinder regulating access to critical business assets. CA ControlMinder provides policy-based control of who can access specific systems, what they can do within them, and when they are allowed access. Policies can be created, managed, and distributed on an enterprise-wide basis. With its hardened operating system security, and secure audit ability, CA ControlMinder includes built-in baseline policies to give organizations immediate results right out of the box. Open and extensible, CA AccessControl supports all types of applications and provides published interfaces allowing it to secure any resource. . root@ip-10-0-0-69:/home/ubuntu/CM12.8.01318#	

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

```
root@ip-10-0-0-69:/opt/CA/AccessControl/bin# ./seload
CA ControlMinder seload v12.80.0.1318 - Loader Utility
Copyright (c) 2013 CA. All rights reserved.
18 Oct 2013 07:46:46> WAKE_UP : Server going up
18 Oct 2013 07:46:46> INFO    : Filter mask: 'WATCHDOG*' is registered
18 Oct 2013 07:46:46> INFO    : Filter mask: 'INFO    : Setting PV*' is registered
18 Oct 2013 07:46:46> INFO    : Filter mask: 'INFO    : DB*' is registered
18 Oct 2013 07:46:46> INFO    : Filter mask: '*seosd.trace*' is registered
18 Oct 2013 07:46:46> INFO    : Filter mask: '*FILE*secons*(*/log/*)*' is register
ed
Starting seosd. PID = 6451.
Checking database ...
Starting seagent. PID = 6454
seagent: Loading database image...
Starting seoswd. PID = 6458
seagent: Initialization phase completed
Executing [daemons] command: /opt/CA/AccessControlShared/lbin/report_agent.sh
/opt/CA/AccessControlShared/bin/ReportAgent
ERROR: Report Agent already running.
root@ip-10-0-0-69:/opt/CA/AccessControl/bin#
```

```
root@ip-10-0-0-69:/opt/CA/AccessControl/bin# ./secons -s
CA ControlMinder secons v12.80.0.1318 - Console utility
Copyright (c) 2013 CA. All rights reserved.
CA ControlMinder is now DOWN !
root@ip-10-0-0-69:/opt/CA/AccessControl/bin#
```

To configure the endpoint software for automatic startup

Navigate to:

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

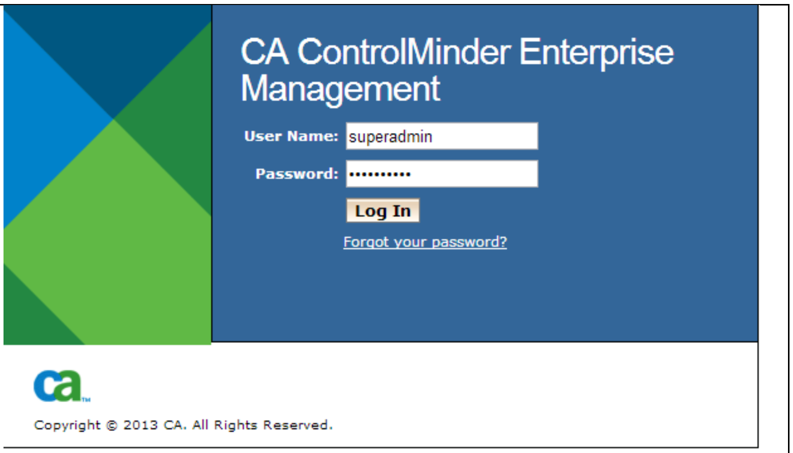
This directory contains a sample script that can be used to start CA ControlMinder at system startup time.

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

Validate Endpoint Installation

Login to Enterprise Management using the superadmin account.

NOTE: The superadmin account's password was specified when Enterprise Management was installed.



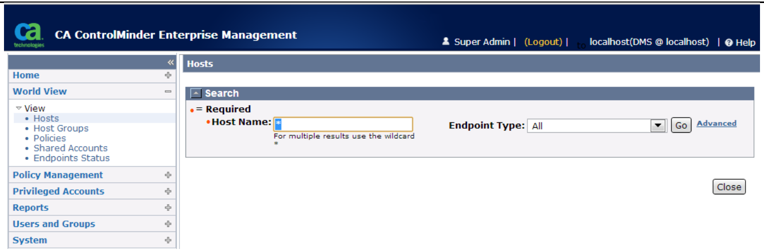
CA ControlMinder Enterprise Management

User Name: superadmin

Password: ••••••••••

Copyright © 2013 CA. All Rights Reserved.

Navigate to World View -> View -> Hosts



CA ControlMinder Enterprise Management

• = Required

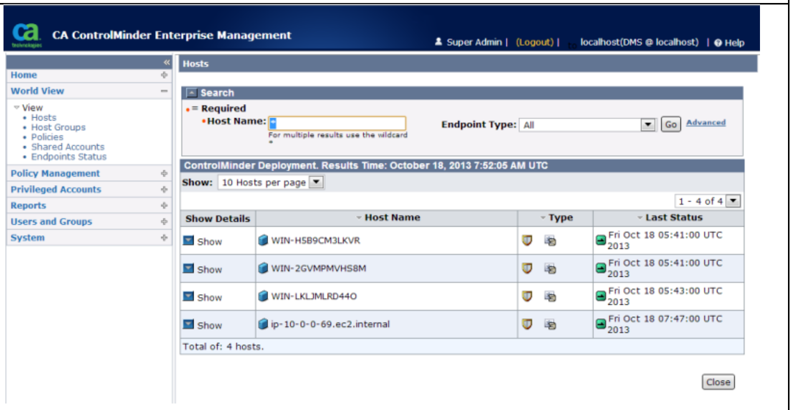
•Host Name: *

For multiple results use the wildcard *

Endpoint Type: All

Click Go to display the list of registered endpoints

Observe that the ENTM Server, Distribution Server, and Windows and Ubuntu endpoints (on which ControlMinder endpoint software was installed) are listed.



CA ControlMinder Enterprise Management

• = Required

•Host Name: *

For multiple results use the wildcard *

Endpoint Type: All

ControlMinder Deployment. Results Time: October 18, 2013 7:52:05 AM UTC

Show: 10 Hosts per page

1 - 4 of 4

Show Details	Host Name	Type	Last Status
Show	WIN-H5B9CM3LKVR		Fri Oct 18 05:41:00 UTC 2013
Show	WIN-2GVMPMVHS8M		Fri Oct 18 05:41:00 UTC 2013
Show	WIN-LKLJMLRD44O		Fri Oct 18 05:43:00 UTC 2013
Show	ip-10-0-0-69.ec2.internal		Fri Oct 18 07:47:00 UTC 2013

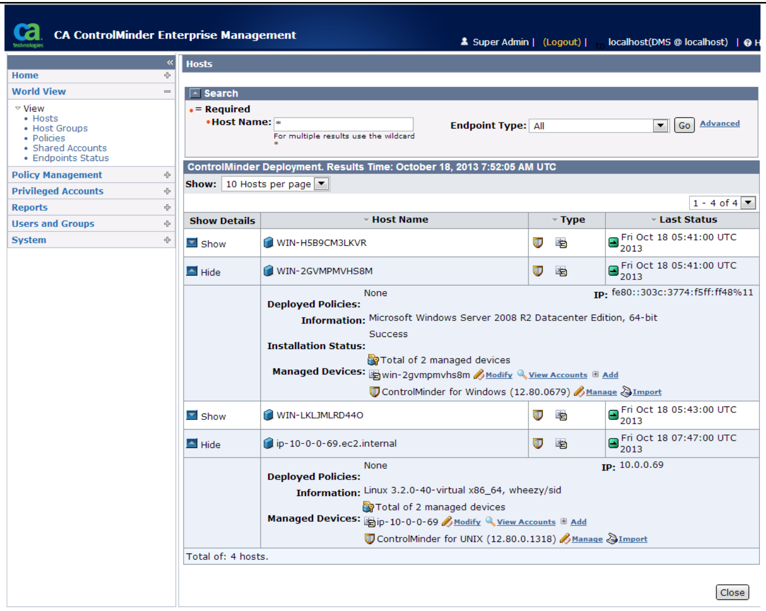
Total of: 4 hosts.

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.



• = Required

•Host Name: *

For multiple results use the wildcard *

Endpoint Type: All

ControlMinder Deployment. Results Time: October 18, 2013 7:52:05 AM UTC

Show: 10 Hosts per page

1 - 4 of 4

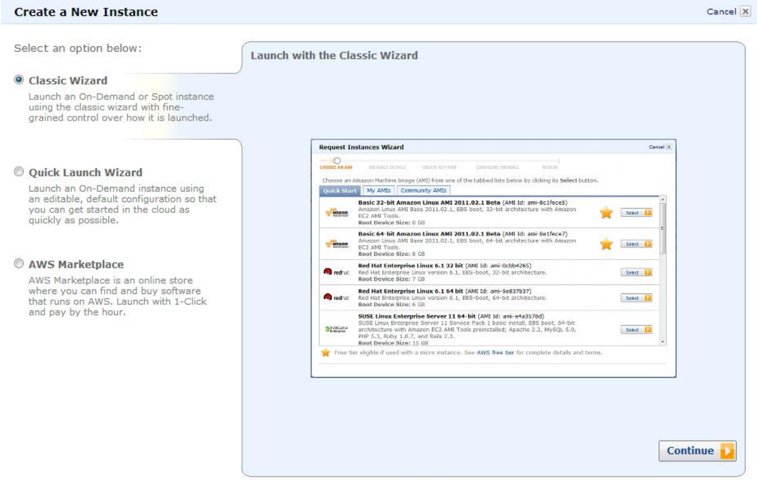
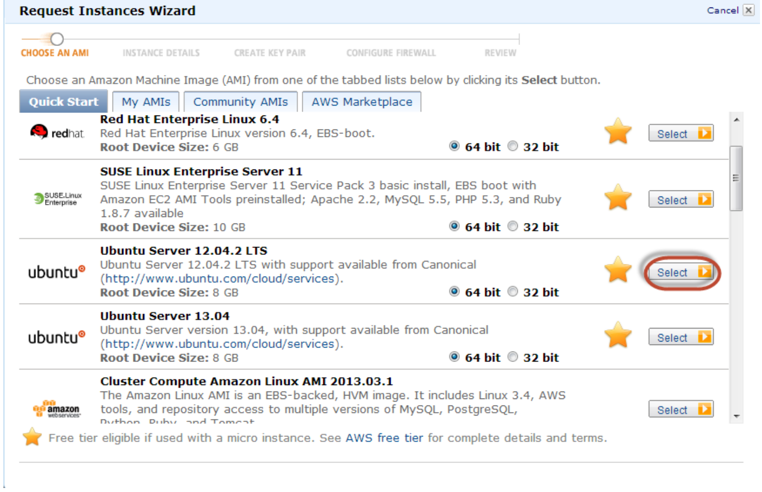
Show Details	Host Name	Type	Last Status
Show	WIN-H5B9CM3LKVR		Fri Oct 18 05:41:00 UTC 2013
Hide	WIN-2GVMPMVHS8M		Fri Oct 18 05:41:00 UTC 2013
	Deployed Policies: None Information: Microsoft Windows Server 2008 R2 Datacenter Edition, 64-bit Installation Status: Success Managed Devices: Total of 2 managed devices win-2gvmpmvhs8m Modify View Accounts Add ControlMinder for Windows (12.80.0679) Manage Import	IP: fe80::303c:3774:f5ff:ff48%11	
Show	WIN-LKLJMLRD44O		Fri Oct 18 05:43:00 UTC 2013
Hide	ip-10-0-0-69.ec2.internal		Fri Oct 18 07:47:00 UTC 2013
	Deployed Policies: None Information: Linux 3.2.0-40-virtual x86_64, wheezy/sid Managed Devices: Total of 2 managed devices ip-10-0-0-69 Modify View Accounts Add ControlMinder for UNIX (12.80.0.1318) Manage Import	IP: 10.0.0.69	

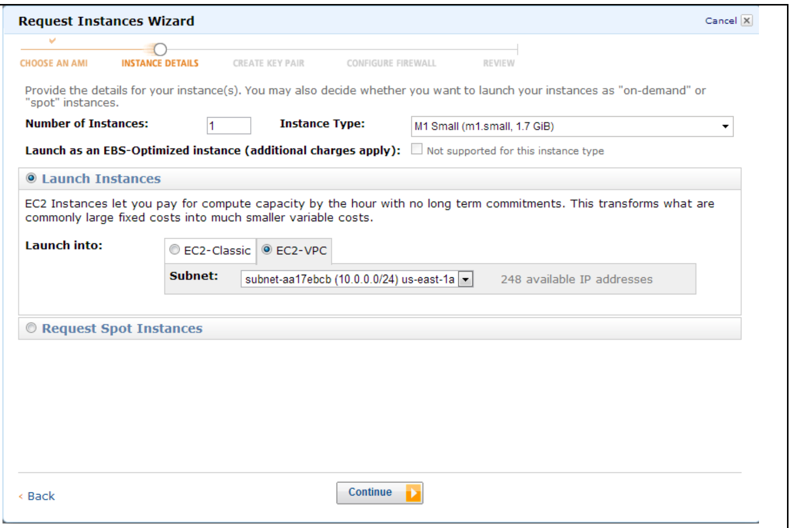
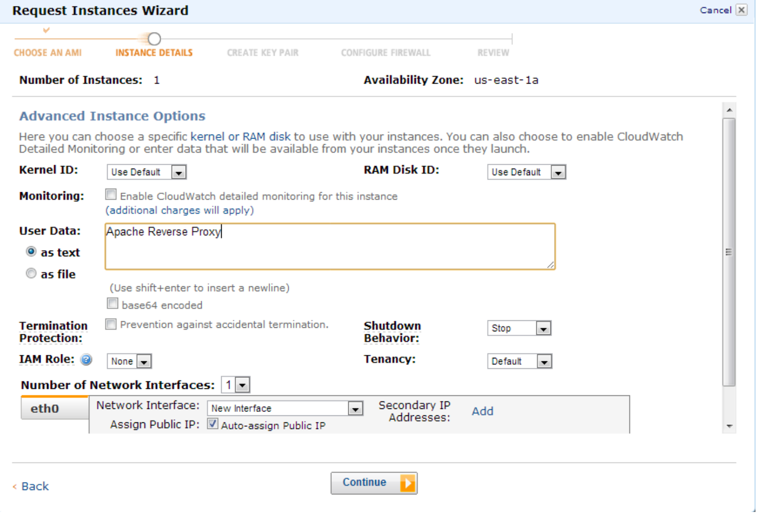
Total of: 4 hosts.

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

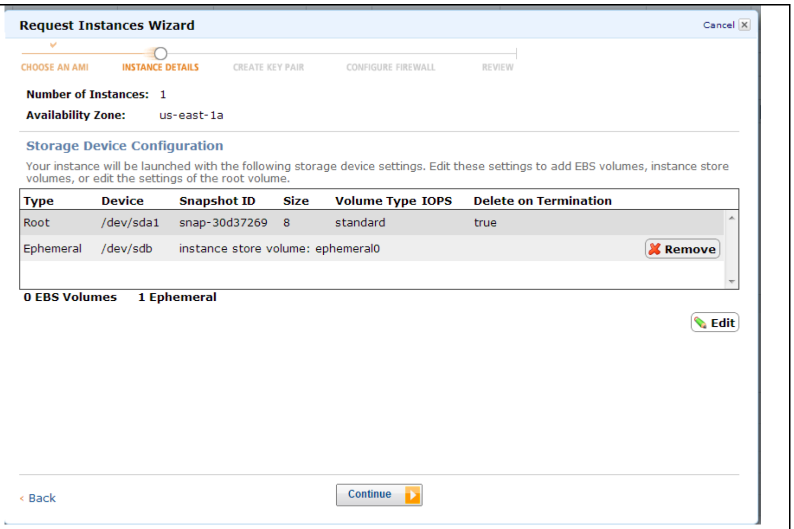
Use the Classic Wizard to launch an Ubuntu instance.	 Create a New Instance Cancel ☒ Select an option below: ● Classic Wizard Launch an On-Demand or Spot instance using the classic wizard with fine-grained control over how it is launched. ○ Quick Launch Wizard Launch an On-Demand instance using an editable, default configuration so that you can get started in the cloud as quickly as possible. ○ AWS Marketplace AWS Marketplace is an online store where you can find and buy software that runs on AWS. Launch with 1-Click and pay by the hour. Launch with the Classic Wizard Request Instances Wizard CHOOSE AN AMI · INSTANCE DETAILS · CREATE KEY PAIR · CONFIGURE FIREWALL · REVIEW Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its **Select** button. Quick Start · My AMIs · Community AMIs **Basic 32-bit Amazon Linux AMI 2011.02.1 Beta** (AMI Id: ami-8c1fece5) Amazon Linux AMI Base 2011.02.1, EBS boot, 32-bit architecture with Amazon EC2 AMI Tools. **Root Device Size:** 8 GB **Basic 64-bit Amazon Linux AMI 2011.02.1 Beta** (AMI Id: ami-8e1fece7) Amazon Linux AMI Base 2011.02.1, EBS boot, 64-bit architecture with Amazon EC2 AMI Tools. **Root Device Size:** 8 GB **Red Hat Enterprise Linux 6.1 32 bit** (AMI Id: ami-0cbb4265) Red Hat Enterprise Linux version 6.1, EBS-boot, 32-bit architecture. **Root Device Size:** 7 GB **Red Hat Enterprise Linux 6.1 64 bit** (AMI Id: ami-5e837b37) Red Hat Enterprise Linux version 6.1, EBS-boot, 64-bit architecture. **Root Device Size:** 6 GB **SUSE Linux Enterprise Server 11 64-bit** (AMI Id: ami-e4a3578d) SUSE Linux Enterprise Server 11 Service Pack 1 basic install, EBS boot, 64-bit architecture with Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.0, PHP 5.3, Ruby 1.8.7, and Rails 2.3. **Root Device Size:** 15 GB Free tier eligible if used with a micro instance. See AWS free tier for complete details and terms. Continue
Scroll through the Quick Start list of Amazon Machine Images (AMIs) and select a 64-bit Ubuntu Server.	 Request Instances Wizard Cancel ☒ CHOOSE AN AMI · INSTANCE DETAILS · CREATE KEY PAIR · CONFIGURE FIREWALL · REVIEW Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its **Select** button. Quick Start · My AMIs · Community AMIs · AWS Marketplace **Red Hat Enterprise Linux 6.4** Red Hat Enterprise Linux version 6.4, EBS-boot. **Root Device Size:** 6 GB ● 64 bit ○ 32 bit **SUSE Linux Enterprise Server 11** SUSE Linux Enterprise Server 11 Service Pack 3 basic install, EBS boot with Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available **Root Device Size:** 10 GB ● 64 bit ○ 32 bit **Ubuntu Server 12.04.2 LTS** Ubuntu Server 12.04.2 LTS with support available from Canonical (http://www.ubuntu.com/cloud/services). **Root Device Size:** 8 GB ● 64 bit ○ 32 bit **Ubuntu Server 13.04** Ubuntu Server version 13.04, with support available from Canonical (http://www.ubuntu.com/cloud/services). **Root Device Size:** 8 GB ● 64 bit ○ 32 bit **Cluster Compute Amazon Linux AMI 2013.03.1** The Amazon Linux AMI is an EBS-backed, HVM image. It includes Linux 3.4, AWS tools, and repository access to multiple versions of MySQL, PostgreSQL, Python, Ruby, and Tomcat Free tier eligible if used with a micro instance. See AWS free tier for complete details and terms.

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.	 **Request Instances Wizard** Cancel ☒ CHOOSE AN AMI · INSTANCE DETAILS · CREATE KEY PAIR · CONFIGURE FIREWALL · REVIEW Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances. **Number of Instances:** 1 **Instance Type:** M1 Small (m1.small, 1.7 GiB) **Launch as an EBS-Optimized instance (additional charges apply):** □ Not supported for this instance type ● **Launch Instances** EC2 Instances let you pay for compute capacity by the hour with no long term commitments. This transforms what are commonly large fixed costs into much smaller variable costs. **Launch into:** ○ EC2-Classic ● EC2-VPC **Subnet:** subnet-aa17ebcb (10.0.0.0/24) us-east-1a 248 available IP addresses ○ **Request Spot Instances** ‹ Back Continue
Provide User Data to identify your instance. Ensure the Auto-assign Public IP checkbox is checked. Click the Continue button.	 **Request Instances Wizard** Cancel ☒ CHOOSE AN AMI · INSTANCE DETAILS · CREATE KEY PAIR · CONFIGURE FIREWALL · REVIEW **Number of Instances:** 1 **Availability Zone:** us-east-1a **Advanced Instance Options** Here you can choose a specific kernel or RAM disk to use with your instances. You can also choose to enable CloudWatch Detailed Monitoring or enter data that will be available from your instances once they launch. **Kernel ID:** Use Default **RAM Disk ID:** Use Default **Monitoring:** □ Enable CloudWatch detailed monitoring for this instance (additional charges will apply) **User Data:** Apache Reverse Proxy ● 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 Secondary IP Addresses: Add Assign Public IP: ☑ Auto-assign Public IP ‹ Back Continue

Keep the default storage configuration.

8 gigabytes of disk storage is sufficient for the Apache Reverse Proxy Server.

Click the Continue button.



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

Storage Device Configuration

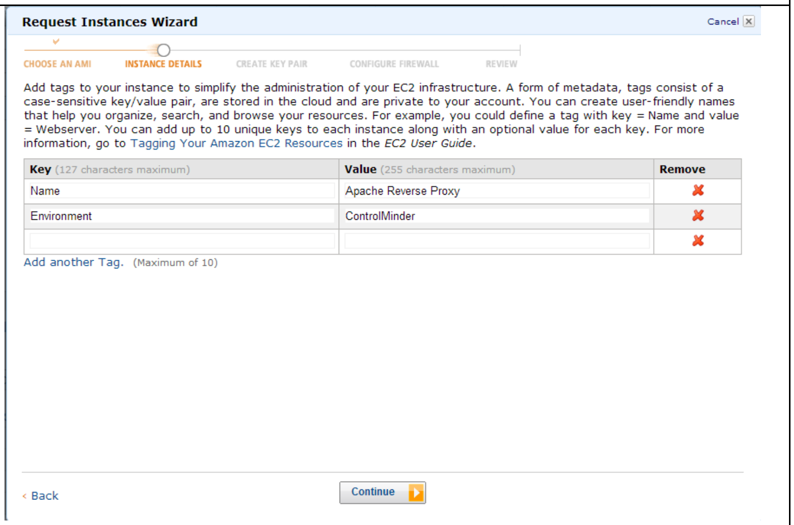
Your instance will be launched with the following storage device settings. Edit these settings to add EBS volumes, instance store volumes, or edit the settings of the root volume.

Type	Device	Snapshot ID	Size	Volume Type	IOPS	Delete on Termination
Root	/dev/sda1	snap-30d37269	8	standard		true
Ephemeral	/dev/sdb	instance store volume: ephemeral0				

0 EBS Volumes **1 Ephemeral**

Name your instance and provide any additional tags as required.

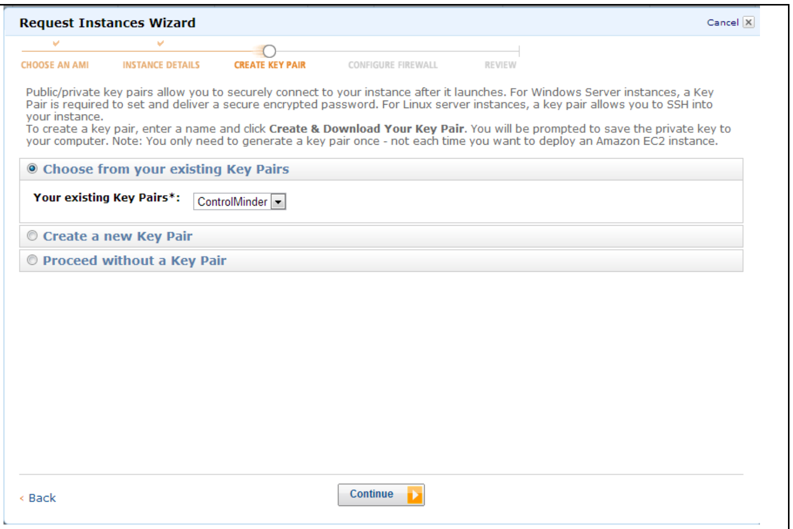
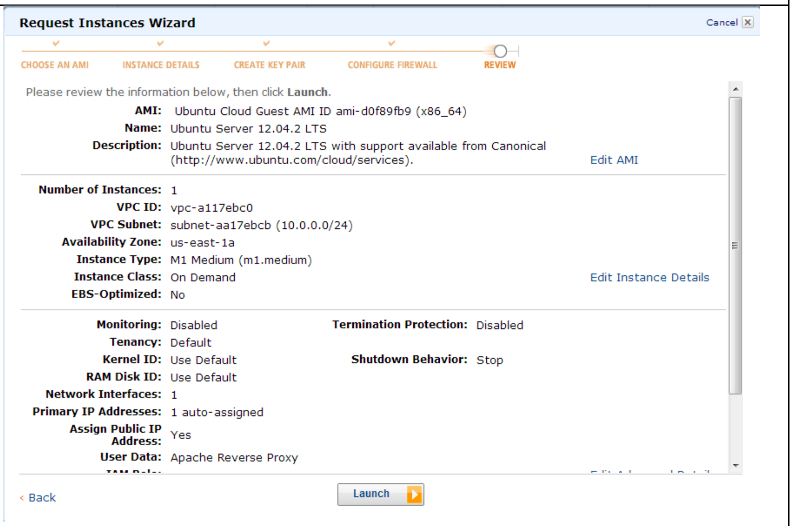
Click the Continue button.

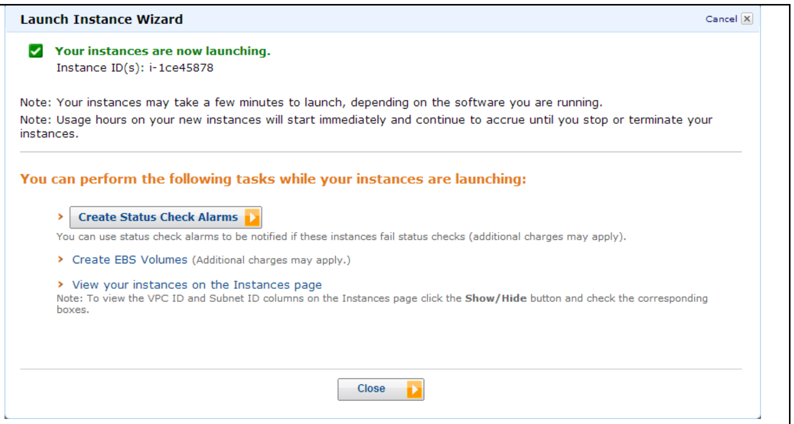


Add tags to your instance to simplify the administration of your EC2 infrastructure. A form of metadata, tags consist of a case-sensitive key/value pair, are stored in the cloud and are private to your account. You can create user-friendly names that help you organize, search, and browse your resources. For example, you could define a tag with key = Name and value = Webserver. You can add up to 10 unique keys to each instance along with an optional value for each key. For more information, go to Tagging Your Amazon EC2 Resources in the *EC2 User Guide*.

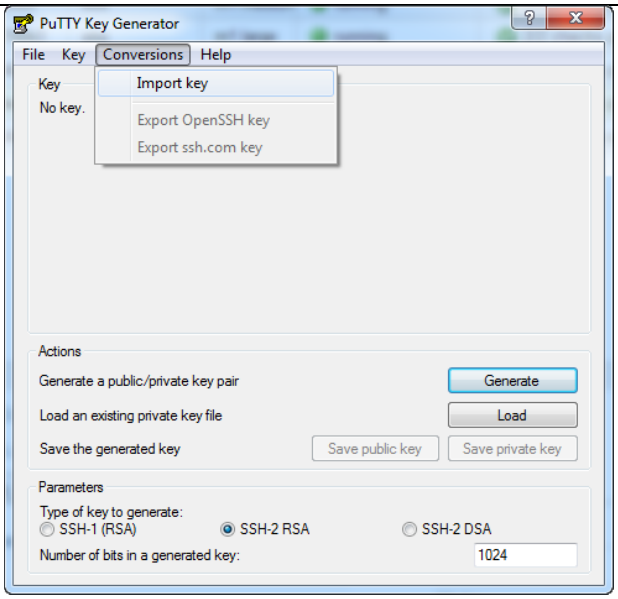
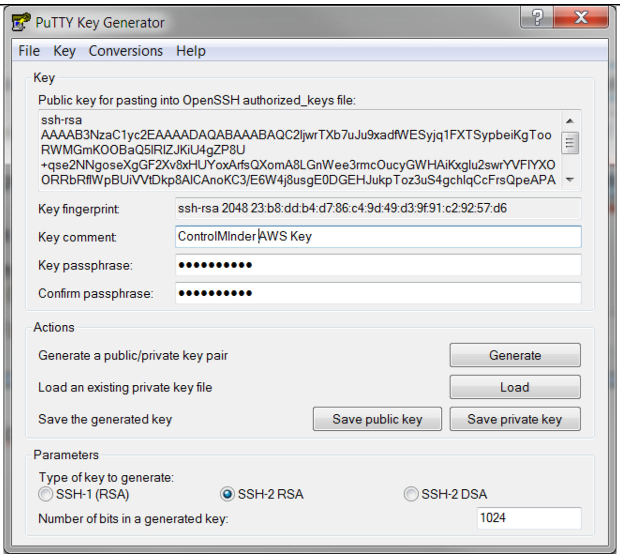
Key (127 characters maximum)	**Value** (255 characters maximum)	**Remove**
Name	Apache Reverse Proxy	✘
Environment	ControlMinder	✘
		✘

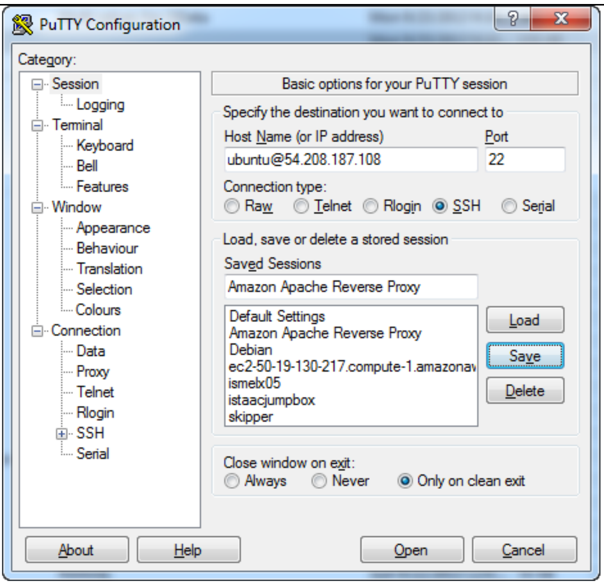
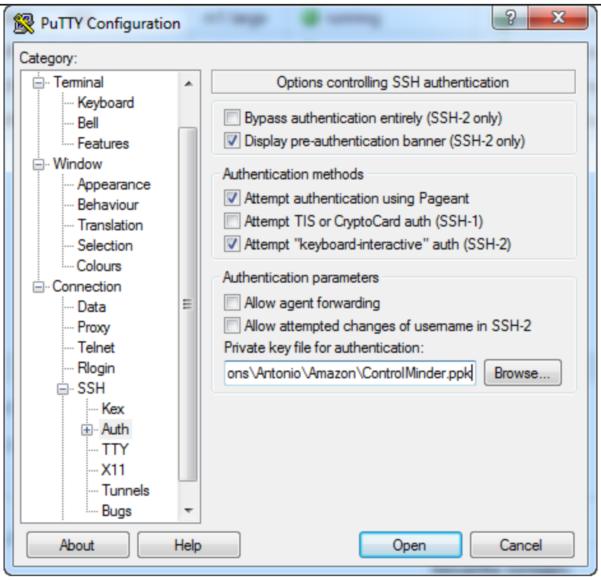
Add another Tag. (Maximum of 10)

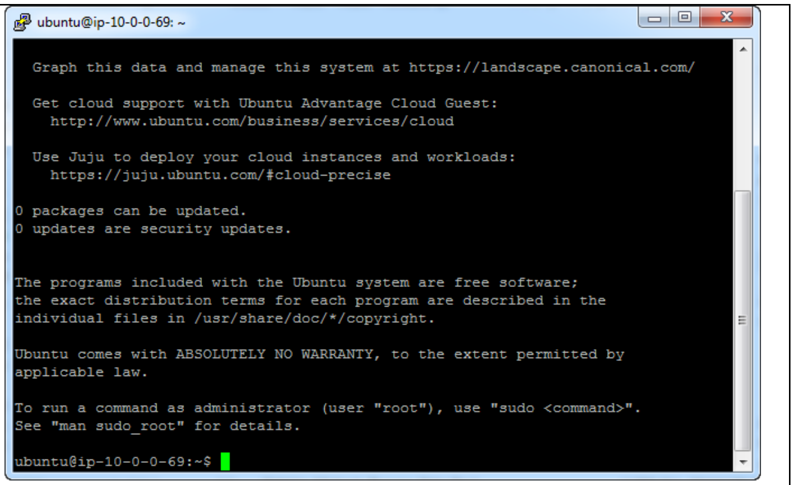
Use the key pair associated you're your AWS ECS Account. Click the Continue button.	 **Request Instances Wizard** Cancel ☒ CHOOSE AN AMI INSTANCE DETAILS CREATE KEY PAIR CONFIGURE FIREWALL REVIEW Public/private key pairs allow you to securely connect to your instance after it launches. For Windows Server instances, a Key Pair is required to set and deliver a secure encrypted password. For Linux server instances, a key pair allows you to SSH into your instance. To create a key pair, enter a name and click **Create & Download Your Key Pair**. You will be prompted to save the private key to your computer. Note: You only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance. ● Choose from your existing Key Pairs **Your existing Key Pairs***: ControlMinder ○ Create a new Key Pair ○ Proceed without a Key Pair
Add Default_Public and RDP_SSH and Web_Access security group to this instance	
Click 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:** Ubuntu Cloud Guest AMI ID ami-d0f89fb9 (x86_64) **Name:** Ubuntu Server 12.04.2 LTS **Description:** Ubuntu Server 12.04.2 LTS with support available from Canonical (http://www.ubuntu.com/cloud/services). **Number of Instances:** 1 **VPC ID:** vpc-a117ebc0 **VPC Subnet:** subnet-aa17ebcb (10.0.0.0/24) **Availability Zone:** us-east-1a **Instance Type:** M1 Medium (m1.medium) **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:** Yes **User Data:** Apache Reverse Proxy

Click the Close button.	 **Launch Instance Wizard** ☑ **Your instances are now launching.** Instance ID(s): i-1ce45878 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. **You can perform the following tasks while your instances are launching:** › Create Status Check Alarms You can use status check alarms to be notified if these instances fail status checks (additional charges may apply). › Create EBS Volumes (Additional charges may apply.) › View your instances on the Instances page Note: To view the VPC ID and Subnet ID columns on the Instances page click the **Show/Hide** button and check the corresponding boxes.

Connect to the Apache Reverse Proxy Server

Start a Remote Desktop session to the JumpBox Server logging in as Administrator.	Follow instructions already described.
Download PuTTy the JumpBox Server	
Install PuTTy on the JumpBox Server	Specific instructions are not provided since this is a straight forward installation.
The following steps describe how to convert your AWS ECS account certificate to a certificate that can be used by PuTTy to login to your Ubuntu instances. You will convert the ControlMinder.PEM Key Pair into the PPK format used by PuTTy. Run PuTTYKeyGen. From the Conversions menu item, choose Import Key.	 PuTTY Key Generator File Key Conversions Help Import key Export OpenSSH key Export ssh.com key Key No key. Actions Generate a public/private key pair Generate Load an existing private key file Load Save the generated key Save public key Save private key Parameters Type of key to generate: ○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA Number of bits in a generated key: 1024
Make your AWS ECS account certificate available. In the examples throughout this document, the key pair file is named ControlMinder.pem. Choose the ControlMinder.pem key pair file to import. Create and confirm a key passphrase. Remember this passphrase because you must provide it each time you login to the Apache Reverse Proxy Server. Click the <u>Save private key</u> button and the file as ControlMinder.ppk.	 PuTTY Key Generator File Key Conversions Help Key Actions Generate a public/private key pair Generate Load an existing private key file Load Save the generated key Save public key Save private key Parameters Public key for pasting into OpenSSH authorized_keys file: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC2ljwrTXb7uJu9xadfWESyjq1FXTSypbeiKgToo RWMGmKOOBaQ5IRIZJKiU4gZP8U +qse2NNgoseXgGF2Xv8xHUYoxArfsQXomA8LGnWee3rmcOucyGWHAiKxglu2swrYVFIYXO ORRbRflWpBUiVVtDkp8AICAnoKC3/E6W4j8usgE0DGEHJukpToz3uS4gchlqCcFrsQpeAPA Key fingerprint: ssh-rsa 2048 23:b8:dd:b4:d7:86:c4:9d:49:d3:9f:91:c2:92:57:d6 Key comment: ControlMInder AWS Key Key passphrase: •••••••••• Confirm passphrase: •••••••••• Type of key to generate: ○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA Number of bits in a generated key: 1024

Run PuTTY. Set Host Name to: ubuntu@<apache host name> where <apache host name> is either the hostname or the IP address of the Apache Reverse Proxy Server. The JumpBox must be able to resolve the hostname if hostname is used. Under Saved Sessions, name the session Amazon Apache Reverse Proxy. Click the Save button to save the session.	 PuTTY Configuration Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address): ubuntu@54.208.187.108 Port: 22 Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial Load, save or delete a stored session Saved Sessions: Amazon Apache Reverse Proxy Default Settings Amazon Apache Reverse Proxy Debian ec2-50-19-130-217.compute-1.amazonav ismelx05 istaacjumpbox skipper Close window on exit: ○ Always ○ Never ● Only on clean exit Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial Load Save Delete About Help Open Cancel
Under Category, select Connection → SSH → Auth Specify the path to ControlMinder.ppk in Private key file for authentication Under Category, select Session and save the session again. Click the Open button.	 PuTTY Configuration Options controlling SSH authentication ☐ Bypass authentication entirely (SSH-2 only) ☑ Display pre-authentication banner (SSH-2 only) Authentication methods ☑ Attempt authentication using Pageant ☐ Attempt TIS or CryptoCard auth (SSH-1) ☑ Attempt "keyboard-interactive" auth (SSH-2) Authentication parameters ☐ Allow agent forwarding ☐ Allow attempted changes of username in SSH-2 Private key file for authentication: ons\Antonio\Amazon\ControlMinder.ppk Category: Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Kex Auth TTY X11 Tunnels Bugs Browse... About Help Open Cancel

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.	

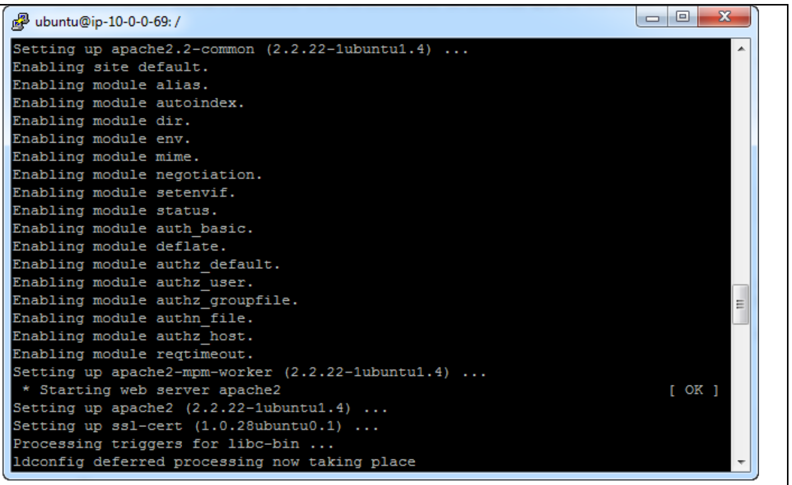
```
  Graph this data and manage this system at https://landscape.canonical.com/

  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

Install Apache Reverse Proxy Server.

Execute the following commands:

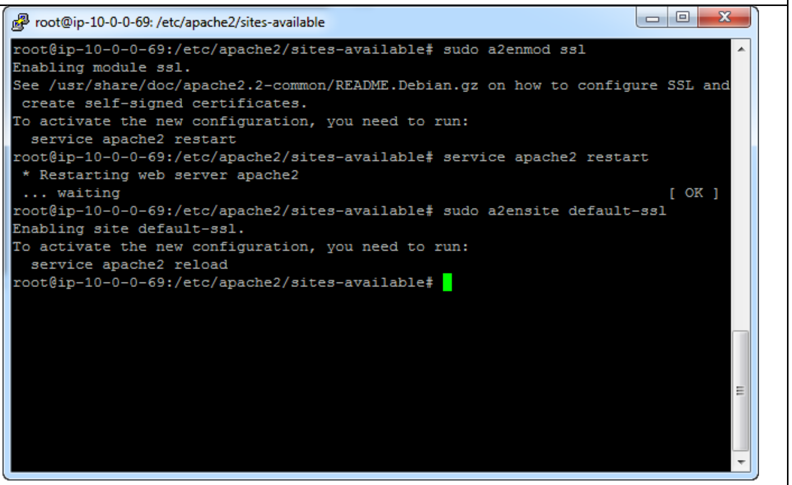
- sudo apt-get update
- sudo apt-get install apache2



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

Enable SSL by running:

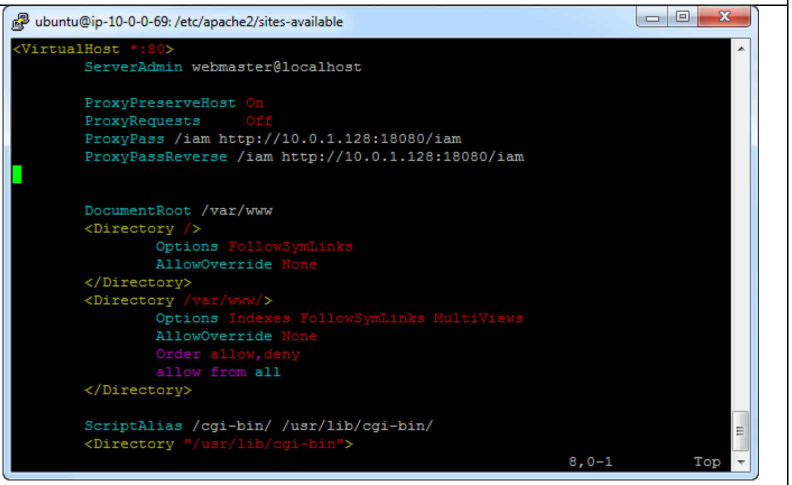
- sudo a2enmod ssl
- sudo a2ensite default-ssl



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

Run the following commands to enable Reverse Proxy:

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



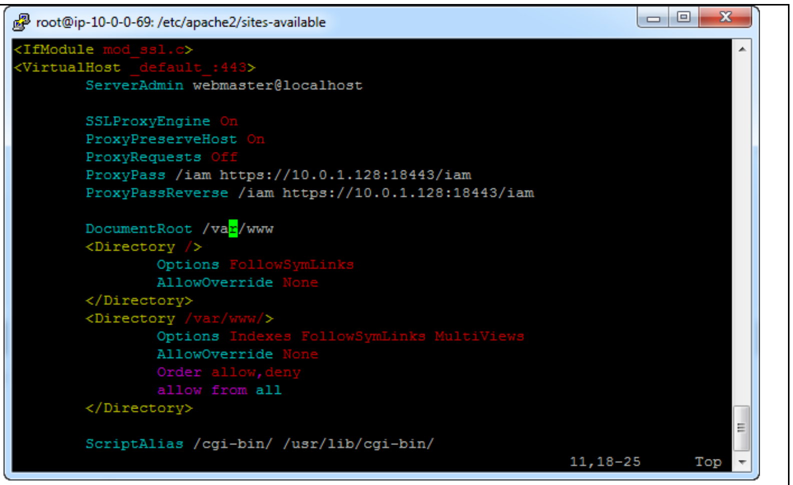
```
<VirtualHost *:80>
        ServerAdmin webmaster@localhost

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


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

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

Modify the reverse proxy settings:

sudo vi /etc/apache2/sites-available/default

Add the following lines:

ProxyPreserveHost On
ProxyRequests Off
ProxyPass / http://<ENTM private IP>:18080/iam
ProxyPassReverse / http://<ENTM Private IP>:18080/iam



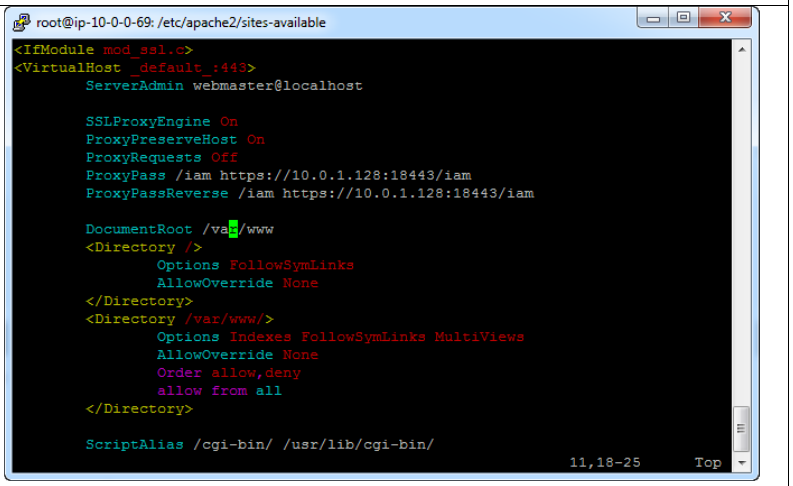
root@ip-10-0-0-69: /etc/apache2/sites-available

```
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
        ServerAdmin webmaster@localhost

        SSLProxyEngine On
        ProxyPreserveHost On
        ProxyRequests Off
        ProxyPass /iam https://10.0.1.128:18443/iam
        ProxyPassReverse /iam https://10.0.1.128:18443/iam

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

        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
                                                  11,18-25      Top
```

sudo vi /etc/apache2/sites-available/default-ssl

Add the following lines:

SSLProxyEngine On
ProxyPreserveHost On
ProxyRequests Off
ProxyPass / https://<ENTM private IP>:18443/iam
ProxyPassReverse / https://<ENTM Private IP>:18443/iam



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

```
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
        ServerAdmin webmaster@localhost

        SSLProxyEngine On
        ProxyPreserveHost On
        ProxyRequests Off
        ProxyPass /iam https://10.0.1.128:18443/iam
        ProxyPassReverse /iam https://10.0.1.128:18443/iam

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

        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
                                                  11,18-25      Top
```

Execute the following command to restart Apache:

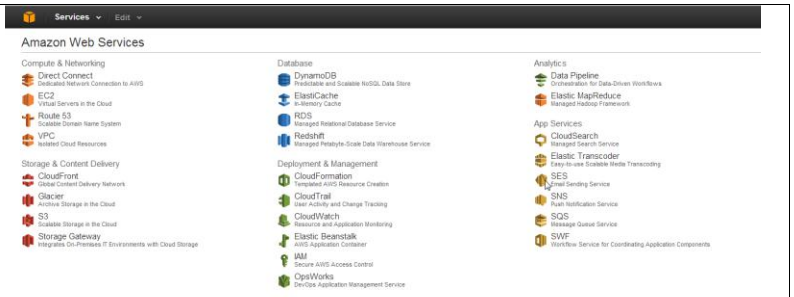
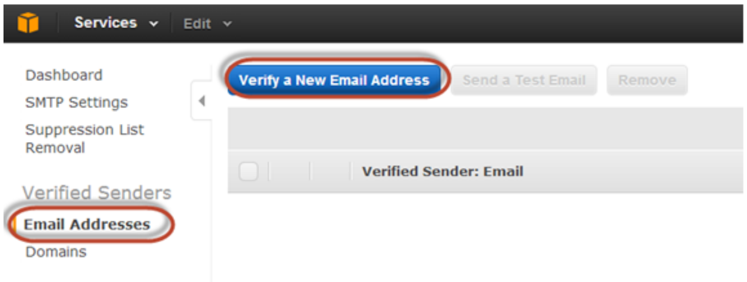
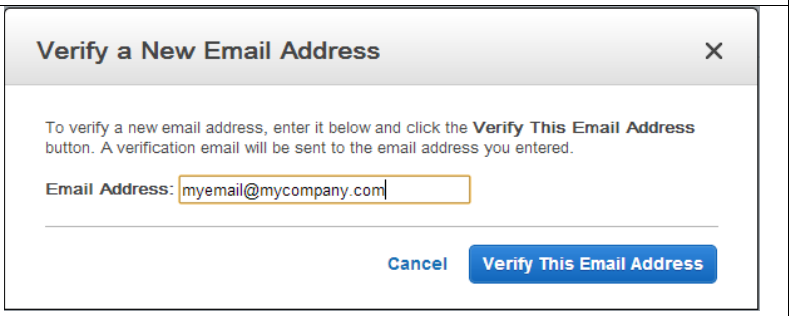
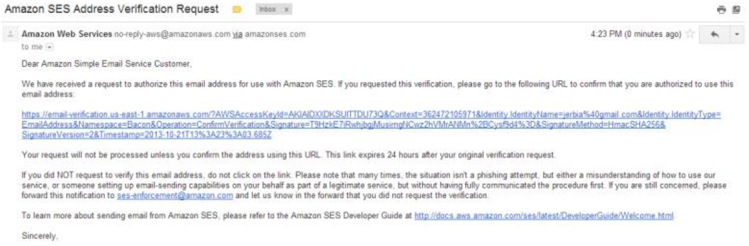
- service apache2 restart

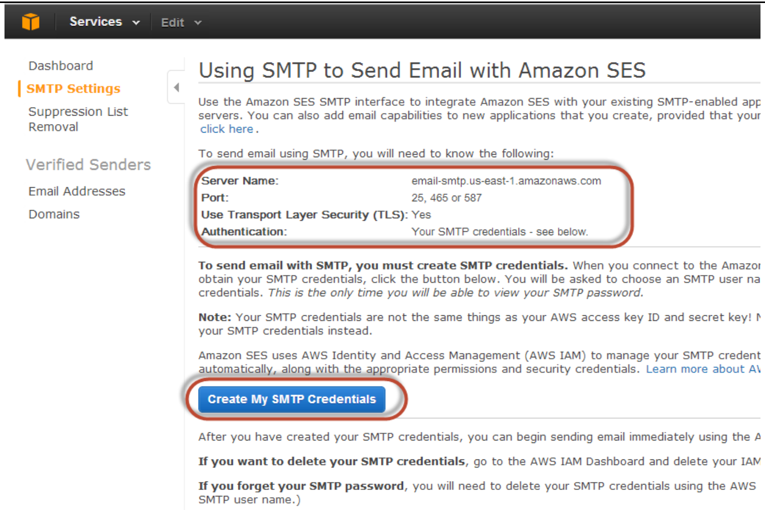
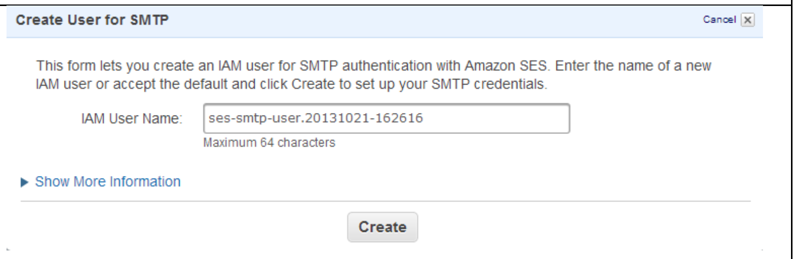
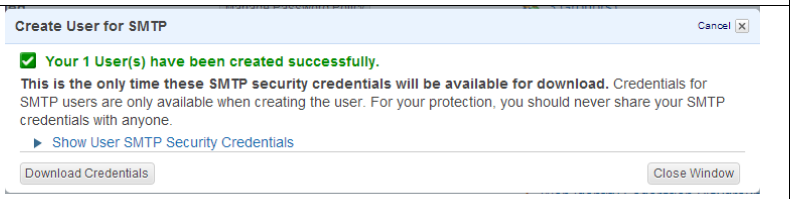
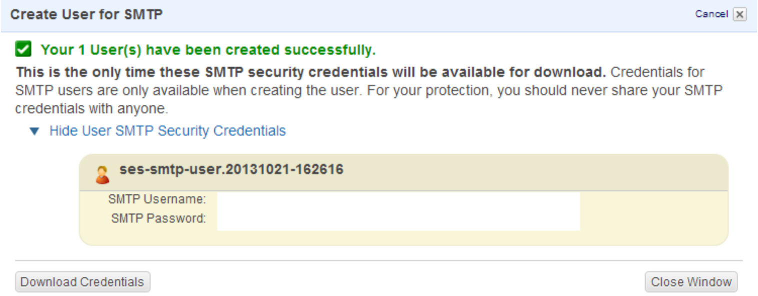
Appendix B - Setup email notification using Amazon SES

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

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

Create E-Mail Sandbox

Go to Amazon AWS console. Choose the SES Service to enable Amazon Email Service.	 Services Edit Amazon Web Services Compute & Networking Direct Connect Dedicated Network Connection to AWS EC2 Virtual Servers in the Cloud Route 53 Scalable Domain Name System VPC Isolated Cloud Resources Storage & Content Delivery CloudFront Global Content Delivery Network Glacier Archive Storage in the Cloud S3 Scalable Storage in the Cloud Storage Gateway Integrates On-Premises IT Environments with Cloud Storage Database DynamoDB Predictable and Scalable NoSQL Data Store ElastiCache In-Memory Cache RDS Managed Relational Database Service Redshift Managed Petabyte-Scale Data Warehouse Service Deployment & Management CloudFormation Templated AWS Resource Creation CloudTrail User Activity and Change Tracking CloudWatch Resource and Application Monitoring Elastic Beanstalk AWS Application Container IAM Secure AWS Access Control OpsWorks DevOps Application Management Service Analytics Data Pipeline Orchestration for Data-Driven Workflows Elastic MapReduce Managed Hadoop Framework App Services CloudSearch Managed Search Service Elastic Transcoder Easy-to-use Scalable Media Transcoding SES Email Sending Service SNS Push Notification Service SQS Message Queue Service SWF Workflow Service for Coordinating Application Components
You must register the email address of each sender and each recipient when using "sandbox" access. Click the Email Addresses button. Click the Verify a New Email Address button.	 Services Edit Dashboard SMTP Settings Suppression List Removal Verified Senders Email Addresses Domains Verify a New Email Address Send a Test Email Remove Verified Sender: Email
Specify the email address you will be using.	 Verify a New Email Address To verify a new email address, enter it below and click the **Verify This Email Address** button. A verification email will be sent to the email address you entered. **Email Address:** myemail@mycompany.com
A verification email is sent to the email address. The recipient must click on the link within this email.	 Amazon SES Address Verification Request **Amazon Web Services** no-reply-aws@amazonaws.com via amazonses.com to me 4:23 PM (0 minutes ago) Dear Amazon Simple Email Service Customer, We have received a request to authorize this email address for use with Amazon SES. If you requested this verification, please go to the following URL to confirm that you are authorized to use this email address: https://email-verification.us-east-1.amazonaws.com/?AWSAccessKeyId=AKIAIDXXDKSUITTDU73Q&Context=362472105971&Identity.IdentityName=jerbia%40gmail.com&Identity.IdentityType=EmailAddress&Namespace=Bacon&Operation=ConfirmVerification&Signature=T9HzkE7iRwhjbgjMusimgNCwz2hVMrANMn%2BCysf9d4%3D&SignatureMethod=HmacSHA256&SignatureVersion=2&Timestamp=2013-10-21T13%3A23%3A03.685Z Your request will not be processed unless you confirm the address using this URL. This link expires 24 hours after your original verification request. If you did NOT request to verify this email address, do not click on the link. Please note that many times, the situation isn't a phishing attempt, but either a misunderstanding of how to use our service, or someone setting up email-sending capabilities on your behalf as part of a legitimate service, but without having fully communicated the procedure first. If you are still concerned, please forward this notification to ses-enforcement@amazon.com and let us know in the forward that you did not request the verification. To learn more about sending email from Amazon SES, please refer to the Amazon SES Developer Guide at http://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html. Sincerely,

Capture the SMTP settings from the SMTP Settings menu. Click the Create My SMTP Credentials button.	 Services Edit Dashboard SMTP Settings Suppression List Removal Verified Senders Email Addresses Domains Using SMTP to Send Email with Amazon SES Use the Amazon SES SMTP interface to integrate Amazon SES with your existing SMTP-enabled app servers. You can also add email capabilities to new applications that you create, provided that your click here. To send email using SMTP, you will need to know the following: **Server Name:** email-smtp.us-east-1.amazonaws.com **Port:** 25, 465 or 587 **Use Transport Layer Security (TLS):** Yes **Authentication:** Your SMTP credentials - see below. **To send email with SMTP, you must create SMTP credentials.** When you connect to the Amazor obtain your SMTP credentials, click the button below. You will be asked to choose an SMTP user na credentials. *This is the only time you will be able to view your SMTP password.* **Note:** Your SMTP credentials are not the same things as your AWS access key ID and secret key! N your SMTP credentials instead. Amazon SES uses AWS Identity and Access Management (AWS IAM) to manage your SMTP credent automatically, along with the appropriate permissions and security credentials. Learn more about A\ Create My SMTP Credentials After you have created your SMTP credentials, you can begin sending email immediately using the A **If you want to delete your SMTP credentials**, go to the AWS IAM Dashboard and delete your IAM **If you forget your SMTP password**, you will need to delete your SMTP credentials using the AWS SMTP user name.)
Specify a user name or accept the default. Click the Create button.	 **Create User for SMTP** Cancel ☒ This form lets you create an IAM user for SMTP authentication with Amazon SES. Enter the name of a new IAM user or accept the default and click Create to set up your SMTP credentials. IAM User Name: ses-smtp-user.20131021-162616 Maximum 64 characters ▸ Show More Information Create
Click on the Show Security Credentials.	 **Create User for SMTP** Cancel ☒ ☑ **Your 1 User(s) have been created successfully.** **This is the only time these SMTP security credentials will be available for download.** Credentials for SMTP users are only available when creating the user. For your protection, you should never share your SMTP credentials with anyone. ▸ Show User SMTP Security Credentials Download Credentials Close Window
Copy the SMTP user name and password	 **Create User for SMTP** Cancel ☒ ☑ **Your 1 User(s) have been created successfully.** **This is the only time these SMTP security credentials will be available for download.** Credentials for SMTP users are only available when creating the user. For your protection, you should never share your SMTP credentials with anyone. ▾ Hide User SMTP Security Credentials **ses-smtp-user.20131021-162616** SMTP Username: SMTP Password: Download Credentials Close Window

Configure Email Workflow Notification

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

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

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

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

The two most common events of interest include:

BreakGlassCheckOutAccountEvent

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

CreatePrivilegedAccountExceptionNotStartedEvent

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

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

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

To configure email notification settings follow these steps:

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

Stop the JBoss service from the Services panel.

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

<JBoss_HOME>/server/default/deploy

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

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

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

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

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

Locate the following entry in the file:

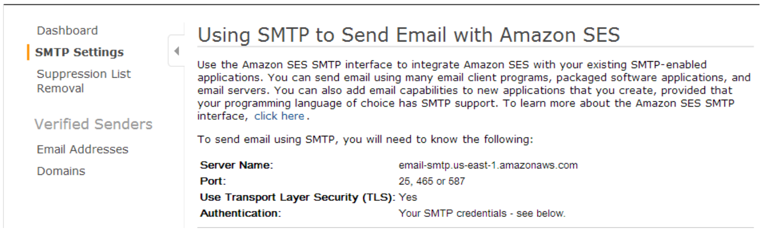
```
<property name="mail.smtp.host" value="smtp.nosuchhost.nosuchdomain.com"/>
```

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

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

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

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



Using SMTP to Send Email with Amazon SES

Use the Amazon SES SMTP interface to integrate Amazon SES with your existing SMTP-enabled applications. You can send email using many email client programs, packaged software applications, and email servers. You can also add email capabilities to new applications that you create, provided that your programming language of choice has SMTP support. To learn more about the Amazon SES SMTP interface, click here.

To send email using SMTP, you will need to know the following:

Server Name:	email-smtp.us-east-1.amazonaws.com
Port:	25, 465 or 587
Use Transport Layer Security (TLS):	Yes
Authentication:	Your SMTP credentials - see below.

Update the smtp port if required.

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

Save the changes.

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

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

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

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

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

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

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

Repeat the above process for the following template:

BreakGlassCheckOutAccountEvent.tmpl found in the directory:

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

Ensure that the files are saved.

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

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

Edit the following entry:

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

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

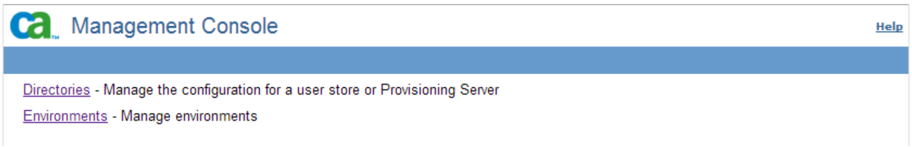
```
admin.email.address= cmadmin@mydomain.com
```

Start JBoss.

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

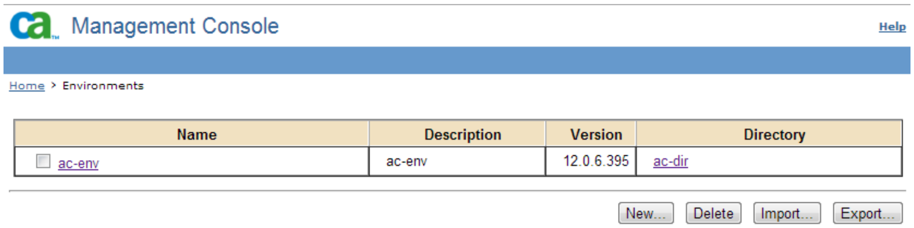
Open the IdentityMinder Management Console by browsing to the following link: https://localhost:18443/idmmanage

In the CA IdentityMinder^{TM} Management Console, click Environments.



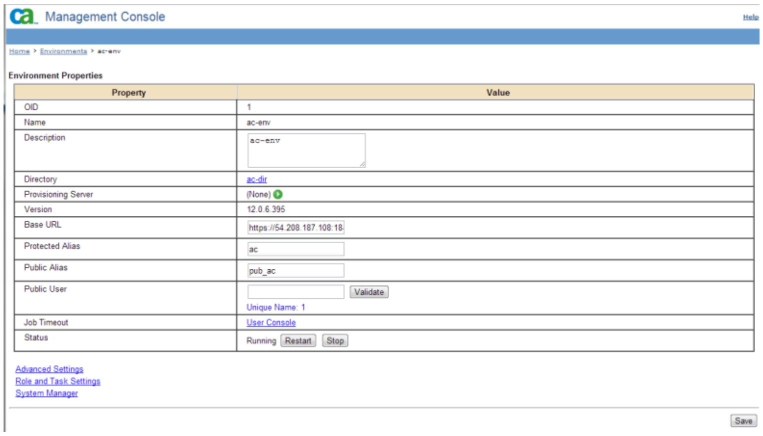
Directories - Manage the configuration for a user store or Provisioning Server
Environments - Manage environments

Select ac-env.



Name	Description	Version	Directory
□ ac-env	ac-env	12.0.6.395	ac-dir

Select Advanced Settings.



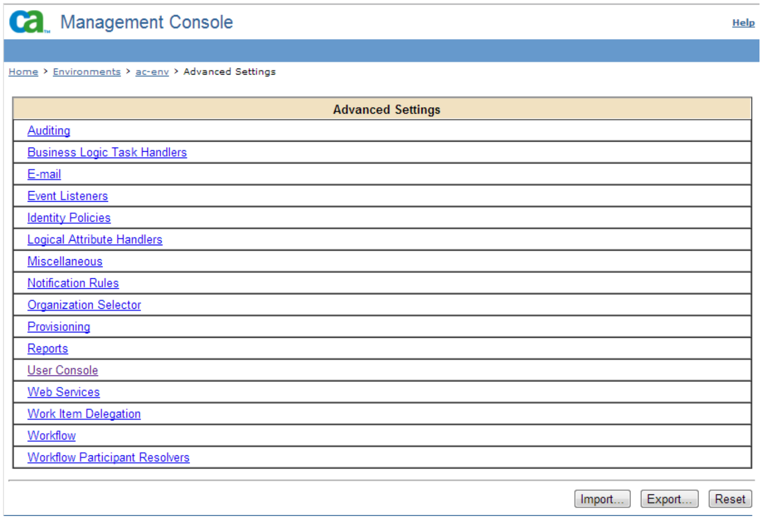
Home > Environments > ac-env

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	Validate Unique Name: 1
Job Timeout	User Console
Status	Running Restart Stop

Advanced Settings
Role and Task Settings
System Manager

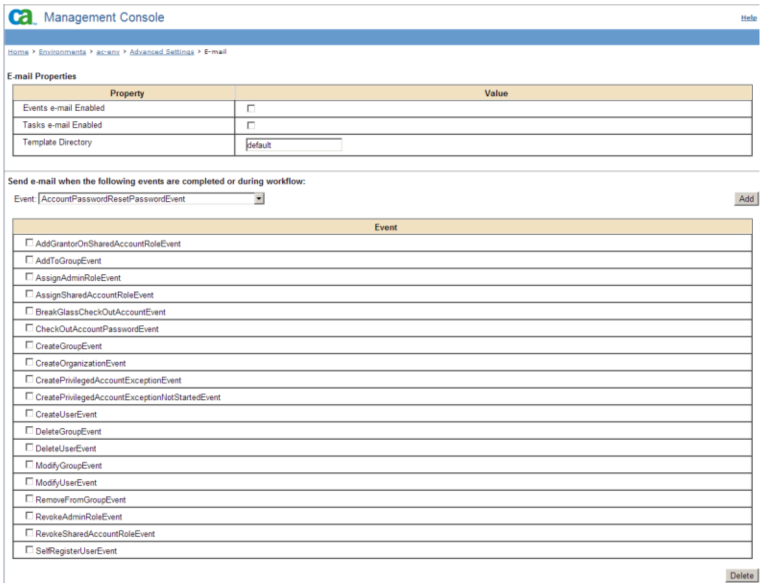
Select E-mail.



Home > Environments > ac-env > Advanced Settings

Advanced Settings
Auditing
Business Logic Task Handlers
E-mail
Event Listeners
Identity Policies
Logical Attribute Handlers
Miscellaneous
Notification Rules
Organization Selector
Provisioning
Reports
User Console
Web Services
Work Item Delegation
Workflow
Workflow Participant Resolvers

The E-mail Properties window appears.



E-mail Properties

Property	Value
Events e-mail Enabled	□
Tasks e-mail Enabled	□
Template Directory	default

Send e-mail when the following events are completed or during workflow:

Event: AccountPasswordResetPasswordEvent

Event
□ AddGrantorOnSharedAccountRoleEvent
□ AddToGroupEvent
□ AssignAdminRoleEvent
□ AssignSharedAccountRoleEvent
□ BreakGlassCheckOutAccountEvent
□ CheckOutAccountPasswordEvent
□ CreateGroupEvent
□ CreateOrganizationEvent
□ CreatePrivilegedAccountExceptionEvent
□ CreatePrivilegedAccountExceptionNotStartedEvent
□ CreateUserEvent
□ DeleteGroupEvent
□ DeleteUserEvent
□ ModifyGroupEvent
□ ModifyUserEvent
□ RemoveFromGroupEvent
□ RevokeAdminRoleEvent
□ RevokeSharedAccountRoleEvent
□ SelfRegisterUserEvent

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

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

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

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

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

Specify the events for which to send email notifications.

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

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

- BreakGlassCheckOutAccountEvent
- CreatePrivilegedAccountExceptionNotStartedEvent

Click Delete.

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

All other notifications are deleted.

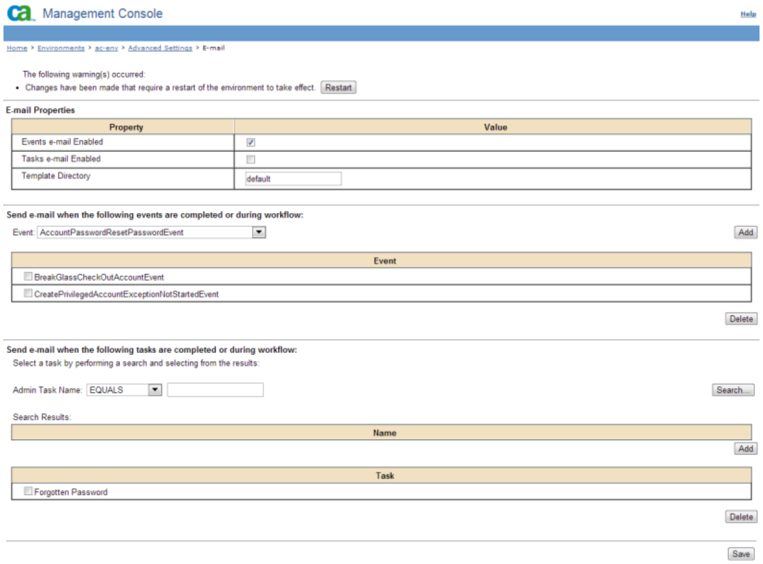
You have configured CA ControlMinder Enterprise Management to send email notifications for the selected SAM events.

Click Save.

The email notification properties are saved.

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

Click the Restart button.



The following warning(s) occurred:

- Changes have been made that require a restart of the environment to take effect. Restart

E-mail Properties

Property	Value
Events e-mail Enabled	☑
Tasks e-mail Enabled	□
Template Directory	default

Send e-mail when the following events are completed or during workflow:

Event: AccountPasswordResetPasswordEvent ▾ Add

Event
□ BreakGlassCheckOutAccountEvent
□ CreatePrivilegedAccountExceptionNotStartedEvent

Delete

Send e-mail when the following tasks are completed or during workflow:

Select a task by performing a search and selecting from the results:

Admin Task Name: EQUALS ▾ Search...

Search Results:

Name

Add

Task
□ Forgotten Password

Delete

Save

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

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