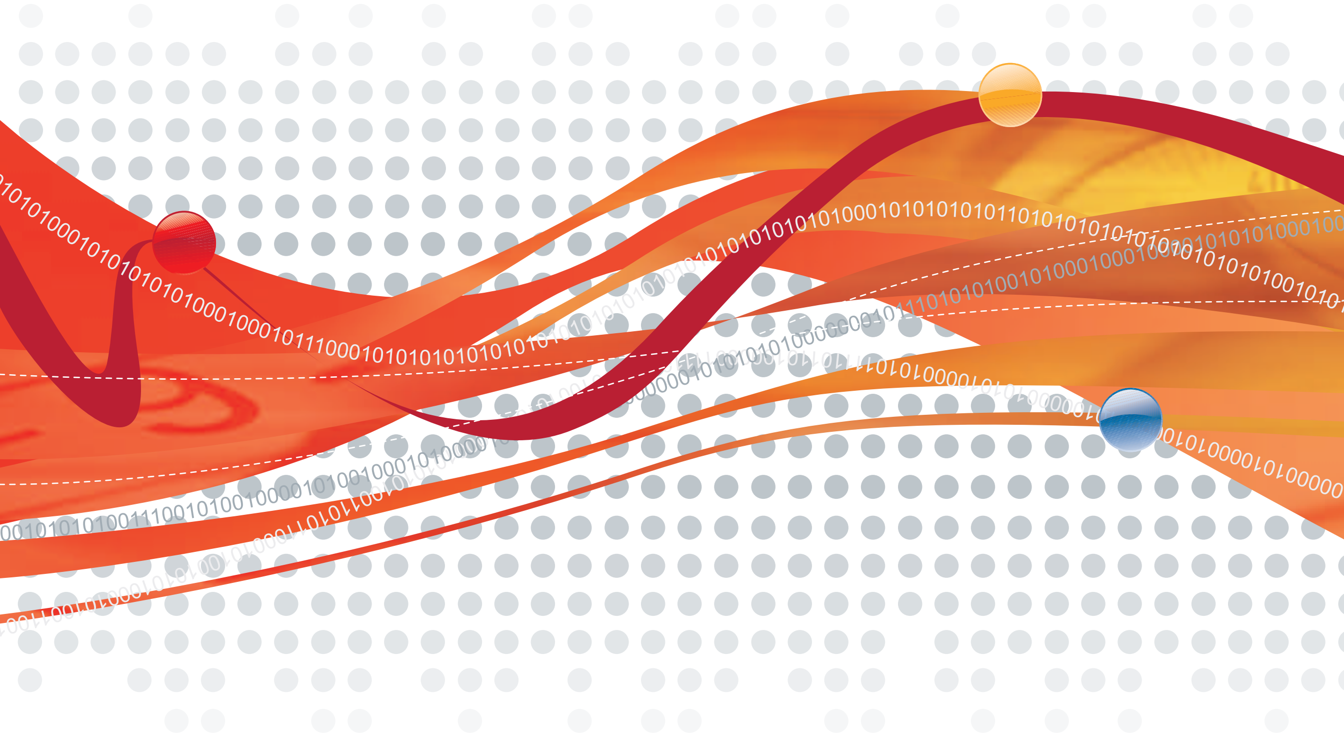
TREND MICRO™

SecureCloud™

Private Security for the Public Cloud

Administrator's Guide



Protected Cloud

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme. This document and SecureCloud are released pursuant to NDA Only and is confidential.

Document Part No. APEM04403/100227

Release Date: October, 2010

The user documentation for Trend Micro SecureCloud is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

To contact Trend Micro Support, please see Appendix C, *Contact Information and Web-based Resources* of this document.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Contents

Preface

Chapter 1: Introducing SecureCloud

Chapter 2: Using SecureCloud

Chapter 3: Understanding Running Instance Information

Chapter 4: Managing Policies

Chapter 5: Machine Image and Data Storage Device Information

Chapter 6: Reports and Logs

Chapter 7: Administration

Chapter 8: Provisioning for Data Storage Encryption

Appendix A: Installing and Uninstalling the SecureCloud Runtime Agent

Appendix B: Frequently Asked Questions

Appendix C: Contact Information and Web-based Resources

Appendix D: Basic Troubleshooting Information

Glossary

Index

Preface

Preface

Welcome to the *Trend Micro™ SecureCloud™ Administrator's Guide* for the 1.0 release of SecureCloud. This guide provides detailed information about configuring and using SecureCloud. Topics include how to add users, devices, and machine images and how to approve or deny a key request.

This preface describes the following:

- *SecureCloud Documentation*
- *Audience*
- *Document Conventions*

SecureCloud Documentation

In addition to the *Trend Micro™ SecureCloud Administrator's Guide*, the documentation set includes the following:

- **Online Help**—The purpose of online help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online Help is accessible from the SecureCloud Web console.
- **Readme file**—This file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and, release history.

  The latest versions of the Administrator's Guide and readme file are available in electronic form at:

  `http://www.trendmicro.com/download/`

Audience

The SecureCloud documentation is written for IT managers and system administrators working in a medium or large enterprise environment. The documentation assumes that the reader has in-depth knowledge of networks schemas, including details related to the following:

- Amazon EC2
- Eucalyptus
- VMware vCloud
- Hosted services
- Linux / CentOS
- Microsoft Windows Server
- Virtual machines

The documentation does not assume the reader has any knowledge of antivirus or malware technology.

Document Conventions

To help you locate and interpret information easily, the SecureCloud documentation uses the following conventions.

TABLE P-1. Document Conventions

CONVENTION	DESCRIPTION
LOCATION: Example: LOCATION: WEB CONSOLE MAIN MENU | POLICIES > POLICIES PAGE | ADD POLICY BUTTON > ADD POLICY PAGE	The path to the location where the action is being performed in SecureCloud. This includes screens and/or windows and any buttons and/or links that you need to click.
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

Chapter 1

Introducing SecureCloud

Trend Micro™ SecureCloud 1.0 is a Software as a Service (SaaS) release. SecureCloud provides security for public and private cloud infrastructures. Data is encrypted on a virtual machine before being written to storage and decrypted when read back. The keys for the encryption are stored off site and delivered when required. A manual or automatic approval process takes place before SecureCloud releases the keys. SecureCloud's unique identity and integrity policy-based key management allows it—with a degree of confidence—to ensure encryption keys are released only into safe cloud environments. This is achieved through numerous rules that help SecureCloud assess the cloud environment’s identity and integrity.

Topics in this chapter include:

- *System Requirements*
- *Features and Benefits*
- *How SecureCloud Works*

System Requirements

As a SaaS solution, there are only minimal requirements needed to run the SecureCloud Runtime Agent in your cloud service provider's environment.

Use one of the following browsers to access the SecureCloud Web console:

- Microsoft® Internet Explorer 7.0 or 8.0
- Mozilla Firefox 3.6

Note: In order for the browser to work properly with SecureCloud, JavaScript must be enabled.

Server Requirements for the Runtime Agent

TABLE 1-2. Runtime Agent Requirements for Various Operating Systems

Requirement	Description
Cloud provider	• Amazon EC2 • Eucalyptus 1.6 • Eucalyptus 2.0 • VMware vCloud
Instance type	• Amazon EC2: - Windows and 64-bit Linux: Small (m1.small, 1.7GB) - 32-bit Linux: Micro (t1.micro, 613MB) • Eucalyptus: Configure for the smallest size that accommodates your needs • VMware vCloud: Configure a virtual machine that accommodates your needs
CPU	One virtual-core processor
Memory	613MB
Hard disk space	• 30MB to install SecureCloud Runtime Agent • 440MB to install Eucalyptus Provisioning Server • 620MB to install vCloud Provisioning Server
Guest operating system	• CentOS 5.4 32-bit and 64-bit version • Windows 2003 R2 Data Center Edition 32-bit

Features and Benefits

The following are the main features of SecureCloud and their benefits.

Standard Protocols and Advanced Techniques for Securing Information

- Uses industry-standard AES encryption
- Encrypts and decrypts data in real time, so data at rest and data moving through the cloud infrastructure is always protected
- Applies whole-volume encryption to secure all data, metadata and associated structures without impacting application functionality

Access and Authentication Controls

- Employs role-based management to help ensure proper separation of duties

Robust Auditing, Reporting and Alerting

- Performs audit logging for all agent, key, policy and user events
- Provides detailed reporting and alerting features for logged events. SecureCloud can issue several types of notifications in response to cloud security events. Administrator notifications are sent via email to the designated administrator contacts. User notifications are presented in the requesting client's browser. Both administrator and user notifications can be customized.

Policy-driven Key Management

- Utilizes identity- and integrity-based policy enforcement to ensure that only authorized virtual machines receive keys or access secure volumes
- Automates key release and virtual machine authorization for rapid operations or requires manual approval for increased security
- Delivers keys using SSL encrypted internet channels with an additional layer of encrypted communication
- Offers central key management as a hosted service within Trend Micro's secure data centers

How SecureCloud Works

SecureCloud provides a data encryption layer within a machine image to decrypt customer data in real-time after the appropriate credentials have been validated. Likewise, SecureCloud encrypts customer data in real-time when putting the information back into data storage.

When the machine image boots up, it uses the Runtime Agent to provide its credentials to SecureCloud and request an encryption and decryption key along with the appropriate information to connect to data storage. For example, a virtual machine image could provide such integrity information as pattern file version, last full scan, and location of the instance to SecureCloud during the request. The integrity and credential information helps to ensure that the instance meets the policy criteria set by the administrator in order to run certain applications.

SecureCloud provides and maintains your encryption keys. The virtual machine image does not store encryption or decryption keys. SecureCloud also provides other management capabilities such as limited reporting and auditing functions.

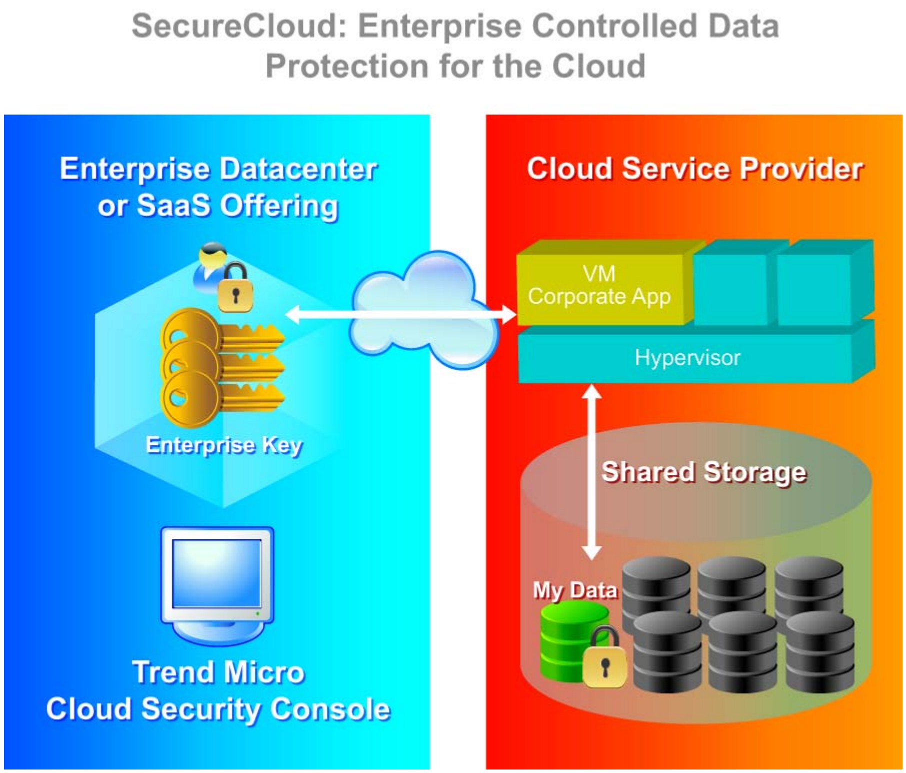

SecureCloud: Enterprise Controlled Data Protection for the Cloud
Enterprise Datacenter or SaaS Offering
Enterprise Key
Trend Micro Cloud Security Console
Cloud Service Provider
VM Corporate App
Hypervisor
Shared Storage
My Data

FIGURE 1-1. Overview of how SecureCloud functions

As a SaaS product, SecureCloud has a multi-tenant environment where multiple organizations are served. You access SecureCloud through a secure Internet connection. Using this portal, you define the criteria on which instances can receive encryption/decryption keys. For example, criteria can include the location of the application, host name, the latest OS patch, and/or the latest Trend Micro engine and pattern file. In addition, for this release you can get limited report and audit information about your account using the portal.

Basic Components of SecureCloud

The following are the basic components of SecureCloud:

Runtime Agent

The SecureCloud Runtime Agent is the software module that is installed with your virtual machine image in your cloud service provider's environment. The Runtime Agent is compatible with CentOS 5.4 and Windows Server 2003 R2 DataCenter Edition. The SecureCloud Runtime Agent provides limited integrity check functionality such as IP address and location. The Runtime Agent uses AES-128 as the encryption and decryption standard.

The Configuration Tool is part of the SecureCloud Runtime Agent. After product installation, you can launch the Configuration Tool from the installation wizard. If you decline to run the Configuration Tool at this time, you can launch it later.

The Configuration Tool configures the following:

- Cloud service provider's credentials
- SecureCloud account ID
- Device information for the running machine instance

Management Server

Trend Micro hosts the SecureCloud Management Server with multi-tenant capability. There is no enterprise console option for the SaaS version of the product. The Management Server hosts the key approval process, log collection and reporting.

The SecureCloud Web console is the Graphical User Interface (GUI) front end to the Management Server. Your interaction with the SecureCloud Web console is based on role-based administration and privilege levels. The Management Server allows for multiple users, having varying user roles (see *User Role Management* on page 7-3).

Provisioning Service

The Provisioning Service is a Web-based, virtual appliance that runs within your cloud service provider. It connects to SecureCloud and keeps the application aware of active devices in the cloud service provider. From the SecureCloud Web console, you implement an instance of the Provisioning Server to encrypt any available devices, which are then registered with the SecureCloud Management Server automatically.

Chapter 2

Using SecureCloud

Topics in this chapter include the following:

- *Registering the SecureCloud Product*
- *Using the SecureCloud Web Console*
- *Summary of Operations*

Registering the SecureCloud Product

Before you can use SecureCloud, you must create and register a user account with Trend Micro. If you are a Managed Service Provider (MSP), you can register multiple accounts on behalf of your customers.

Procedure:

1. Go to `https://console.securecloud.com/`
2. From the Log On page, click the **Click here** link.
3. From the Registration page, enter all the necessary information.

   The password must be 8 to 32 characters, containing at least one of each of the following:

   - Upper-case character
   - Lower-case character
   - Numeral
   - Special character (~!@#$%^&*()_+)

   The **Minimum password criteria validation** indicator rates the strength of your password based on the variety of characters used.
4. Click **Continue**.

   An email is sent to you, using the email address that you specified. This email contains a link to complete the product-registration process.
5. In the email, click the link to complete the product-registration process.
6. Return to the Log On page and complete the fields and then click **Log on**.

   If you forget your password, see *How do I Recover a Forgotten Web Console Password?* on page B-5.

Using the SecureCloud Web Console

SecureCloud consists of a main menu with a viewing area to the right of this menu. The main menu is comprised of the Running Instances, Policies, Inventory, Reports, Logs, and Administration menu items. The Inventory menu item consist of submenus for viewing or editing existing images and adding devices and changing existing device information. The Administration menu consists of submenus for managing notifications, users, roles, and the password and product license.

The amount of functionality available to a user in SecureCloud is based on user roles. The possible user roles are administrator, data analyst, auditor, and key approver, with administrator having the most privileges and data analyst having the least. See *User Role Management* on page 7-3 for complete details.

Use the following URL to open the SecureCloud Web console:

```
https://console.securecloud.com/
```

Summary of Operations

Beginning with the cloud service provider, the following are the basic steps necessary to initiate a cloud service and launch the SecureCloud product.

Step 1. Register your SecureCloud product with Trend Micro.

Product registration is done at log on. If you are a MSP, you are able to register multiple accounts on behalf of your customers at this time.

See *Registering the SecureCloud Product* on page 2-2.

Step 2. Create a data storage device.

You create a data storage device within your cloud service provider. You can either create a new device or clone an existing one. Once this is done, the new device is available for encryption from the SecureCloud Web console.

See *Creating a Data Storage Device in Your Cloud Service Provider Environment* on page 8-2 and your cloud service provider documentation for details.

Attention: *For the vCloud cloud environment, steps 3 and 4 are combined.*

Step 3. Encrypt and register the data storage device with SecureCloud.

This is done by the Provisioning Service. From the SecureCloud Web console, the application uses the Provisioning Service to encrypt and register selected data storage devices using the device key issued from SecureCloud Management Server. Once this process is complete, machine images registered with the SecureCloud Management Server can access encrypted data.

Note: For the vCloud environment, you must create a user within your vCloud organization who has read-only access to the whole organization.

See Chapter 8, *Provisioning for Data Storage Encryption*.

Step 4. Prepare a machine image.

You create a machine image within your cloud service provider. The machine image contains your applications, which access your secured data. This data is stored in an encrypted data storage device that you attach and mount to an instance of the machine image.

Note: For the vCloud cloud environment, you need to add an additional data storage device for encryption. SecureCloud does not recognize or encrypt the first device.

See your cloud service provider documentation to create a machine image.

a. Install SecureCloud Runtime Agent in the machine image.

The Runtime Agent makes the Management Server functionalities available to you once you launch an instance of the machine image. This functionality is controlled from the SecureCloud Web console.

b. Register the machine image.

A machine image is registered with the command line-based SecureCloud Configuration Tool. You need to register the image with the Management Server in order to see the image in SecureCloud.

See *Registering a Machine Image* on page 5-2.

Note: The SecureCloud Configuration Tool is only used for machine images in the Amazon and Eucalyptus environments. For vCloud, the process of registering an image and provisioning a device is combined and happens when the user is prompted to reboot their machine image (see *Encrypting a New Data Storage Device* on page 8-6). Therefore, for vCloud there is no configuration utility and the user has no further interaction.

Ensure that the network configuration of your cloud service provider's environment enables communications between the virtual machine instances (vApps) running the SecureCloud agent or Provisioning Service are able to connect to the vCloud Director (vCD) web services using HTTP and HTTPS (see Appendix D, *Basic Troubleshooting Information*).

c. Bundle the machine image to be used as a template.

To bundle the machine image is to save the configured machine image as a template for creating instances or other machine images.

Note: For the vCloud environment, steps 4b and 4c are not necessary since image registration is automatic.

See your cloud service provider documentation to bundle the machine image.

Step 5. Create policies.

A policy is a record that identifies what machine images can access which data storage devices and under what conditions. Based on whether these conditions are met or not, you also specify how access will be granted or denied to the encrypted data storage device.

New machine images and data storage devices that are added will be assigned to the default policy if you have not yet created your own policy.

See *Creating a Policy* on page 4-3.

Step 6. Add users and assign them roles.

The role assigned to a user determines the level of functionality this person has in SecureCloud.

See *Adding a New User* on page 7-2 and *User Role Management* on page 7-3.

Step 7. Setup notification alerts.

SecureCloud can issue an email alerting you of various conditions surrounding a key request or if a device has not yet been assigned to a policy.

See *Creating a Notification* on page 7-4.

Step 8. Launch the instance

To use your applications under the protection of SecureCloud, launch an instance of the machine image hosting your applications and the SecureCloud Runtime Agent. Launching the instance invokes the Runtime Agent. The Runtime Agent requests data storage device access (an encryption key) from the SecureCloud Management Server. The Management Server then validates the request based on the conditions specified in the policy.

See your cloud service provider documentation to launch an instance. See *Viewing and Changing Data Storage Device Information* on page 5-6 for data storage device and instance status.

Step 9. Approve or deny any pending key request.

A key request with a "Pending" status requires you to manually approve or deny the request. A "Pending" status is given to a key request that was set for manual approval if it either met or failed to meet the rules specified in the policy.

See *Acting Upon a Pending Key* on page 3-4.

Step 10. Generate any desired reports.

To better help you manage SecureCloud, the application enables you to generate reports describing key requests, inventory items (instances, machine images, data storage devices), and audit information (who did what and when).

See *Reports* on page 6-2.

Step 11. Generate any desired logs.

SecureCloud logs all the system events. SecureCloud enables you to query logs based on a date range or log event types.

See *Logs* on page 6-3.

Note: To obtain trouble-shooting information regarding log-management issues, see Appendix D, *Basic Troubleshooting Information*.

Chapter 3

Understanding Running Instance Information

From the Running Instances page, you can view how many machine images are active and how many instances of each machine image are running. For each instance, you can learn what is the associated data storage device or devices, where the secure data is stored. SecureCloud enables you to group the information in the Running Instances page based on the filter criteria you specify in a drop-down list.

If the approval for a machine image to decrypt data on a device is pending, then you can manually grant this approval.

Finally, the Running Instances page provides the integrity status of the virtual machine images and the date when device access was requested (see *Figure 3-2*).

Note: If the Runtime Agent fails to send a "heartbeat" response to SecureCloud, the instance will be marked as missing and eventually removed from the Running Instances page.

Topics in this chapter include the following:

- *About Key Status and Virtual Machine Integrity*
- *Viewing and Changing Machine Image Information*
- *Viewing Instance and Related Information*

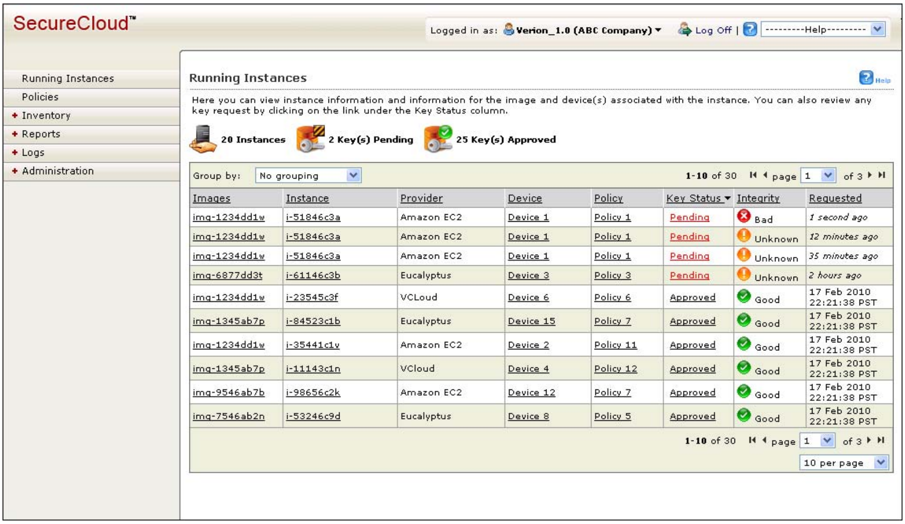
- *Acting Upon a Pending Key*

About Key Status and Virtual Machine Integrity

SecureCloud checks the version of OSSEC running to ensure that the instance meets the policy criteria set by the administrator in order to run certain applications.

From the Running Instances page, you can view the possible key statuses (see *Figure 3-2*):

- Pending
- Approved
- Delivered
- Denied



Running Instances

Here you can view instance information and information for the image and device(s) associated with the instance. You can also review any key request by clicking on the link under the Key Status column.

20 Instances 2 Key(s) Pending 25 Key(s) Approved

Group by: No grouping 1-10 of 30 page 1 of 3

Images	Instance	Provider	Device	Policy	Key Status	Integrity	Requested
img-1234dd1w	i-51846c3a	Amazon EC2	Device 1	Policy 1	Pending	Bad	*1 second ago*
img-1234dd1w	i-51846c3a	Amazon EC2	Device 1	Policy 1	Pending	Unknown	*12 minutes ago*
img-1234dd1w	i-51846c3a	Amazon EC2	Device 1	Policy 1	Pending	Unknown	*35 minutes ago*
img-6877dd3t	i-61146c3b	Eucalyptus	Device 3	Policy 3	Pending	Unknown	*2 hours ago*
img-1234dd1w	i-23545c3f	VCLoud	Device 6	Policy 6	Approved	Good	17 Feb 2010 22:21:38 PST
img-1345ab7p	i-84523c1b	Eucalyptus	Device 15	Policy 7	Approved	Good	17 Feb 2010 22:21:38 PST
img-1234dd1w	i-35441c1v	Amazon EC2	Device 2	Policy 11	Approved	Good	17 Feb 2010 22:21:38 PST
img-1345ab7p	i-11143c1n	VCloud	Device 4	Policy 12	Approved	Good	17 Feb 2010 22:21:38 PST
img-9546ab7b	i-98656c2k	Amazon EC2	Device 12	Policy 7	Approved	Good	17 Feb 2010 22:21:38 PST
img-7546ab2n	i-53246c9d	Eucalyptus	Device 8	Policy 5	Approved	Good	17 Feb 2010 22:21:38 PST

1-10 of 30 page 1 of 3

10 per page

FIGURE 3-1. Typical view of the Running Instances page

As indicated by the hyperlink, you can click on key status of "Pending", "Approved" and "Delivered" to view the key request information.

Clicking the desired "Pending" link from the "Status" column should open the Key Request window, unless the device and machine image are not assigned to the same policy. In this case, SecureCloud opens a window which prompts you to correct the situation.

The following are the possible integrity ratings that a virtual machine image can receive:

- Good
- Bad
- Unknown

  The Unknown rating means that a data storage device with a key request status of "Pending" or "Denied" is not yet associated with a machine image or is not yet in a policy.

Viewing and Changing Machine Image Information

For information beyond the machine image name and description, see *Changing Machine Image Information and Viewing Related Information* on page 5-4 to learn how the image relates to policies and instances.

Procedure:

LOCATION WEB CONSOLE MAIN MENU | RUNNING INSTANCES > RUNNING INSTANCES PAGE | DESIRED MACHINE IMAGE LINK > RUNNING INSTANCES - EDIT IMAGE PAGE

1. Use the appropriate fields to changes the machine image name and/or description.
2. Click **Save**.

Viewing Instance and Related Information

Procedure:

LOCATION WEB CONSOLE MAIN MENU | RUNNING INSTANCES > RUNNING INSTANCES PAGE

1. From the "Instances" column, click the desired instance link.

   From the "Device List" area of the Running Instances page, click the desired device link in the "Device ID" column to view device, policy, and device encryption information and specify certain device and policy information (see *Viewing and Changing Data Storage Device Information* on page 5-6 and *Creating a Policy* on page 4-3).

2. From the Running Instances page, click **Back**.

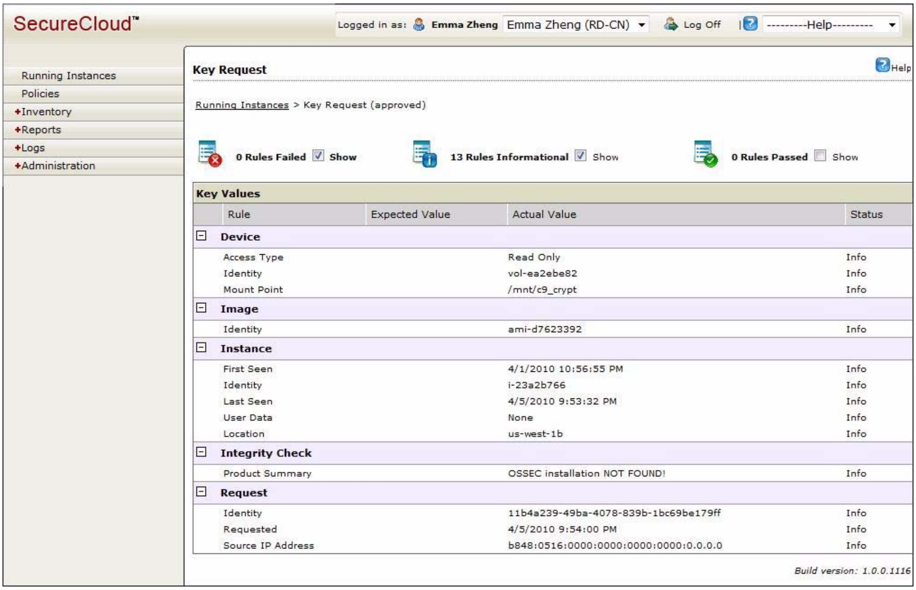
Acting Upon a Pending Key

A key with "Pending" status is a key that was set for manual approval if it either met or failed to meet the credentials defined by the policy. See *About Key Status and Virtual Machine Integrity* on page 3-2 to learn more about the "Pending" status.

Procedure:

LOCATION WEB CONSOLE MAIN MENU | RUNNING INSTANCES > RUNNING INSTANCES PAGE | DESIRED PENDING LINK > KEY REQUEST WINDOW

The Key Request window lists information by device, image, and instance. This window summarizes how many rules failed and passed and how many rules are informational. Rules Informational are the set of rules that a system administrator deems not necessary for key approval criteria, but they can provide useful information.



Key Request

Running Instances > Key Request (approved)

0 Rules Failed ☑ Show   13 Rules Informational ☑ Show   0 Rules Passed □ Show

Key Values

Rule	Expected Value	Actual Value	Status
⊟ **Device**			
Access Type		Read Only	Info
Identity		vol-ea2ebe82	Info
Mount Point		/mnt/c9_crypt	Info
⊟ **Image**			
Identity		ami-d7623392	Info
⊟ **Instance**			
First Seen		4/1/2010 10:56:55 PM	Info
Identity		i-23a2b766	Info
Last Seen		4/5/2010 9:53:32 PM	Info
User Data		None	Info
Location		us-west-1b	Info
⊟ **Integrity Check**			
Product Summary		OSSEC installation NOT FOUND!	Info
⊟ **Request**			
Identity		11b4a239-49ba-4078-839b-1bc69be179ff	Info
Requested		4/5/2010 9:54:00 PM	Info
Source IP Address		b848:0516:0000:0000:0000:0000:0.0.0.0	Info

Build version: 1.0.0.1116

FIGURE 3-2. Key request page

1. To filter by rules that failed, passed, or are simply informational, select the appropriate check box(es) at the top of the window.
2. Click **Approve** to approve the key request.

   SecureCloud changes the status of the key request from "Pending" to "Delivered". You can click on the "Delivered" status in the Running Instances page to view the key request information again.

   Once a key request has been approved and delivered, this cannot be reversed.

Chapter 4

Managing Policies

SecureCloud stores unallocated machine images and data storage devices in the default policy. This policy can be edited in the same way as all other policies can, except for the device and image lists.

Policies are managed from the Policies page. From here you can create a policy and then add machine images, devices, and rules to the policy. For the policy, you can also specify the rules for encryption key approval.

Likewise, for an existing policy you can change what machine images, devices, and rules are included in the policy. You can also change the conditions necessary for encryption key approval. Finally, you can delete a policy from the Policies page.

Topics in this chapter include the following:

- *About the Default Policy*
- *Creating a Policy*
- *Changing a Policy*
- *Deleting a Policy*
- *About the Default Policy*

About the Resource Pool

By enabling resource pooling in a policy, the Management Server is able to instruct the Runtime Agent as to which data storage device(s) it should use in the event the requested device is in use by another instance. See *Creating a Policy* on page 4-3 to enable resource pooling.

For each requested device that is already in use, the Management Server will select an unallocated device from the same resource pool (policy) as the originally requested device, and instruct the agent to use this.

If the machine image belongs to multiple policies, and one policy has resource pooling enabled and one does not, SecureCloud will return only a new device from the policy that has resource pooling enabled, in the non-resource pooled policy, the device key request may fail if the intended device is already in use.

Note: Resource pooling is not applicable for vCloud where devices cannot be dynamically attached to a running instance.

About the Default Policy

Images and devices that you add to the SecureCloud inventory are automatically placed in the default policy. From the Policies page, the default policy can be edited in the same way as all other policies can, except for the device and image lists. The default policy cannot be deleted. It uses the rule that checks for the presence of OSSEC 2.3 or higher on the instance, and has a default action of "manual approve" for key-request approval.

To remove an unallocated device or image from the default policy, you must add the device or image to a new or existing policy (see *Creating a Policy* on page 4-3 and *Changing a Policy* on page 4-9).

Note: Each machine image you register is automatically added to the default policy.

Creating a Policy

Complete this procedure to create a policy and to add machine images, devices, and rules to it. Finally, when creating a policy you can specify the conditions for encryption key approval.

Procedure:

LOCATION WEB CONSOLE MAIN MENU | POLICIES > POLICIES PAGE | ADD POLICY BUTTON > ADD POLICY PAGE

1. Specify a policy name and description in the "Policy Information" area.

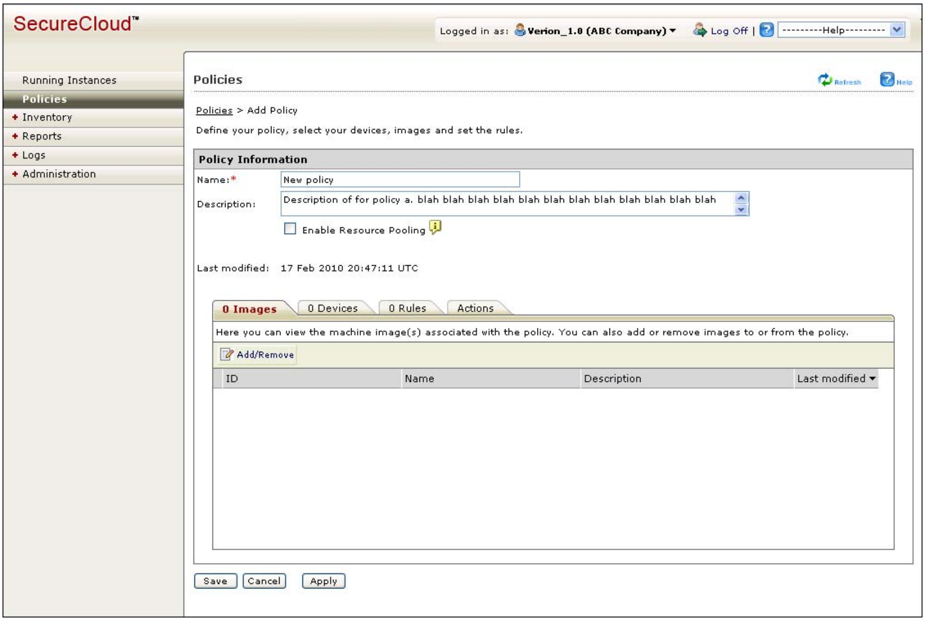
The **Name** and **Description** fields are required.

2. To make resource pooling available in the policy, select the **Enable Resource Pooling** check box.

Resource pooling provides an alternative device if the intended device is busy. See *About the Resource Pool* on page 4-2.

3. Click **Next**.

The Images, Devices, Rules, and Action tabs appear in the Policies (Policy Information) page (see *Figure 4-3*).



Policies > Add Policy

Define your policy, select your devices, images and set the rules.

Name:* New policy

Description: Description of for policy a. blah blah blah blah blah blah blah blah blah blah blah

□ Enable Resource Pooling

Last modified: 17 Feb 2010 20:47:11 UTC

Here you can view the machine image(s) associated with the policy. You can also add or remove images to or from the policy.

ID	Name	Description	Last modified

FIGURE 4-3. Policies page displaying tabs

4. Click the **Images** tab to add a machine image to the policy.

   See *Adding or Removing a Machine Image* on page 4-5.

5. Click the **Devices** tab to add a device to the policy.

   See *Adding or Removing a Data Storage Device* on page 4-5.

6. Click the **Rules** tab to add a rules to the policy.

   See *Adding or Removing Rules* on page 4-6.

7. Click the **Action** tab to specify the encryption key approval process.

   See *Specifying the Encryption Key Approval Process* on page 4-6.

8. Click **Save** to save changes and return to the **Policies** page.

   Click **Apply** to apply changes and continue working in the **Policies** page.

   The new policy appears in the Policies page.

Adding or Removing a Machine Image

The machine images available for addition are those that you created in the cloud provider.

Procedure:

WEB CONSOLE MAIN MENU | POLICIES > POLICIES PAGE | DESIRED POLICY LINK > EDIT POLICY PAGE

1. Click the **Images** tab.

   See *Figure 4-3* on page 4-4. All machine images registered with SecureCloud are listed in the Images tab.

2. Click **Add/Remove**.
3. Click the check box next to the desired machine image(s) to either select or deselect the machine image(s).
4. Click **Save** to save changes and return to the **Policy** page.

   Click **Apply** to apply changes and continue working in the **Add Policy** page.

Adding or Removing a Data Storage Device

The data storage devices available for addition are those that you created in the cloud service provider.

Procedure:

WEB CONSOLE MAIN MENU | POLICIES > POLICIES PAGE | DESIRED POLICY LINK > EDIT POLICY PAGE

1. Click the **Device** tab.

   See *Figure 4-3* on page 4-4. All devices registered with SecureCloud are listed in the Devices tab.

2. Click **Add/Remove**.
3. Click the check box next to the desired data storage device and either select or deselect the data storage device.
4. Click **Save** to save changes and return to the **Policy** page.

   Click **Apply** to apply changes and continue working in the **Add Policy** page.

Adding or Removing Rules

Before an instance can access an encrypted data storage device, you can specify that the instance, along with the device, image, and request, first meet certain criteria. You can also specify the criteria for certain environment checks. This criteria is expressed in SecureCloud as rules.

A rule for which you assign the **Information only** evaluator is not evaluated. Rather, in the Key Request page, you just use the rule value to make your key-approval decision.

Procedure:

WEB CONSOLE MAIN MENU | POLICIES > POLICIES PAGE | DESIRED POLICY LINK > EDIT POLICY PAGE

1. Click the **Rules** tab.

   See *Figure 4-3* on page 4-4.
2. Click **Add/Remove**.
3. Click the check box next to the desired rule to either select or deselect the rule.

   When selecting a rule, also complete the adjacent field for that rule.
4. Click **Save** to save changes and return to the **Policy** page.

   Click **Apply** to apply changes and continue working in the **Add Policy** page.

Specifying the Encryption Key Approval Process

SecureCloud provides an encryption and decryption key to a virtual machine image after its credentials have been approved. If the requesting machine instance meets the criteria defined in the policies, then you can take one of the following actions on the pending key:

- Manual approval
- Auto approval within a certain period of time

Note: The period of time is set by the system administrator from the SecureCloud Web console | Policies > Policies page > Policies - Edit Policies page | Actions tab.

To approve the credentials of the requesting machine instance (see *Figure 4-3*), the Runtime Agent must collect the following information and pass it to the Management Server for validation:

- Virtual Machine ID

  The VMID is a unique identifier for each of the virtual machine.
- Physical location of the machine
- IP address of the virtual machine
- Time of day
- Day of week
- OSSEC version number

TABLE 4-3. Credential information for encryption key approval

CREDENTIAL INFORMATION	DESCRIPTION	EXAMPLE
Device Access Type	The requested access type, either read/write or read-only	read-only or read/write
Device Identity	The requested device identity.	Vol-12345
Device Mount Point	The mounting point for the device if keys are approved.	/mnt/secure or X
Image Identity	The machine image identity as provided by the instance agent.	Ami-12345
Instance Identity	The machine instance identity as provided by the instance agent.	i-12345
Instance First seen	Date and time the instance was last seen by the system.	
Instance Last seen	Date and time the instance was last seen by the system.	
Instance User Data	The data packet provided to the instance at start up.	DataKey= MySecretKey

TABLE 4-3. Credential information for encryption key approval

CREDENTIAL INFORMATION	DESCRIPTION	EXAMPLE
Instance Location	The location of the server farm running the machine instance.	Us-east-1c
Integrity Check Product Summary	The ICM product summary.	
Integrity Check File Version	The version of the `ossec-init.conf` security file.	2.3 or 2.2
Request Source IP Address	The IP address that requested the keys.	
Request Requested	Date and time the key request was received.	
Request Identity	The key requested identity.	

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | POLICIES > POLICIES PAGE | DESIRED POLICY LINK > EDIT POLICY PAGE

1. Click the **Actions** tab.
2. Specify the key approval action for SecureCloud to take when rules either match or do not match.

   Approve — SecureCloud approves the key request automatically at encryption key download time.

   Manual Approve — To set the key approval process to "Manual Approve" either when the rules match or do not match will give the key a status of "Pending" in the Running Instances page. In this case, you will have the option to either approve or deny a key to access the secure data storage (see *Acting Upon a Pending Key* on page 3-4).

   If you select "Manual Approve" for either the **If all rules match** drop-down or **If one or more rule fails** drop-down, SecureCloud enables you to specify a time when automatic approval will occur if no manual approval is taken.

3. Click **Save** to save changes and return to the Policy page.

   Click **Apply** to apply changes and continue working in the Add Policy page.

Changing a Policy

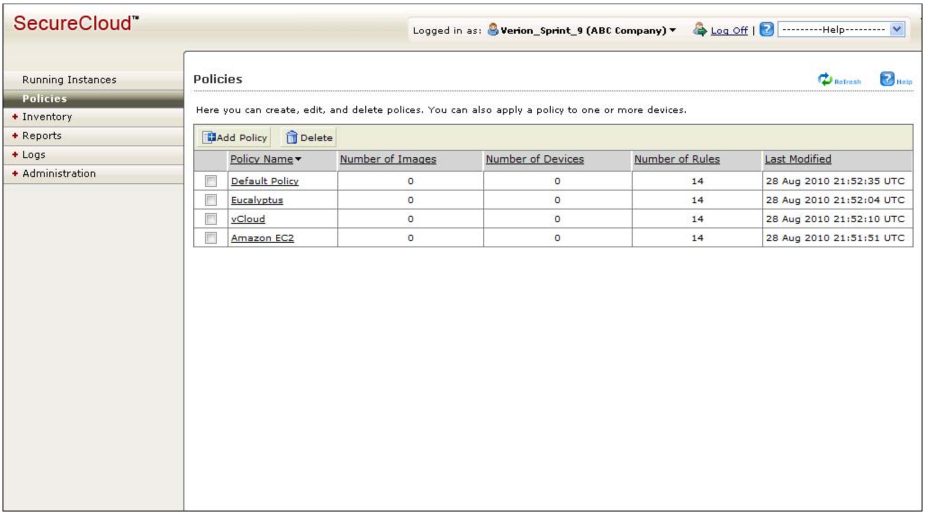
Complete this procedure to change what machine images, devices, and rules are included in the policy. You can also change the conditions necessary for encryption key approval.

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | POLICIES > POLICIES PAGE

1. In the "Policy" column, click the desired policy link.

   See *Figure 4-4*.



Policies

Here you can create, edit, and delete polices. You can also apply a policy to one or more devices.

	Policy Name	Number of Images	Number of Devices	Number of Rules	Last Modified
□	Default Policy	0	0	14	28 Aug 2010 21:52:35 UTC
□	Eucalyptus	0	0	14	28 Aug 2010 21:52:04 UTC
□	vCloud	0	0	14	28 Aug 2010 21:52:10 UTC
□	Amazon EC2	0	0	14	28 Aug 2010 21:51:51 UTC

FIGURE 4-4. Policies page showing existing policies

2. From the "Policy Information" area, access the appropriate fields to change the policy name and description.

3. To add or remove a machine image, click the **Images** tab and then make the appropriate selection(s) in the tab.

   See *Adding or Removing a Machine Image* on page 4-5.

4. To add or remove a device, click the **Devices** tab and then make the appropriate selection(s) in the tab.

   See *Adding or Removing a Data Storage Device* on page 4-5.

5. To add or remove a rule, click the **Rules** tab and then make the appropriate selection(s) in the tab.

   See *Adding or Removing Rules* on page 4-6.

6. To change the settings for encryption key approval, click the **Actions** tab and then make the appropriate changes.

   See *Specifying the Encryption Key Approval Process* on page 4-6.

7. Click **Save** to save changes and return to the Policy page.

   Click **Apply** to apply changes and continue working in the Add Policy page.

Deleting a Policy

If you delete a policy which contains devices, SecureCloud requires you to reassign them to another policy or policies before policy deletion.

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | POLICIES > POLICIES PAGE

- Select the check box next to each policy that you want to delete and then click **Delete**.

  See *Figure 4-4*.

Note: All devices and images must belong to at least one policy, and as such the default policy cannot be deleted.

Chapter 5

Machine Image and Data Storage Device Information

Topics in this chapter include the following:

Registering a Machine Image

Note: This section applies to Amazon and Eucalyptus cloud environments. For vCloud, the process of registering an image and provisioning a device is combined and happens when the user is prompted to reboot their machine image (see *Encrypting a New Data Storage Device* on page 8-6).

After installing the Runtime Agent in the machine image, you need to register the image with the SecureCloud Management Server in order to see the image in the SecureCloud Web console. The registration is done by the SecureCloud Configuration Tool, which prompts you for your cloud service provider's credentials. In addition to this prompting method, the Configuration Tool can accept cloud credential data using command-line parameters.

For machine images in the Amazon and Eucalyptus environments, cloud credentials are stored in encrypted form in the image. The credentials keys are stored in the SecureCloud Management Server.

WARNING! For security reasons, please delete your cloud credentials, such as the private key and certificate, from the image after the Configuration Tool has run and before the image is bundled. If you would rather not delete your cloud credentials, you can move them to the `/mnt` or `/tmp` folder.

Table 5-4 lists the command-line parameters you can use to specify the machine image credentials.

Note: The cloud credentials specified in *Table 5-4* are never sent to the Management Server.

TABLE 5-4. Input parameters for machine image credentials

COMMAND-LINE PARAMETER	COMMAND-LINE SWITCH	DESCRIPTION
MS_Account_GUID	-g	The user's Management Server account GUID, which can be obtained from the MS Web console.
ReadWrite_Devices	-w	Comma-delimited list of device IDs that should be mounted by this image with read/write access.
ReadOnly_Devices	-r	Comma-delimited list of device IDs that should be mounted by this image with read-only access.
AMAZON-ONLY PARAMETERS		
CSP_Private_Key	-k	The location of a file containing the user's service provider private key.
CSP_Certificate	-c	For Amazon, this is the location of a file containing the user's service provider certificate.
EUCALYPTUS-ONLY PARAMETERS		
CSP_Access_Key	-a	The base-64 encoded service provider access key.
CSP_Secret_Key	-s	The base-64 encoded service provider secret key.

Changing Machine Image Information and Viewing Related Information

The machine image name and description can also be changed from the Edit Image page, as described in *Viewing and Changing Machine Image Information* on page 3-3.

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | INVENTORY > IMAGES > IMAGES PAGE | DESIRED IMAGE LINK > IMAGES - EDIT IMAGE PAGE

1. From the "Image Information" area, use the appropriate fields to change the machine image name and/or description.

   The mount point is the path you assign to the data storage device.
2. From the "Policy" area, you can learn to which policy or policies the machine image belongs.
3. From the "Instance(s)" area, you can learn which instances are associated with the machine image.

   To learn more about an instance, click on the desired link (see *Viewing Instance and Related Information* on page 3-3).

Data Storage Device Information

From the Devices page, you can view and change data storage device information. A device is added or removed from SecureCloud in your cloud service provider environment. See your cloud service provider documentation for details.

Data Storage Device Assignment

Note: This section applies to Amazon and Eucalyptus cloud environments. For vCloud, the data storage device assignment process is done at the time of creating the virtual machine image.

In SecureCloud, you can determine the data storage device assignment by using one of the following:

- Configuration file

- User data
- Resource pools on the Management Server (for Amazon and Eucalyptus environments only)

  See *About the Resource Pool* on page 4-2.

You can specify user data when you launch a machine image instance by typing the desired text in the **User Data** field using the following format:

```
devices=[dev_id1,dev_access1,dev_mountPoint1][dev_id2,dev_access2,
dev_mountPoint2]
```

For example:

```
devices=[vol-1111,readWrite,/mnt/test1][vol-2222,readOnly,/mnt/
test2]
```

After the machine image instance is launched, the user data is introduced into the instance so the agent knows the user data, using the cloud service provider's API. Providing that you follow the correct user data format, SecureCloud extracts the device information from the user data to do the following:

- Request a key for the specified device(s) from the Management Server
- Attach the specified data storage device to the running machine image instance
- Mount the specified data storage device to the specified mount point

The content of the configuration file is determined during agent configuration. During configuration, you need to specify the data storage device ID for each device. The configuration utility will write this information to the configuration file.

The agent treats user data with higher priority than the configuration file. If any device information conflicts with user data and agent configuration file data, then the agent gets the information from the user data first. The user could specify no user data. In this case, the device information in the agent configuration file is used for attaching and mounting devices. For resource pooling, the agent treats device information retrieved from the Management Server with the highest priority.

Viewing and Changing Data Storage Device Information

In order to have access to a data storage device in SecureCloud you need to first create that device within the cloud provider and then register the data storage device with SecureCloud. The Provisioning Service encrypts the data storage device and then registers it with SecureCloud (see Chapter 8, *Provisioning for Data Storage Encryption*). Once registered, the encrypted data storage device is available to you in SecureCloud.

For any data storage device with the status of "Available" you are able to change device name, description, and mount point.

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | INVENTORY > DEVICES > DEVICES PAGE | DESIRED DEVICE LINK > DEVICES - EDIT DEVICE PAGE

1. From the "Device Information" area, change any desired information.

   Access the appropriate fields to change the device name and description. Your cloud service provider automatically generated the device identity and device name.

   The following are the possible device statuses:

   - **Available** — Not currently in use and not yet encrypted
   - **Attached** — Attached to an instance but the encryption key has not yet been given to an application in order to access the encrypted data.
   - **Mounted** — Attached to an instance and the encryption key has been given to an application in order to access the encrypted data.

   The mount point is the path you assign to the data storage device.

2. From the "Instance(s)" area, click the link of any desired instance to see complete instance details.

3. From the "Policy" area, you can view information about the policy associated with the device.

   See Chapter 4, *Managing Policies*.

4. From the "Encryption Key" area, you can view the encryption settings for the key that has access to the data storage device.

ENCRYPTION KEY INFORMATION	DESCRIPTION
Cipher	The encryption algorithm used by SecureCloud is the Advanced Encryption Standard (AES).
Key size	128 bits is the encryption key size.
Mode	The mode of operation for the AES cipher is Cipher Block Chaining (CBC).
Key management type	Linux Unified Key Setup (LUKS) is a disk-encryption specification for data storage devices. **Note:** For the vCloud environment, with a Windows based image, LUKS is not used.
Hash	In LUKS mode the hash algorithm used in PBKDF2 to protect against dictionary attacks.

5. Click **Save** to save changes and return to the Devices page.

   Click **Apply** to apply changes and continue working in the Edit Device page.

To change additional device information, see *Encrypting a New Data Storage Device* on page 8-6.

Chapter 6

Reports and Logs

SecureCloud enables you to generate logs and reports to assist day-to-day administration and provide evidence for security compliance as mandated by law.

Topics in this chapter include the following:

- *Generating Reports*
- *Understanding Generated Reports*
- *Querying Logs*
- *Understanding Archived Logs*

Reports

SecureCloud enables you to generate reports. SecureCloud provides the following canned reports based on a specified time range:

- Number of keys have been requested, denied and approved
- Intervals between key request and approvals
- Total number of instances that have been spun off
- Total number of machine images
- Total number of data storage devices
- Auditing reports—describes who is accessing the console, who and what time a user created and/or deleted a policy, and who approves manual key requests.

You can generate a report either in PDF or Microsoft Excel (XLS) format.

Generating Reports

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | REPORTS > GENERATE REPORT > GENERATE REPORT PAGE

1. Specify a report name in the **Name** field.

   The **Name** field is required.

2. Specify any other necessary information to create your report.

   In the "Date Range" area, the default in the **From** and **To** fields is the current date.

   Before a report can be generated, you need to select at least one criterion in the "Type of Reports" area.

   In the "Format" area, specify the format in which you want to view the composite report.

3. Click **Generate Report**.

Understanding Generated Reports

SecureCloud generates a composite report that includes data for all the criterion that you specify. This composite report appears in a separate window. For each specified report criterion, SecureCloud creates a graph or chart to represent the data. Following each chart is a table that further describes the data.

Logs

SecureCloud logs all the system events. SecureCloud enables you to query logs based on the following configurable information:

- Date range
- Log event types

From the Log Query page and log window, you can export the log data to an CSV file.

Querying Logs

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | LOGS > QUERY > LOG QUERY PAGE

1. Specify the date range.

   The hours and minutes (hh:mm) information is optional.
2. Specify the log type:
   - Agent Events:
     - Date and time the machine image requested a key and the result
     - Record of the data encrypted
   - Key Action Events:
     - Date and time of each key request and result
     - Key requests from machine images
   - Policy Events:
     - Record of machine image policy creation and removal
   - User Events:
     - Record of user account login

- User activity in SecureCloud Web console

The log data appears in a separate window and is organized by date. From either the Log Query screen or the query window, you can export the log data to an CSV file.

SecureCloud saves log data for a 12-month rolling cycle. Archived logs are saved for an additional 12 months, after which SecureCloud deletes them.

Understanding Archived Logs

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | LOGS > ARCHIVED LOGS > ARCHIVED LOGS PAGE

- Click the hyperlink of the desired archived log.

  The log information appears.

  Because SecureCloud purges the log data after 12 months, you can save this data to an Excel file before the purge by clicking the XLS icon near the desired log file(s).

Chapter 7

Administration

Topics in this chapter include the following:

- *Adding a New User*
- *Changing User Information*
- *Deleting a User*
- *User Role Management*
- *Notification Management*
- *Changing a Password*
- *Product License*
- *Data Recovery*

Adding a New User

SecureCloud enables you to add a user you want to have access to the service.

Procedure:

LOCATION WEB CONSOLE MAIN MENU | ADMINISTRATION > ACCOUNT MANAGEMENT > ACCOUNT MANAGEMENT PAGE (USERS TAB)

1. Click **Add User**.
2. From the "User Information" area, complete all the required fields.

   See *User Role Management* on page 7-3 for a description of each possible role.
3. Click **Save**.

Changing User Information

Once you create a user, SecureCloud enables you to change user information, including the assigned role.

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | ADMINISTRATION > ACCOUNT MANAGEMENT > ACCOUNT MANAGEMENT PAGE (USERS TAB) | DESIRED USER LINK

1. From the "User Information" area, change the desired field(s).

   See *User Role Management* on page 7-3 for a description of each possible role.
2. Click **Save**.

Deleting a User

SecureCloud enables you to remove a user you no longer want to have access to the service.

Procedure:

LOCATION WEB CONSOLE MAIN MENU | ADMINISTRATION > ACCOUNT MANAGEMENT > ACCOUNT MANAGEMENT PAGE (USERS TAB)

1. Click the check box of the desired user(s) to delete.
2. Click **Delete**.

User Role Management

The assigned user role determines the level of funtionality a user has in SecureCloud. *Table 7-5* details these user roles.

TABLE 7-5. SecureCloud funtionality based on user roles

ROLE	DESCRIPTION
Administrator	Provides full functionality for all operations.
Data Analyst	Provides full report and log functionality. No other functionality is supported.
Auditor	Provides full report and log functionality. All other functionality is limited to read-only access.
Key Approver	Provides functionality to deny or approve key requests. Policy, Image, and device functionality is limited to read-only access. No other functionality is supported.

Viewing Assigned User Roles

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | ADMINISTRATION > ACCOUNT MANAGEMENT > ACCOUNT MANAGEMENT PAGE (ROLES TAB)

From the Roles page, you can view how many users are assigned to each role.

Viewing User Role Permissions

The same account cannot belong to two roles. For example, an account with the System Administrator role cannot also have the Auditor role.

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | ADMINISTRATION > ACCOUNT MANAGEMENT > ACCOUNT MANAGEMENT PAGE (ROLES TAB)

1. Click the link of the desired role.
2. From the Role Information page, view user role information.
3. Click **Back** to return to the Account Management page (Roles tab).

Notification Management

SecureCloud can issue an email alerting you of the following conditions:

- A pending key request exists.
- Errors occurred during a key request.
- A key request timed out.
- A data storage device has not been assigned to a policy.

SecureCloud can send email notifications to a single or multiple individuals.

Creating a Notification

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | ADMINISTRATION > NOTIFICATIONS > NOTIFICATIONS PAGE | ADD NOTIFICATION BUTTON > NOTIFICATIONS SETTINGS PAGE

1. In the "General Information" area, specify a group name and description.

   The **Name** field is required.
2. In the "Email Message" area, specify the email address of the individual or individuals who are to receive the email notifications.

   The sender email address will always be `noreply@securecloud.com` and cannot be changed.

   Use a semicolon (;) to separate multiple email addresses.
3. In the "Body Section" area, specify the email subject, header, contents, and footer.

   In the "Content" section, specify the condition(s) to which you want to be notified.

   If you are not satisfied with the default message for a notification event, type a new message in the text box.

To use a variable in the message, place the cursor in the desired position in the text, click **Insert Variable**, and then choose the appropriate variable.

4. In the "Notification Frequency" area, specify how often you want to send email notifications.

   A consolidated notification is an email that contains all the issued notifications.

5. Click **Save**.

   The new notification appears in the Notifications page.

Changing an Existing Notification

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | ADMINISTRATION > NOTIFICATIONS > NOTIFICATIONS PAGE

1. In the "Notifications" area, click the desired notification in the "Name" column.
2. In the Notification Settings page, make the appropriate changes and then click **Save**.

   See *Creating a Notification* on page 7-4 starting with Step 1.

Deleting a Notification

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | ADMINISTRATION > NOTIFICATIONS > NOTIFICATIONS PAGE

1. In the "Notifications" area, click the check box of the notification(s) you want to delete.
2. Click **Delete**.

Changing a Password

SecureCloud enables you to change your log-in password. The password was originally set during product registration (see *Registering the SecureCloud Product* on page 2-2).

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | ADMINISTRATION > CHANGE PASSWORD > CHANGE PASSWORD PAGE

1. Specify the current password and the new password in the appropriate fields.

   The password must be 8 to 32 characters, containing at least one of the following:

   - Upper case character
   - Lower case character
   - Numeral
   - Special character (~!@#$%^&*()_+)
2. Re-specify the new password in the **Confirm new password** field.
3. Click **Save**.

Product License

A license comes with an activation code that you use to activate the SecureCloud product. A license grants permission to a certain amount of keys used to encrypt and decrypt a data storage device.

SecureCloud warns you when the number of concurrent keys is approaching the maximum number of licensed keys.

Upgrading From a Trial License

If you want to continue using SecureCloud after your trial license has expired, you need to get a standard license from your reseller and from this license, specify the activation code in the License page.

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | ADMINISTRATION > PRODUCT LICENSE > LICENSES PAGE

1. Click the **Enter a new code** link.
2. From the Enter A New Code page, specify the new activation code and then click **Activate**.

   If you do not have an activation code, please register online with your registration code for a valid activation code.

   `https://olr.trendmicro.com/registration/us/en-us/login.aspx`

Migrating from Beta to Production

At the end of the beta you can migrate from the beta license to a production license; increasing the number of encryption keys entitlement for your current license and expiration date. This can be done by purchasing additional keys from your reseller. Migration from beta to production will require that you obtain a new activation code from your reseller. Once you have obtained your new activation code, use it to replace the beta activation code in the SecureCloud Web console > Administration > Product License page.

Data Recovery

Encrypted Data Backup

Back up your encrypted data just as though it were unencrypted. Restore this data to a device and then mount this device to a machine image running the SecureCloud agent. Request and approve the keys for the device.

Device Encryption Keys Backup and Site Readiness

The device-encryption keys are stored in a SecureCloud database, protected by several layers of encryption. This database is backed up regularly, with backups taken offsite and stored encrypted. The encryption keys for these database backups are also stored securely offline.

If the primary database should go down, the backup database will be used in its place. In the event of a catastrophic failure to the SecureCloud facility, a backup site will quickly come online, making the latest backup of encryption keys available to you.

Chapter 8

Provisioning for Data Storage Encryption

Provisioning to encrypt a data storage device starts in your cloud service provider where you create a device and then launch the Provisioning Server. Next from the SecureCloud Web console you specify which device(s) you want the Provisioning Server to encrypt.

Topics in this chapter include the following:

- *About the Provisioning Service*
- *Creating a Data Storage Device in Your Cloud Service Provider Environment*
- *Adding a Data Storage Device to the Inventory*
- *Deleting a Data Storage Device from the Inventory*

About the Provisioning Service

The *Provisioning Service* is a Web-based, virtual appliance that runs within your cloud service provider. The Provisioning Service is a one-time instance that connects to SecureCloud and passes the application a list of active devices. SecureCloud then "cross references" this list to see which devices are already encrypted. From SecureCloud, you can view the results of this "cross reference" and direct the Provisioning Service to encrypt any un-encrypted devices.

The Provisioning Service encrypts your specified devices using the device encryption keys generated by the SecureCloud Management Server. Furthermore, when the Provisioning Service encrypts a device, it also implicitly registers that device with the SecureCloud Management Server. This registration is necessary in order for a machine image to have access to an encrypted device.

Creating a Data Storage Device in Your Cloud Service Provider Environment

After SecureCloud confirms your registration, you need to go to your cloud service provider and create a data storage device for encryption. You can either create a new device or clone an existing one. Once this is done, the new device is available for encryption from the SecureCloud Web console using the Provisioning Service.

Creating a New Data Storage Device

Before a data storage device can be encrypted and added to the SecureCloud inventory, you must create the device within your cloud service provider and launch the SecureCloud Provisioning Service in your cloud service provider environment.

Procedure:

1. From your cloud service provider, create a new data storage device to encrypt.

   Refer to your cloud service provider documentation for complete details.

2. Load the SecureCloud Provisioning Server in your cloud service provider's environment.

   - For an Amazon environment, see *Launching the SecureCloud Provisioning Service in Amazon* on page 8-3.

- For an Eucalyptus environment, see *Launching the SecureCloud Provisioning Server in Eucalyptus* on page 8-4.
- For an Amazon environment, see *Encrypting a Data Storage Device in vCloud* on page 8-5.

3. Launch an instance of the SecureCloud Provisioning Server.

This is necessary so that the SecureCloud Web console can communicate with the cloud service provider and learn how many devices are available and also to direct the Provisioning Service to encrypt and register any specified device(s).

Launching the SecureCloud Provisioning Service in Amazon

After creating a data storage device, complete the steps in this section to launch the Provisioning Server.

Procedure:

- Pick the appropriate community AMI based on your Amazon zone requirements:

TABLE 8-6. Amazon Community AMIs

REGION	AMI ID	AMI NAME
US-EAST	ami-8a7782e3	US-EAST-SC-PS-V1.0-1155B
US-WEST	ami-8c1242c9	US-WEST-SC-PS-V1.0-1155B
EU-WEST	ami-f27a4f86	EU-WEST-SC-PS-V1.0-1155B
AP-SOUTHEAST	ami-b01f61e2	ASIA-SOUTH-EAST-SC-PS-V1.0-1155B

Note: In order to launch the Provisioning Server in your cloud service provider's environment, you need to open port 443, the port on which the Provisioning Service listens.

Launching the SecureCloud Provisioning Server in Eucalyptus

After creating a data storage device, complete the steps in this section to launch the SecureCloud Provisioning Server.

Procedure:

Note: In order to launch the Provisioning Server in your cloud service provider's environment, you need to open port 443, the port on which the Provisioning Service listens.

1. Download the Provisioning Service EMI from the Trend Micro portal:
   `http://downloadcenter.trendmicro.com/`
2. Load the Provisioning Server EMI into your Eucalyptus environment:
   - **a.** Use FTP/SCP tool to upload this package to your Eucalyptus controller machine or any running Eucalyptus instance
   - **b.** Decompress it using the following command:

     ```
     bzip2 -cd ProvisionAgentB1155.tar.bz2 | tar -xvf -
     ```

     You will get a `image.img` file under `./mnt` folder
   - **c.** Use the command, `euca-describe-images|grep eki` to get the correct kernel. It looks like the following:

     ```
     centos-5.3-kernel-bucket-4g-3rd/vmlinuz-2.6.28-11-server.man
     ifest.xml
     ```

     Remember the kernel name, such as `eki-aaaa`.
   - **d.** Use command `euca-describe-images|grep eri` to get the correct ramdisk. It looks like the following:

     ```
     centos-5.3-kernel-bucket-4g-3rd/initrd.img-2.6.28-11-server.
     manifest.xml
     ```

     Remember the ramdisk name, such as `eri-bbbb`.
   - **e.** Bundle eucalyptus image using the following command:

     ```
     euca-bundle-image -i image.img -d . -r i386 --kernel
     eki-aaaa --ramdisk eri-bbbb
     ```

f. After bundling completes, you can upload the bundled image using the following command:

```
euca-upload-bundle -b Trendmicro-Provision-Server
-m./image.img.manifest.xml
```

g. After upload completes, you can use the following command to register your image:

```
euca-register
Trendmicro-Provision-Server/image.img.manifest.xml
```

This results in you receiving an EMI.

h. Run it with the `euca-run-instance` command.

Encrypting a Data Storage Device in vCloud

After creating a data storage device, complete the steps in this section to encrypt the device.

Procedure:

Note: In order to launch the Provisioning Server in your cloud service provider's environment, you need to open port 443, the port on which the Provisioning Service listens.

---

1. Download the Provisioning Service OVF from the Trend Micro portal:

   `http://downloadcenter.trendmicro.com/`

2. Load your vCloud Provisioning Server into your vCloud environment.

   a. Download PS vCloud image (`vCloud-SC-PS-V1.0-1155B.zip` file) from Trend Micro and then decompress it.

   b. Open vCloud organization Web console and login as an organization administrator account.

   c. Go to **Catalogs > vApp Templates tab**.

   d. Add a new data storage device (disk) to the VM.

   e. Click the upload button (upward-pointing arrow) and then select the "PS OVF" file from step 1.

Adding a Data Storage Device to the Inventory

You can either add a new device or a cloned one to the SecureCloud inventory. SecureCloud can encrypt a new device created from your cloud service provider. SecureCloud does not encrypt a device clone since it retains the encryption from the originating, cloned device.

Encrypting a New Data Storage Device

Note: Encrypting a data storage device for use with SecureCloud is a destructive process and should not be performed on a device that contains data.

Prerequisite:

Create a data storage device from your cloud service provider (see *Creating a New Data Storage Device* on page 8-2).

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | INVENTORY > DEVICES > DEVICES PAGE | ADD BUTTON > DEVICES - SELECT OPTION PAGE

Note: For the vCloud environment, you must first set up a low-privilege user—with read-only access to the entire organization in vCloud. These "read-only" credentials are what you specify during device encryption.

1. Select **Prepare new device(s) for encryption** and then click **Next**.
2. From the Devices - Prepare New Device(s) for Encryption page, specify the Provisioning Service information.

   The fields in the "Provisioning Service" area are all required.

   The **IP address/Hostname/DNS** field is where you identify the server hosting the Provisioning Service. The **Port number** field is where you identify the port that the Management Server uses to communicate with the Provisioning Server.

   If your Provisioning Service is public and accessible through the Internet, select the check box in the "Provisioning Service" area to add additional security to your public cloud environment. This feature is not applicable in a private cloud environment.

3. Click **Connect**.
4. From the Devices - Credential Information page, specify your cloud service provider credential information.

   Note: For security reasons, the SecureCloud Management Server does not save your credential information. Therefore, you must re-enter it each time you start an encryption session.

   ### For Amazon

   - Enter certificate and private key information in the fields provided and then click **Next**.

     The certificate and private key were available for download from the Amazon console when you created your Amazon account.

   ### For Eucalyptus

   - Upload the credential file.

     You obtain the credential file by downloading it from the Eucalyptus management console.

   ### For vCloud

   - In the "Account Information" area, specify the IP address or hostname of the vCloud Service Director.
   - In the "Credential Information" area, specify the username, password, and organization.

     These are the "read-only" credentials that should be entered during provisioning. It is important that the "full access" credentials are not specified here because they will get stored in both the Provisioning Service and the machine image itself, albeit encrypted but with non-secret data.

5. Click **Next**.
6. From the Device Encryption page, select the device(s) you wish to encrypt and then click **Encrypt**.

Please ensure that a mount point for the device you wish to encrypt is specified. If a mount point is not specified, click the appropriate device ID and specify a mount point. By clicking a device ID, you can also change certain device information.

Device Information	Description
Name	A name to identify this device by in the SecureCloud Management Server.
Description	A description of the device (optional).
Operating system	The operating system this device will be used by.
File system	The file system type you wish to format the device with. SecureCloud supports the following file systems: Windows: FAT32 and NTFS; Linux: EXT3 and XFS.
Mount point	The path you assign to the data storage device.
See *Viewing and Changing Data Storage Device Information* on page 5-6 for a complete description of encryption key information.	

For the vCloud service provider, you must reboot a machine image associated with the device you wish to encrypt in order to initiate the encryption process.

Note: A vCloud encrypted device is attached to specific instances and can never be attached to a different instance.

The newly encrypted device appears in the Device page with a status of "Encrypted".

Adding a Device Clone

When you clone a device in your cloud service provider's environment, a snap shot of the device data is taken and placed in temporary storage in the cloud service provider's environment. When you add the cloned device to the SecureCloud inventory, the data is restored from the temporary memory location to a new device. The new device uses the same encryption keys that are used by the originating, cloned device.

Prerequisite:

From your cloud service provider, create a device clone from the desired device. Refer to your cloud service provider documentation for complete details. Note the new device ID, and originating device ID. You will need to specify this information when you add the device clone to the SecureCloud inventory.

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | INVENTORY > DEVICES > DEVICES PAGE | ADD BUTTON > DEVICES - SELECT OPTION PAGE

1. Select **Assign an encryption key to a cloned device** and then click **Next**.
2. In the "New Cloned Device Information" area, provide the necessary device clone information.
3. In the "Inherit Property and Encryption Key from Registered SecureCloud Device" area, provide the ID of the originating cloned device.

   The device clone uses the same encryption keys that are used by the originating cloned device.
4. Click **Save**.

   The device clone appears in the Device page with a status of "Available".

Deleting a Data Storage Device from the Inventory

Deleting a device from the SecureCloud inventory, whether it be a clone or non-clone device, does not remove it from your cloud service provider environment. Therefore, it is always possible to add a deleted device back to the SecureCloud inventory.

Note: It is not possible to recover the encryption key of a deleted device. By re-adding it to the SecureCloud inventory you will destroy all existing data.

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | INVENTORY > DEVICES > DEVICES PAGE

- Select the desired device(s) with a status of "Available" and then click **Delete**.

Note: You cannot delete a device with a status of "In use".

Appendix A

Installing and Uninstalling the SecureCloud Runtime Agent

The SecureCloud Runtime Agent can be installed in a Windows or Linux (CentOS) environment on the machine image.

Topics in this appendix include the following:

- *Installing SecureCloud*
- *Uninstalling SecureCloud*

Installing SecureCloud

Before installing the SecureCloud Runtime Agent, ensure that you have done the following:

- Create a data storage device in your cloud environment.

  See *Creating a Data Storage Device in Your Cloud Service Provider Environment* on page 8-2 and your cloud service provider documentation for details.
- Encrypt and register the data storage device with SecureCloud (for Amazon and Eucalyptus environments only).

Note: In the Amazon and Eucalyptus environments, you can run the Configuration Tool after installation and supply the device ID to configure with the machine image. Therefore, it is best to provision the device first, although this is not a requirement.

See see Chapter 8, *Provisioning for Data Storage Encryption*.

Installing in a Linux Environment

Prerequisites:

These prerequisites apply to the Amazon and Eucalyptus cloud environments.

Before installing the SecureCloud Runtime Agent in the machine image, please make sure the following software prerequisites are installed on the Provisioning Service machine image:

- All cloud service providers
  - Sun JRE 1.6 or above (download and install from `http://www.java.com/getjava/`)
  - RPM Forge Yum Repository
- Amazon
  - EC2 API Tools (download and install from `http://developer.amazonwebservices.com/connect/entry.jspa?externalID=351&categoryID=88`)

  - EC2 AMI Tools (download and install from `http://developer.amazonwebservices.com/connect/entry.jspa?externalID=368&categoryID=88`)
- Eucalyptus
  - EMI Tools (download and install from http://open.eucalyptus.com/wiki/Euca2oolsCentosInstall_v1.1)

Install the RPM Forge Yum Repository:

32-bit:

```
wget http://packages.sw.be/rpmforge-release/rpmforge-
release-0.5.1-1.el5.rf.i386.rpm rpm -ivh
rpmforge-release-0.5.1-1.el5.rf.i386.rpm
```

64-bit:

```
wget http://packages.sw.be/rpmforge-release/rpmforge-release-
0.5.1-1.el5.rf.x86_64.rpm rpm -ivh
rpmforge-release-0.5.1-1.el5.rf.x86_64.rpm
```

Procedure:

1. Download the appropriate agent build for your cloud instance from the Trend Micro beta portal:

   `http://www.trendbeta.com/`
2. Upload the public and private key pair obtained from your cloud service provider. (This step is not relevant for vCloud.)
3. Use Yum to install the RPM package by executing the following command:

   `yum install --nogpgcheck <c9agent.rpm>`

   `where <c9agent.rpm>` is the name of the installation package downloaded in step 1.
4. Launch the SecureCloud Configuration Tool by executing the following command:

   `/var/cloud9/config_main.sh`
5. Accept the license agreement.
6. When prompted, select the appropriate option for your cloud service provider.

   If your provider is VMware vCloud, then there is an extra window of information you have to provide. This information is the provision server IP address, vCloud organization, and the Management Server ID.

If your provider is Eucalyptus, then there is an extra window of information you have to provide. The information is the Eucalyptus controller IP and port.

7. Enter your SecureCloud Account ID when prompted.

   The SecureCloud Account ID can be found in the SecureCloud Web console main menu | Administration > Account Management

8. Follow the prompts as they appear.

Installing in a Windows Environment

Prerequisites:

This prerequisite applies to the Amazon and Eucalyptus cloud environments.

Before installing the SecureCloud Runtime Agent in the machine image, please make sure the following software prerequisite is installed on the Provisioning Service machine image:

- Sun JRE 1.6 or above (download and install from `http://www.java.com/getjava/`)

Procedure:

1. Launch the machine image on which you want to install the SecureCloud Runtime Agent.
2. Download the agent build for your machine image instance from the Trend Micro beta portal:

   `http://www.trendbeta.com/`

3. Upload the public and private key pair obtained from your cloud provider.

   This step is not relevant for vCloud.

4. Execute the installation package downloaded in step 2 and then follow the on-screen instructions.

   The Installation Wizard prompts you for your cloud service provider. The following information is required, based on your cloud service provider:

   - Amazon:
     - Management Server ID
     - Certificate
     - Private key

    - Devices to mount
- Eucalyptus:
    - Controller IP/port
    - Management Server ID
    - x509 credentials ZIP file
    - Devices to mount
- vCloud:
    - Management Server ID
    - Provisioning Server IP address
    - vCloud organization

5. Enter your SecureCloud Account ID when prompted.

   The SecureCloud Account ID can be found in the SecureCloud Web console | Administration > Account Management

6. Enter the path of the private and public key files uploaded in step 3.

   This step is not relevant for vCloud.

7. Enter the volume ID for the device you provisioned for earlier.

   For example: `vol-234121`

   This step is not relevant for vCloud.

Maintenance Install for Windows Environment

The Installation Wizard can repair errors in the most recent installation by fixing missing or corrupt files and registry entries.

Procedure:

1. Launch the Installation Wizard executable.

   If you did not retain the Installation Wizard executable from the initial installation, then revisit the download site (`http://www.trendbeta.com/`) and download and open the appropriate agent build.

   The Installation Wizard will detect an existing installation of SecureCloud and therefore display the screen for installation maintenance or removal.

2. Click **Repair** from the Repair or Remove the Trend Micro SecureCloud Agent screen.

3. Following the on-screen instructions.

Uninstalling SecureCloud

You can uninstall the SecureCloud agent from one machine image and then install it on another. Uninstalling the SecureCloud agent does not remove your data from the encrypted data storage device(s). If you choose to uninstall the SecureCloud agent and also want to remove your data from the encrypted data storage device(s), contact Trend Micro Technical Support to perform this latter operation.

Note: Contact Trend Micro Technical Support if you want to remove your data from the encrypted data storage device prior to uninstalling the SecureCloud agent.

Uninstalling from a Linux Environment

Procedure

- From a command shell, execute the following command:

```
rpm -ev c9agent
```

Uninstalling from a Windows Environment

Procedure:

1. Launch the Installation Wizard executable.

   If you did not retain the Installation Wizard executable from the initial installation, then revisit the download site (`http://www.trendbeta.com/`) and download and open the appropriate agent build.
2. Click **Remove** from the Repair or Remove the Trend Micro SecureCloud Agent screen.
3. Following the on-screen instructions.

Appendix B

Frequently Asked Questions

This appendix describes questions that may arise when using SecureCloud.

How do I Upgrade My cryptsetup from 1.0.3 to 1.0.7?

Procedure:

Execute the following commands:

```
yum -y install gcc automake autoconf libtool make
e2fsprogs-devel

wget
http://cryptsetup.googlecode.com/files/cryptsetup-1.0.7.tar.bz2

tar -jxvf cryptsetup-1.0.7.tar.bz2

cd cryptsetup-1.0.7

./configure

make

make install

mv /sbin/cryptsetup /sbin/cryptsetup_bak
```

```
cp /usr/sbin/cryptsetup /sbin/cryptsetup
```

How do I Upgrade from a Trial License?

If you want to continue using SecureCloud after your trial license has expired, you need to get a standard license from your reseller and from this license, specify the activation code in the License page.

Procedure:

LOCATION WEB CONSOLE MAIN MENU | ADMINISTRATION > PRODUCT LICENSE > LICENSES PAGE

1. Click the **Enter a new code** link.
2. From the Enter A New Code page, specify the new activation code and then click **Activate**.

   If you do not have an activation code, please register online with your registration code for a valid activation code.

   `https://olr.trendmicro.com/registration/us/en-us/login.aspx`

How do I Migrate from Beta to Production?

At the end of the beta you can migrate from the beta license to a production license; increasing the number of encryption keys entitlement for your current license and expiration date. This can be done by purchasing additional keys from your reseller. Migration from beta to production will require that you obtain a new activation code from your reseller. Once you have obtained your new activation code, use it to replace the beta activation code in the SecureCloud Web console > Administration > Product License page.

What Hypervisors are Supported?

SecureCloud is designed to be used within cloud environments. Integrating at the operating system level, it is not aware of the hypervisor. Therefore, as long as SecureCloud supports the cloud provider API and operating system it will work with any underlying hypervisor the cloud service provider is using.

How do I Install Amazon AMI and API Tools in Linux?

Procedure:

1. Download AMI tools:

   `http://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip`

2. Download API tools:

   `http://www.amazon.com/gp/redirect.html/ref=aws_rc_ec2tools?location=http://s3.amazonaws.com/ec2-downloads/ec2-api-tools.zip&token=A80325AA4DAB186C80828ED5138633E3F49160D9`

3. Unzip to your preferred location. Example uses /opt.
4. Include AMI tools to the PATH variable and EC2_HOME:
   a. `export EC2_HOME=/opt/ec2-api-tools`
   b. `export PATH=$PATH:$EC2_HOME/bin`

How do I Install Amazon AMI and API Tools on Windows?

Procedure:

1. Download AMI tools:

   `http://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip`

2. Download API tools:

   `http://www.amazon.com/gp/redirect.html/ref=aws_rc_ec2tools?location=http://s3.amazonaws.com/ec2-downloads/ec2-api-tools.zip&token=A80325AA4DAB186C80828ED5138633E3F49160D9`

3. Unzip to your preferred location. Example uses `C:\`.
4. Choose **Start > Control Panel > Performance and Maintenance > System**.

   The `EC2_HOME` and `PATH` variables are automatically set when you install them using the installation wizard.

5. Click the **Advanced** tab.
6. Click **Environment Variables**.
7. In the "System variables" area, click **New**.

8. Type `EC2_HOME` in the **Variable name** field and `c:\ec2-api-tools` in the **Variable value** field.
9. Click **OK**.
10. For the `PATH` variable, select **PATH** in the "System variables" area and then click **Edit**.
11. Append `;c:\ec2-api-tools\bin` to the contents of the **Variable value** field.

In Which Time Zones are the Logs Saved and can I Change the Time Zones?

SecureCloud saves the logs in the UTC time zone. It is not possible to change the time zone preference in V1.0. V1.1 will allow SecureCloud hosted service customers to change the time zone preference for the date and time logging.

What Certifications does SecureCloud Hold?

SecureCloud data centers are SAS-70 type II certified.

How can I Ensure all Communication is Secure?

In addition to HTTPS, SecureCloud employs AES 256 encryption for all internal communication protocols.

How does Trend Micro Protect my Cloud Service Provider Credentials?

Trend Micro does not save or store the credentials to your cloud environment. Cloud environment credentials are used during installation and then encrypted within the image. This secures against malicious probing of the credentials.

How do I Recover a Forgotten Web Console Password?

1. Go to the Log On page and click the **Forgot your password?** link
2. Type your email address that you specified when you registered, and then click **Continue**.
3. Click **OK**.

   A "Password Reset Verification" email is sent to you where you click the provided link to complete the password reset.
4. Click the link in the email to reset your password.

What is the Service Availability for SecureCloud?

Trend Micro takes every measure possible to ensure SecureCloud hosted services provide customers with the highest level of service. The SecureCloud SaaS solution hosting is provided by one of our data centers in Europe in a high availability configuration with a standby site hosted out of another datacenter in Europe.

In the event of a catastrophic failure resulting in interruption in service, Trend Micro has processes and procedures in place resume services from a backup location within a matter of hours.

What Kind of Encryption Key Security Exists?

The encryption keys used to encrypt the volumes in the cloud are stored within an encrypted database. The encryption key for the database is securely stored offsite. Controls and measures have been put in place to ensure the encryption keys are secure and protected; however in the event an encryption key and, or SecureCloud agent is suspected to be compromised; customers can migrate data from the original volume to a newly encrypted volume using a different encryption key.

How is SecureCloud Protected from Man-in-middle Attacks?

All transmissions of information are encrypted using AES 256 and takes place over SSL to provide an additional layer of protection.

Who is Responsible for Lost or Stolen Data?

SecureCloud uses industry-standard encryption techniques and takes no ownership of the encryption technology used. SecureCloud offers a unique key management solution validating the virtual environments identity and integrity prior to releasing the managed encryption key into that environment. Therefore, Trend Micro provides no indemnification for lost or stolen data.

Appendix C

Contact Information and Web-based Resources

This appendix provides information on getting further assistance with any technical support questions that you may have.

Topics in this appendix include:

- *Knowledge Base*
- *TrendEdge*
- *Contacting Technical Support*
- *TrendLabs*

Knowledge Base

The Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products and services. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do to. New solutions are added daily.

Also available in Knowledge Base are service FAQs, hot tips, preventive antivirus advice, and regional contact information for support and sales.

http://esupport.trendmicro.com/

And, in case if you cannot find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question in an email message. Response time is typically 24 hours or less.

Note: Because SecureCloud is a new product, the Knowledge Base does not yet contain much information on this product.

TrendEdge

A program for Trend Micro employees, partners, and other interested parties that provides information on unsupported, innovative techniques, tools, and best practices for Trend Micro products. The TrendEdge database contains numerous documents covering a wide range of topics.

http://trendedge.trendmicro.com

Note: Because SecureCloud is a new product, the TrendEdge database does not yet contain much information on this product.

Contacting Technical Support

If you are not able to find an answer in the documentation, Knowledge Base, or through TrendEdge, you can contact Trend Micro Technical Support at:

http://esupport.trendmicro.com/SRFMain.aspx

At this site, please specify your activation code along with other product-related information.

General Contact Information

General US phone and fax numbers follow:

Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

Our US headquarters is located in the heart of Silicon Valley:

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014

For a list of the worldwide support offices, go to:

http://kb.trendmicro.com/solutions/includes2/ContactTechSupport.asp

TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and technical support centers that provide customers with up-to-the minute security information.

The "virus doctors" at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products and services remain secure against emerging risks. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel who provide technical support for a wide range of products and services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA.

Appendix D

Basic Troubleshooting Information

This appendix provides trouble shooting information if you should encounter network configuration problems with vCloud or log management issues.

Topics in this appendix include:

- *Network Configuration and vCloud*
- *Log Management*

Network Configuration and vCloud

Ensure that the network configuration of your cloud service provider's environment enables communications between the virtual machine instances (vApps) running the SecureCloud agent or Provisioning Service are able to connect to the vCloud Director (vCD) Web services using HTTP and HTTPS. Failure to do so may result in errors when provisioning devices or starting the SecureCloud Runtime Agent in the vCloud environment. If your cloud environment is configured such that the vCD is firewalled from the vApps, enable a firewall rule to allow inbound traffic on TCP ports 80 and 443 from the vApp network to the vCD IP address.

Log Management

Location of Log Files

To facilitate troubleshooting, the SecureCloud Runtime Agent and Provisioning Service utilize log files to record runtime and detailed error information. The log files for the SecureCloud Runtime Agent can be found at the following locations:

- Linux:

  ```
  /var/cloud9/logfiles/
  ```

- Windows:

  ```
  C:\Program Files\Trend Micro\SecureCloud\Agent\logfiles
  ```

The log files for the Provisioning Service can be found at the following location:

```
/home/provisioningAgent/logfiles
```

Setting the Log Recording Level

By default, the SecureCloud Runtime Agent installs the software and sets the log level to `INFO` which will log only informational, warning and error messages. It is possible to increase the log-level verbosity in the event of an error such that it is easier to determine the root cause. To do this, edit the file names `c9logger.ini` in the SecureCloud installation folder (`/var/cloud9/c9logger.ini` on Linux, or `C:\Program Files\Trend Micro\SecureCloud\Agent\c9logger.ini` on Windows) named `c9logger.ini` and change the following section:

```
[logger_root]

level=INFO
```

To:

```
[logger_root]

level=DEBUG
```

Save the file and then restart the Runtime Agent service or reboot the machine instance.

Glossary

Account name

A name that uniquely identifies you, or your organization's organization’s account in the Management Server.

Bundling

The process of creating a template image from a running instance in the cloud service provider environment.

Cloned device

A data storage device that was created from another data storage device. The device clone is exactly the same as the originating device and therefore functions the same as the originating device. SecureCloud does not encrypt a device clone since it retains the encryption from the originating, cloned device.

See Also:

- *Adding a Data Storage Device to the Inventory* on page 8-6

Configuration Tool

The SecureCloud Configuration Tool is a the command line-based tool used to configure like what kind of cloud provider you are using and which device(s) you want to attach and mount in the Runtime Agent.

Encryption key

For securing data on the encrypted data storage device, a 128-bit randomly generated key is used for devices that are encrypted and a 256-bit randomly generated key for all internal encryption.

Hypervisor

In virtualization technology, hypervisor is a software program that manages multiple operating systems (or multiple instances of the same operating system) on a single computer system. The hypervisor manages the system's processor, memory, and other resources to allocate what each operating system requires. Hypervisors are designed for a particular processor architecture.

Instance

A running machine image in the cloud service provider environment.

Machine image

A system virtual machine which provides a complete system platform that supports the execution of a complete operating system. SecureCloud supports the Amazon Machine Image (AMI) and Eucalyptus Machine Image (EMI). These machine images are a special type of virtual appliance which is used to instantiate (create) a virtual machine within the cloud service provider’s environment. The machine image serves as the basic unit of deployment for services delivered using the environment of the cloud service provider.

Management Server

The server provides centralized management functionality around machine identity validation, key issue and management, access logs. This server is hosted as SaaS in a multi-tenant service.

Private key and certificate files

Amazon credentials obtained when creating your Amazon account and required by SecureCloud to interact with the Amazon environment.

Provisioning Service

This is a one-time-used tool that encrypts a data storage device and registers the device information with the SecureCloud Management Server for the Amazon, Eucalyptus, and VMware vCloud environments, or private cloud providers.

Runtime agent

This agent is installed inside the production VMs for runtime validation, key access and encrypt/decrypt functionality. It consists of the main three modules: 1) data encryption/decryption module, 2) integrity check module and 3) credential validation and key acquisition module.

SecureCloud Web console

The Web-based user interface to the Management Server.

Index