



SecureCloud[™] 2.0

Private Security for the Public and Private Clouds

SaaS

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.

Copyright © 1996 - 2012 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No. APEM25289/111129

Release Date: February, 2012

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

SecureCloud Documentation	xii
Audience	xii
Document Conventions	xiii

Chapter 1: Introducing SecureCloud

System Requirements	1-2
SecureCloud Runtime Agent Requirements	1-2
Features and Benefits	1-3
New Features	1-5
How SecureCloud Works	1-7
SecureCloud Interaction with the vCloud API	1-9
Basic Components of SecureCloud	1-11

Chapter 2: Using SecureCloud

Registering the SecureCloud Product	2-2
Using the SecureCloud Web Console	2-3
Summary of Operations	2-7

Chapter 3: Understanding Running Instance Information

About Key Status and Virtual Machine Integrity	3-2
Viewing and Changing Machine Image Information	3-3
Viewing Instance and Related Information	3-4

Acting Upon a Pending Key	3-4
---------------------------------	-----

Chapter 4: Managing Policies

About Encryption Key Revocation	4-2
About the Resource Pool	4-3
About the Default Policy	4-3
Scheduling an Integrity Check	4-4
Creating a Policy	4-5
Changing a Policy	4-6
Adding or Removing a Machine Image	4-8
Adding or Removing a Data Storage Device	4-9
Adding or Removing Data Access Rules	4-10
Specifying the Encryption Key Approval Process	4-15
Deleting a Policy	4-16

Chapter 5: Machine Image and Data Storage Device Information

Registering a Machine Image	5-2
Changing Machine Image Information and Viewing Related Information	5-2
Configuring a Data Storage Device	5-3
Specifying Device Configuration Information	5-3
Using Configuration Information from Another Device	5-5
Viewing and Changing Encryption Key Information	5-7
Configuring a RAID Device	5-8
Specifying RAID Device Configuration Information	5-8
Viewing and Changing RAID Device Information	5-9
Changing a Data Storage Device or RAID Device Assignment	5-10
Unconfiguring a Data Storage Device or Device RAID	5-12

Chapter 6: Reports and Logs

Reports	6-2
Creating a Report Template and Generating a Report	6-2
Performing Report Maintenance	6-3
Emailing a Report Notification	6-3
Changing a Report Template	6-4
Deleting a Report Template	6-4
Downloading an Archived Report	6-4
Deleting an Archived Report	6-5
Understanding Generated Reports	6-5
Logs	6-5
Querying Logs	6-6
Understanding Archived Logs	6-6

Chapter 7: Administration

Managing Users in the Web Console	7-1
Adding a New User to the Web Console	7-1
Changing Web Console User Information	7-2
Deleting a Web Console User	7-2
User Roles	7-3
About User Roles	7-3
Viewing User Role Permissions in the Web Console	7-4
Managing Profile Information	7-4
Changing the Log In Password	7-4
Specifying the Time Zone Used for Notifications and Reports	7-5
Web Console Notifications	7-5
Creating a Web Console Notification	7-6
Changing an Existing Web Console Notification	7-7
Deleting a Web Console Notification	7-7
Specifying Deep Security Settings	7-7
Authentication Methods in SecureCloud	7-8
Using Local Authentication	7-8
Product License	7-8

Specifying the Product License Activation Code	7-8
Rotating Amazon Credential Keys	7-9
Data Recovery	7-10
Encrypted Data Backup	7-10
Device Encryption Keys Backup and Site Readiness	7-10
Exporting an Encryption Key to Restore an Encrypted Data Storage Device or RAID	7-10
Exporting the Encryption Key	7-11
Decrypting the Encryption Key File and Mounting the Device with the Key	7-12

Chapter 8: Provisioning for Data Storage Encryption

About the Configuration Tool	8-2
Creating a Data Storage Device in Your Virtualized or Cloud Service Provider Environment	8-3
Creating a Device in Amazon EC2	8-4
Creating a Device in vCloud	8-4
Creating a Data Storage Device in Eucalyptus	8-4
Creating a Device in vSphere	8-5
Native on NFS and iSCSI	8-5
Configuring the Runtime Agent	8-6
Encrypting a Data Storage Device or Device RAID	8-7
Deleting a Data Storage Device From the Inventory	8-8
Deleting a RAID from the Inventory	8-9
Starting the Runtime Agent	8-9
Stopping the Runtime Agent	8-10

Appendix A: Installing and Uninstalling SecureCloud

Installation Summary	A-1
Specifying Application Start Up After Encrypted Device Mount	A-2
Installing the SecureCloud Runtime Agent	A-3

Supported Kernels for Amazon EC2	A-6
Installing the Runtime Agent in a Linux Environment	A-7
Preparing to Install with a Custom Linux Kernel	A-9
Installing the Runtime Agent in a Windows Environment	A-10
Maintenance Install for the Runtime Agent in a Windows Environment	A-12
Starting and Stopping a Dependent Service	A-12
Uninstalling the Runtime Agent	A-13
Uninstalling the Runtime Agent from a Linux Environment	A-13
Uninstalling the Runtime Agent from a Windows Environment ...	A-13
Migrating Data from SecureCloud 1.x to SecureCloud 2.0	A-14
Migrating Data from a Public Cloud	A-14
Migrating Data from a Private Cloud	A-15
Restoring Encrypted Data to Cleat-text Format	A-15
Uninstalling the SecureCloud 1.x Runtime Agent	A-16
Installing the SecureCloud 2.0 Runtime Agent and Provision the Disk	A-17
Copying Clear-text Data to the Newly Provisioned Device	A-17

Appendix B: Frequently Asked Questions

How do I Upgrade from a Trial License?	B-1
How do I Migrate from Beta to Production?	B-2
What Hypervisors are Supported?	B-2
In Which Time Zones are the Logs Saved and Can I Change the Time Zones?	B-2
What Certifications Does SecureCloud Hold?	B-2
How are All Communications Secure?	B-2
How Does Trend Micro Protect My Cloud Service Provider Credentials?	B-3
How Do I Recover a Forgotten Web Console Password?	B-3
What is the Service Availability for SecureCloud?	B-3
What Kind of Encryption Key Security Exists?	B-4

How is SecureCloud Protected From Man-in-the-Middle Attacks?	B-4
Who is Responsible for Lost or Stolen Data?	B-4
How do I Acquire the Installation Log File for Installation Debugging?	B-4
How do I Restore My Device Encryption Key on the Runtime Agent?	B-5

Appendix C: Contact Information and Web-based Resources

Knowledge Base	C-2
TrendEdge	C-2
Contacting Technical Support	C-2
General Contact Information	C-3
TrendLabs	C-3

Appendix D: Basic Troubleshooting Information

Network Configuration and vCloud	D-1
Log Management	D-2
Location of Log Files	D-2
Setting the Log Recording Level	D-2
SSL Configuration and Troubleshooting	D-3

Appendix E: Managing SecureCloud Using RightScale

Possible RightScript Commands	E-2
Installing the Runtime Agent and Provisioning a Data Storage Device	E-3
Uninstalling the Runtime Agent	E-4
Rotating Amazon Credential Keys	E-4

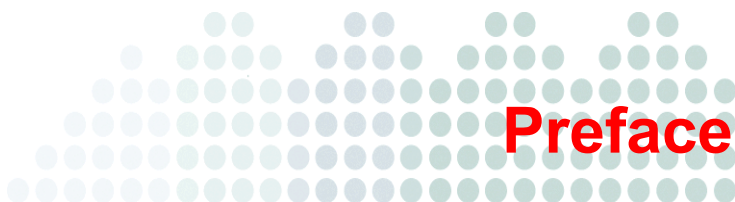
Appendix F: Configuration Tool Scripts

Configuration Tool Commands	F-2
-----------------------------------	-----

Specifying Amazon Credential Keys Rotation	F-7
Updating the Volume List	F-7
Auto-configuring the Runtime Agent	F-7
Performing an Auto Batch Provision of Devices	F-7
Proxy Server Support for the Runtime Agent	F-8
Adding a Proxy Server	F-9
Viewing the Proxy Server Settings	F-10
Testing the Proxy Server Connection	F-10
Removing Proxy Information from the Runtime Agent	F-10

Glossary

Index



Preface

Welcome to the *Trend Micro™ SecureCloud™ Administrator's Guide* for the 2.0 release of SecureCloud SaaS. 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:

- **Quick Reference Guide**—Provides data migration and overview information in a manner that allows for quick and easy access.
- **Online Help**—Provides “how to” information 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**—Provides 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, Quick Reference 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 administrators working in a medium or large enterprise environment. This guide was created based on the assumption that you have in-depth knowledge of networks schemas, including details related to the following:

- Amazon EC2
- Eucalyptus
- VMware vCloud
- vSphere
- Linux
 - CentOS
 - Red Hat Enterprise Linux (RHEL)
 - Ubuntu
- Microsoft Windows Server

- Hosted services
- 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
<i>Italics</i>	References to other documentation
Monospace	Examples, sample command lines, program code, Web URL, file name, and program output
<hr/> Note: <hr/>	Configuration notes
<hr/> Tip: <hr/>	Recommendations

TABLE P-1. Document Conventions (Continued)

CONVENTION	DESCRIPTION
<div><div></div><div>WARNING!</div><div></div></div>	Reminders on actions or configurations that should be avoided



Chapter 1

Introducing SecureCloud

Trend Micro™ SecureCloud provides security for virtualized environments and 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*
- *New Features*
- *How SecureCloud Works*

System Requirements

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

- Microsoft® Internet Explorer 7.0 or 8.0
- Mozilla Firefox 3.x

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

SecureCloud Runtime Agent Requirements

As a SaaS solution, there are only minimal requirements needed to run the SecureCloud Runtime Agent in your cloud service provider's environment. [Table](#) describes the server requirements for the Runtime Agent.

Runtime Agent Requirements for Various Operating Systems

Requirement	Description
Cloud provider	<ul style="list-style-type: none">• Amazon EC2• Eucalyptus 1.6• Eucalyptus 2.0• VMware vCloud 1.0• VMware vCloud 1.5
Virtual Machines	<ul style="list-style-type: none">• vSphere (ESX 4.1)
Instance type	<ul style="list-style-type: none">• Amazon EC2:<ul style="list-style-type: none">- Windows and 64-bit Linux- 32-bit Linux• 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	<ul style="list-style-type: none">• 30MB to install SecureCloud Runtime Agent

Runtime Agent Requirements for Various Operating Systems (Continued)

Requirement	Description
Guest operating system (32- and 64-bit versions)	<ul style="list-style-type: none"> • CentOS 5.4 • CentOS 5.5 • CentOS 5.6 • CentOS 6.0 • Red Hat Enterprise Linux 5.5 • Red Hat Enterprise Linux 6.0 • Ubuntu 9.10 • Ubuntu 10.4 • Ubuntu 10.10 • Ubuntu 11.04 • SUSE Linux Enterprise 11.1 • Windows 7 Professional • Windows 7 Ultimate • Windows Server 2003 R2 Datacenter SP2 • Windows Server 2008 R2 Datacenter SP2 • Windows Server 2008 Datacenter SP2

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 (128, 192 or 256)
- Encrypts and decrypts data in real time, so data at rest and data traversing 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 additional layers of encrypted communication
- Offers central key management as a hosted service within Trend Micro's secure data centers

Scheduled Reporting

SecureCloud enables you to generate reports reoccurring for a specified span of time. Reports are saved to the Management Server so you can download a previously generated report (either one-time or reoccurring) from the Management Server Console.

Support for Cloud Service Provider Plug-ins

SecureCloud enables you to write an plug-in for a Cloud Service Provider (CSP) that is not supported "out of the box." The plug-in is a thin, translation layer which communicates with the API of the CSP and presents a uniform interface between CSPs. The CSP-specific implementation will handle all logic specific to the CSP such that the rest of the Runtime Agent is CSP agnostic.

Support for Virtual Machine and Bare Metal Plugins

You can use a bare-metal (native) plugin to encrypt storage devices in a physical, as well as a vSphere environment. Using a native plugin, SecureCloud can support IDE, NFS, SCSI and iSCSI storage devices.

Simplistic Data Storage Device Provisioning

The SecureCloud Runtime Agent provides the Configuration Tool that enables you to specify your Cloud Service Provider (CSP) or load a new cloud service provider plugin that you have created, and save the configuration file for later use. From the SecureCloud Web Console you can easily provision devices for encryption.

Deep Security Integration

Deep Security Manager (DSM) is a powerful, centralized web-based management system that allows security administrators to create and manage comprehensive security policies and track threats and preventive actions taken in response to them. DSM integrates with different aspects of the datacenter including: VMware vCenter, Microsoft Active Directory and has a Web services API for integration with SecureCloud.

DSM provides additional integrity checking of your environment, thus ensuring the integrity is safe to access sensitive, encrypted information. Should the environment integrity change based on a bad file being found, SecureCloud can revoke the encryption key, thus protecting the sensitive data.

FIPS 140-2 Certified

SecureCloud utilizes the new Trend Micro Encryption Module—a FIPS 140-2 certified crypto engine, providing Full Disk Encryption (FDE) to your physical, virtual or cloud environment for SCSI, iSCSI, IDE and NFS storage devices.

IPv6 Support

SecureCloud supports IPv6, an Internet layer protocol for packet-switched internetworking. This protocol provides end-to-end datagram transmission across multiple IP networks.

New Features

Deep Security Integration

See *Features and Benefits* on page 1-3.

FIPS 140-2 Certified

See *Features and Benefits* on page 1-3.

IPv6 Support

See *Features and Benefits* on page 1-3.

Device RAID Support

SecureCloud supports the Redundant Array of Inexpensive Disks (RAID) for the RAID 0 level. With this support, you can have multiple encrypted devices in a RAID, each controlled by a separate encryption key.

Amazon Credential Keys Rotation

In an effort to optimize security, Amazon allows you to create a new pair of credential keys (access key ID and secret access key). While Amazon does not enforce the use of this key pair, it does recommend that you replace your old key pair with a new one every 90 days. In doing so, SecureCloud provides additional security and clearly separates the duties between the Cloud Service Provider (CSP) administrator and your SecureCloud administrator.

RightScale Script Enhancements

The enhanced RightScale scripts give you the ability to separate the Runtime Agent installation and device provisioning operations. These no longer have to be done as one operation. The enhanced RightScale script will also automatically detect the guest operating system for Runtime Agent installation. Devices can be added and removed from your environment by replacing the device list. Only devices on the list will be part of your environment.

The enhanced RightScale scripts also support credential key rotation for Amazon.

More Guest OS Support

SecureCloud supports certain versions of the CentOS, Ubuntu, SUSE, and Windows Server guest operating systems to implement an extra layer of security. Runtime Agents running on these operating system can employ a crypto engine which encrypts endpoints with coverage that is FIPS 140-2 certified.

Runtime Proxy Server Support

SecureCloud supports the use of a proxy server with the Runtime Agent. The proxy server connection can either be authenticated or unauthenticated. SecureCloud also supports both the HTTP and HTTPS protocols for a proxy server.

How SecureCloud Works

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

When the virtual 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. The SecureCloud Key Manager responds with a request for information pertaining to the environment which it will use to evaluate against policies that have been created for the specific device. For example, a policy can consist of rules to check that the virtual machine is in compliance to the IT policy regarding what network services should be enabled or pattern file version, and location of where the virtual machine is running to name a few. 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, and ensures that the environment is safe to release the encryption key into based on the policy criteria.

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

SecureCloud: Enterprise-controlled Data Protection for the Cloud

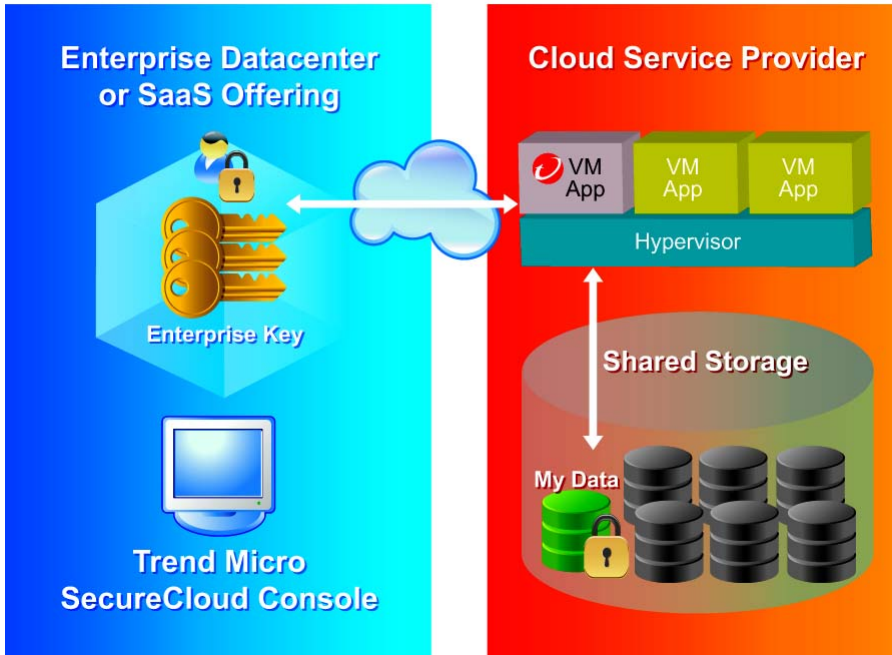


FIGURE 1-1. How SecureCloud SaaS functions

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 operating system patch, and/or the latest Trend Micro engine and pattern file. In addition, you can get report and audit information about your account using the portal.

SecureCloud Interaction with the vCloud API

The vCloud API is used by SecureCloud to determine the identity of a machine image in the vCloud environment. The Configuration Tool uses the vCloud API to learn what data storage devices in the vCloud environment are available for encryption.

The SecureCloud Runtime Agent uses the vCloud API to learn the identity and integrity of the vCloud machine image. This information is retrieved from the vCloud API and sent to the Management Server where the user can either grant or deny an encryption key to the requesting machine image, based on the identity and integrity credentials of the vCloud machine image.

SecureCloud for vCloud: Enterprise-controlled Data Protection for the Cloud

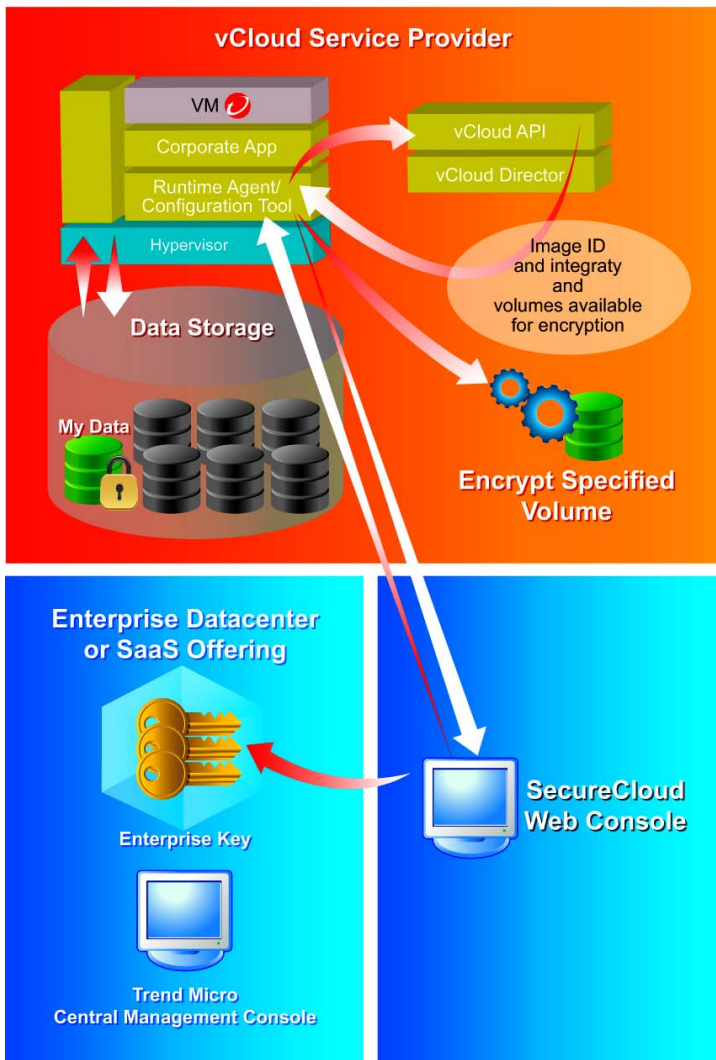


FIGURE 1-2. How SecureCloud functions in the vCloud Environment

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 provides the following functionality:

- Checks the integrity of the cloud environment against the rules set in the SecureCloud policy for the specific virtual machine and device
- Mounts a configured encrypted data storage device
- Establishes an SSL session with the SecureCloud key manager
- Establishes a private session with a separate session key over SSL. This is performed in case the SSL connection is compromised. In doing so, even if the SSL session is compromised the communication between the agent and key server is still encrypted.
- Authenticates the communication between the Runtime Agent and Key Manager using Message Authentication Code.
- Creates and tears down an encrypted area on the virtual machine storage in order to store the cloud service provider's credentials

Configuration Tool

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 and cloud service provider plugin
- Cloud service provider's credentials (includes the rotation of credential keys for Amazon environment)
- SecureCloud account ID
- Web Service API URL
- Device information for the running machine instance
- Device encryption

Management Server

Trend Micro hosts the SecureCloud Management Server with multi-tenant capability. There is no enterprise console option for SecureCloud SaaS. 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 Roles](#) on page 7-3).



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. You will need to obtain a trial license. Complete a trial form by going to the Trend Micro website and completing a trial form for SecureCloud Hosted Services.

SecureCloud trial form:

<http://forms.trendmicro.com/index.php?dom=us&productID=125>

Once you have completed the trial form, you will receive an Activation Code. You will need this trial activation code later in order for SecureCloud Management Server to generate the encryption keys needed.

Procedure:

1. Go to <https://beta.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-3.

Using the SecureCloud Web Console

Use the following URL to access the SecureCloud Web Console:

`https://console.securecloud.com`

The Web Console consists of a main menu with a viewing area to the right of this menu. The main menu is comprised of six main menu items: Running Instances, Policies, Inventory, Reports, Logs, and Administration. These are described in [Table 2-2](#) along with any associated sub-menu items.

The amount of functionality available to a user in the SecureCloud Web Console is based on user roles. The possible user roles are administrator, data analyst, security administrator, auditor, and key approver, with administrator having the most privileges and data analyst having the least (see [User Roles](#) on page 7-3).

TABLE 2-2. Menu items in the Web Console

MENU ITEM	DESCRIPTION	USAGE
Running Instances		
Running Instances	Use to 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 being used to store the secure data. Also use to grant approval for a pending device and view the integrity status of the virtual machine images and the date when device access was requested	See Chapter 3, Understanding Running Instance Information .
Policies		
Policies	Use to create a policy and then add machine images, devices, and rules to the policy. Also use to change or delete an existing policy.	See Chapter 4, Managing Policies .
Inventory		

TABLE 2-2. Menu items in the Web Console (Continued)

MENU ITEM	DESCRIPTION	USAGE
Images	Use to view available machine images and related information.	See Changing Machine Image Information and Viewing Related Information on page 5-2.
Devices	Use to view and change data storage device information. Also use to add, change, and view device RAID information.	<ul style="list-style-type: none"> • See Configuring a Data Storage Device on page 5-3. • See Configuring a RAID Device on page 5-8.
Reports		
Templates	Use to create a new report template or modify or delete an existing one.	See Creating a Report Template and Generating a Report on page 6-2.
Archived	Use to download an archived report or delete an archived report.	<ul style="list-style-type: none"> • See Downloading an Archived Report on page 6-4. • See Deleting an Archived Report on page 6-5.
Logs		
Query	Use to query logs based on date range and log event types.	See Querying Logs on page 6-6.
Archived	Use to view an archived log or to download an archived log as a CSV file.	See Understanding Archived Logs on page 6-6.
Administration		

TABLE 2-2. Menu items in the Web Console (Continued)

MENU ITEM	DESCRIPTION	USAGE
User Management	Use to view account names and IDs. Also, use to manage users and learn about the different user roles and how many users are assigned to each role.	<ul style="list-style-type: none">• See <i>Managing Users in the Web Console</i> on page 7-1.• See <i>User Roles</i> on page 7-3.
Notifications	Use to view, add, change, or delete an email notification.	<ul style="list-style-type: none">• See <i>Creating a Web Console Notification</i> on page 7-6.• See <i>Changing an Existing Web Console Notification</i> on page 7-7.• See <i>Deleting a Web Console Notification</i> on page 7-7.
Deep Security Settings	Use to specify the Deep Security Manager (DSM) settings, which are necessary to establish a connection between SecureCloud and the DSM server.	See <i>Specifying Deep Security Settings</i> on page 7-7.

TABLE 2-2. Menu items in the Web Console (Continued)

MENU ITEM	DESCRIPTION	USAGE
Change Password	Use to change the current user's password, necessary to access the Web Console.	See <i>Changing the Log In Password</i> on page 7-4.
Time Information	Use to specify a time zone used in the time stamping of notifications and reports.	See <i>Specifying the Time Zone Used for Notifications and Reports</i> on page 7-5.
Product License	Use to specify the product license activation code.	See <i>Product License</i> on page 7-8.

Summary of Operations

Beginning with your Cloud Service Provider (CSP), 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.
See *Registering the SecureCloud Product* on page 2-2.

Step 2. Create a data storage device.

You create a data storage device within your CSP. You can either create a new device or clone an existing one. Once this is done and the inventory has been uploaded to SecureCloud, the device will be available in the SecureCloud Web Console (see *Creating a Data Storage Device in Your Virtualized or Cloud Service Provider Environment* on page 8-3 and your CSP documentation).
If you choose, you can manage device operations from your RightScale account (see your RightScale documentation).

Once you have created data storage devices in your CSP, you can create a RAID device, if you choose (see [Configuring a RAID Device](#) on page 5-8).

Step 3. Prepare the virtual machine image.

a. Instantiate a virtual machine.

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. If you choose, you can create a machine image from your RightScale account.

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

See your RightScale documentation to create a machine image.

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

b. 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.

SecureCloud enables you to setup a proxy server for the Runtime Agent (see [Proxy Server Support for the Runtime Agent](#) on page F-8).

Step 4. Encrypt and register the data storage device with SecureCloud.

This is done by the Configuration Tool. From the SecureCloud Web Console, the application uses the Configuration Tool 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. If you choose, you can encrypt and register a device from your RightScale account.

See [Encrypting a Data Storage Device or Device RAID](#) on page 8-7.

See your RightScale documentation for device encryption and registration.

Step 5. Bundle the machine image to be used as a template.

If required by your CSP, bundle the machine image to save the configured machine image as a template for creating instances or other machine images. (This is not required for a vCloud environment.)

See your CSP documentation to bundle the machine image.

Step 6. 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 4-5.

Specify Deep Security settings first, if you plan to use a Deep Security rule in a policy (see [Specifying Deep Security Settings](#) on page 7-7).

Step 7. 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 to the Web Console](#) on page 7-1 and [User Roles](#) on page 7-3.

Step 8. 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 Web Console Notification](#) on page 7-6.

Step 9. 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 [Specifying Device Configuration Information](#) on page 5-3 for data storage device and instance status.

Step 10. 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 11. 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), usage information (instance compute time) and audit information (who did what and when).

See [Reports](#) on page 6-2.

Step 12. 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 6-5.

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 being used to store the secure data.

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 considered missing and subsequently 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 information from the machine instance requesting a key to ensure that the instance meets the policy criteria set by the administrator.

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

- Pending
- Approved
- Delivered
- Denied
- Revoking
- Revoked

SecureCloud™ Logged in as: **John Doe** Log Off | Help

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 device.

30 Instances 4 Key(s) Pending 26 Key(s) Approved

Key Status	Integrity	Device	Images	Instance	Provider	Policy	Requested
Pending	Bad	Device 1	img-1234ddiw	i-51846c3a	Amazon EC2	Policy 1	1 second ago
Pending	Unknown	Device 11	img-1234ddiw	i-51846c3a	Amazon EC2	Policy 1	12 minutes ago
Pending	Unknown	Device 41	img-1234ddiw	i-51846c3a	Amazon EC2	Policy 1	35 minutes ago
Pending	Unknown	Device 3	img-6877dd3t	i-61146c3b	Eucalyptus	Policy 3	2 hours ago
Approved	Good	Device 6	img-1234ddiw	i-23545c3f	Elaster	Policy 6	17 Sep 2011 22:21:38 PST
Approved	Good	Device 15	img-1345ab7p	i-84523ctb	Elaster	Policy 7	31 Aug 2011 22:21:38 PST
Approved	Good	Device 2	img-1234ddiw	i-35441ctv	Amazon EC2	Policy 11	19 Aug 2011 22:21:38 PST
Approved	Good	Device 4	img-1345ab7p	i-11143ctn	VCloud	Policy 12	02 Jul 2011 22:21:38 PST
Approved	Good	Device 12	img-9546ab7b	i-98656c2k	Amazon EC2	Policy 7	01 Jul 2011 22:21:38 PST
Approved	Good	Device 8	img-7546ab2n	i-53246c9d	Eucalyptus	Policy 5	30 Jun 2011 22:21:38 PST

1-10 of 30 1 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 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
- Failed

The "Unknown" rating can mean that a data storage device with a key request status of "Pending" or "Denied" is not yet associated with a machine image, is not yet in a policy, or that the policy to which the device belongs has no rules associated with it.

The "Failed" rating indicates that the results from the scheduled Integrity Check do not match the conditions specified by the 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 5-2 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 change 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 [Specifying Device Configuration Information](#) on page 5-3 and [Creating a Policy](#) on page 4-5).
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 conditions 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 KEY STATUS LINK > KEY REQUEST PAGE

1. Click the desired "Pending" key status link.
 - If the integrity of the cloud environment (instance) is "Unknown", then the "Key Request (Unknown)" page opens. In this page, assign the data storage device to a policy by making a selection from the drop-down list under "Assign to Policy". Click **Submit**. The "Key Request (Pending)" page opens.
If the environment integrity is "Unknown", SecureCloud does not know which policy should be used to evaluate the environment integrity. After associating the device to a policy, SecureCloud will use that policy to verify the environment integrity.
 - If the integrity of the cloud environment is "Bad", then the "Key Request (Pending)" page opens.
The "Key Request (Pending)" page lists information by rules. This page summarizes how many rules failed and passed and how many rules are informational. (You can filter on failed, passed, or informational information or choose to show all this information.) Informational rules are the set of rules

that a system administrator deems not necessary for key approval criteria, but they can provide useful information.

SecureCloud™ Logged in as: John Doe Log Off Help

Running Instances

- Policies
- Inventory
- Reports
- Logs
- Administration


Key Request

Running Instances > Key Request (pending)

Here you can view the status of the key approval rules and filter these rules by status. You can also approve or deny the key request.

3 Rule(s) Failed Show 2 Rule(s) Passed Show 10 Rule(s) Informational Show

RAID 0
Striping



RAID Array ID: Tim's RAID Array

Description: Blah blah blah blah blah

Mount point: /root/test/

Type: RAID 0

Platform: Linux

Devices: vol-b8e66dca, vol-f2a56vaa

Write access: Read only

Image: ami-153asd315a

Key size: 128 Bits

Key Values

Rule	Condition	Actual Value	Status
Failed (3)			
1 Device Mount Point	(= /mnt/disk1/volume2/path3/folder4/file5/1234567890987654321)	/mnt/disk1/volume2/path3/folder4/file5/aaaaaaaaaaaa	Failed
2 Request Source IP Address	(>= 1.1.1.1) AND (<= 1.1.1.200)	1.1.1.201	Failed
3 Instance Location	US AND EU	CDC	Failed
Informational (10)			
1 Device Access Type		xxx	Informational
2 Key Request Date		xxxx	Informational
3 Instance First Seen		xx	Informational
4 Instance User Data		xxx	Informational
5 OSSEC Version		xxx	Informational
6 Security Softwares		Has Deep Security	Informational
7 Trend Micro Virus Scan Engine		xx	Informational
8 Trend Micro Virus Scan Pattern		xx	Informational
9 Deep Security Status		Status = Green Firewall = Not capable	Informational
10 Guest OS Information		xx	Informational
11 Network Services		xx	Informational

Approve Deny Cancel

FIGURE 3-2. "Key Request" page

- To filter by rules that failed, passed, or are simply informational, select the appropriate check box(es) at the top of the window.
- Click the appropriate button to either approve, deny, or cancel the pending key request.

You can click on the status link in the "Running Instances" page to view the key request information again.

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



Chapter 4

Managing Policies

SecureCloud stores un-allocated 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. A policy can also include the additional integrity checking of the Deep Security Manager (DSM) to ensure the integrity of your environment is safe for accessing sensitive, encrypted information.

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

About Encryption Key Revocation

Without scheduled integrity checking enabled, SecureCloud evaluates a machine image instance based on the policy rules for the device in question. If the instance meets the criteria of the device policy rules, then SecureCloud permits the instance to access the device. If the instance fails to meet the criteria specified by the device policy rules, then SecureCloud denies device access to the requesting instance. In both of these cases, SecureCloud evaluates the instance only once during the instance session. If the instance is later in compliance with the device policy rules, the instance will not have another opportunity to request the device key.

With scheduled integrity checking enabled in a device policy, SecureCloud works with the Integrity Check Module (ICM) of the Runtime Agent to evaluate an instance multiple times during the entire instance session. Therefore, if SecureCloud revokes an encryption key, you have an opportunity to make the instance compliant with the policy rules and receive the encryption key back. But even before SecureCloud revokes the encryption key of an offending instance, the application can provide a grace period where the key is not revoked for a time and you are warned that the instance is in violation of the device policy rules.

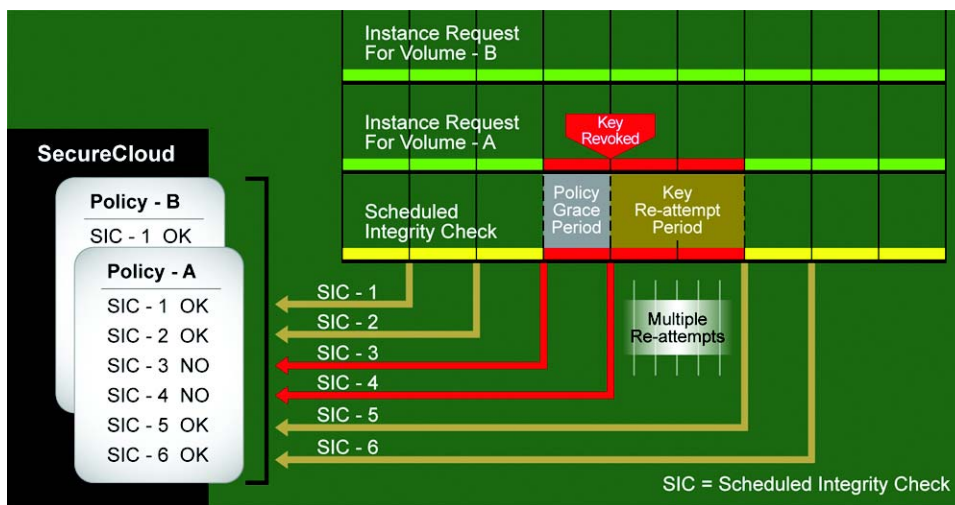


FIGURE 4-3. Process showing key revocation and re-issuing

Scheduled integrity checks can be done either daily or weekly and has the following benefits:

- Enforces the integrity of the instance through out the life cycle to the instance
- Provides the option to revoke the key if the VM instance/cloud environment becomes in violation of the policy rules
- Provide the option to reattempt to issue the key if the violating offense of the instance has been corrected

See Also:

- *[Scheduling an Integrity Check](#)* on page 4-4

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 that the requested device is in use by another instance. See *[Creating a Policy](#)* on page 4-5 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.

Note: Resource pooling is not applicable for vCloud and native machine environment 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 list. The default policy cannot be deleted. It has a default action of "manual approve" for key-request approval, that can be changed after the default policy rules have been specified. Any policy that does not have any rules specified will have action of "manual approve".

To remove a device from the default policy, you must add the device or image to a new or existing policy (see [Creating a Policy](#) on page 4-5 and [Changing a Policy](#) on page 4-6).

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

Scheduling an Integrity Check

An administrator can schedule—on a recurring basis, when a cloud environment is going to be evaluated against policy rules. SecureCloud employs the ICM of the Runtime Agent to evaluate the cloud environment in question. The frequency of the evaluation can be at a specified time each day, or on a specified day and time each week.

As part of the scheduled integrity checking, SecureCloud can be configured to revoke encryption keys to the data storage device if the conditions of the virtual machine have changed and are in conflict with the policy rules. For example, if network service for port 80 is not allowed by the specified rules and the device encryption key was delivered at Runtime Agent start up to a virtual machine that has port 80 open, then SecureCloud will revoke the device encryption key.

If SecureCloud finds a machine image to be compromised or out of compliance based on policy rules, the administrator can set the Runtime Agent to do one of the following:

- Issue a notification email describing the offending condition
- Issue a notification email describing the offending condition and revoke the encryption key within a configurable period (minutes, hours) from the machine image, thereby protecting the data

Note: Setting the action to revoke an encryption key from a running instance can have dire results and possible loss or corruption of data being written to the device by the writing application.

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | POLICIES > POLICIES PAGE

1. Click the **Scheduled Integrity Check Settings** link.
2. From the "Scheduled Integrity Check" page, specify in the "Schedule" area the desired integrity check frequency.
3. From the "Period for Key Request Attempt(s)" area, specify how long SecureCloud should make attempts to re-grant a revoked encryption key.
This feature is implemented if you choose to enable scheduled integrity checking in a policy (see [Specifying the Encryption Key Approval Process](#) on page 4-15).
4. Click **Save**.

Creating a Policy

To create a policy, you need to complete five steps. These steps include defining the policy name, specifying machine image(s) and devices associated with the policy, defining rules for key request approval, and specify the action to be taken if selected image(s) and/or device(s) meets or fails to meet the specified rules.

Prerequisite:

Specify Deep Security settings if you plan to use a Deep Security rule in a policy (see [Specifying Deep Security Settings](#) on page 7-7).

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | POLICIES > POLICIES PAGE

1. Click **Add Policy**.

The Policy page displays the first step of the five-step procedure.

From "Step 1: Define Policy Name" view:

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

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

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 4-3.

3. Click **Next**.

From "Step 2: Select Image(s)" view:

4. Add a machine image or images to the policy and then click **Next**.
Using the search field, you can quickly locate an image.

From "Step 3: Select Device(s)" view:

5. Add a device or devices to the policy and then click **Next**.
Using the search field, you can quickly locate a device.

From "Step 4: Define Rule(s)" view:

6. Add a rule to the policy and then click **Next**.
See *[Adding or Removing Data Access Rules](#)* on page 4-10 starting with Step 2. The graphic in this section illustrates an existing policy, but it is still applicable for a new policy.

From Step 5: Define Action view:

7. Specify the encryption key approval process.
See *[Specifying the Encryption Key Approval Process](#)* on page 4-15 starting with Step 2.
8. Click **Finish** 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.

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](#)*.

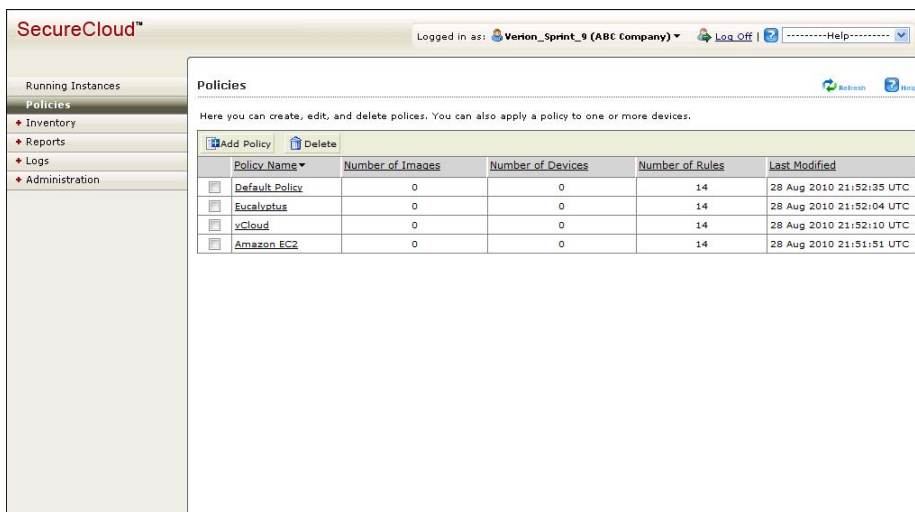


FIGURE 4-4. "Policies" page showing existing policies

2. From the "Policy Information" area of the "Policies > Edit Policy" page, access the appropriate fields to make any changes to 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 4-8.
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 4-9.
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 Data Access Rules* on page 4-10.
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 4-15.
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.

Adding or Removing a Machine Image

Procedure:

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

- 1. Click the **Images** tab.

See *Figure 4-5*.

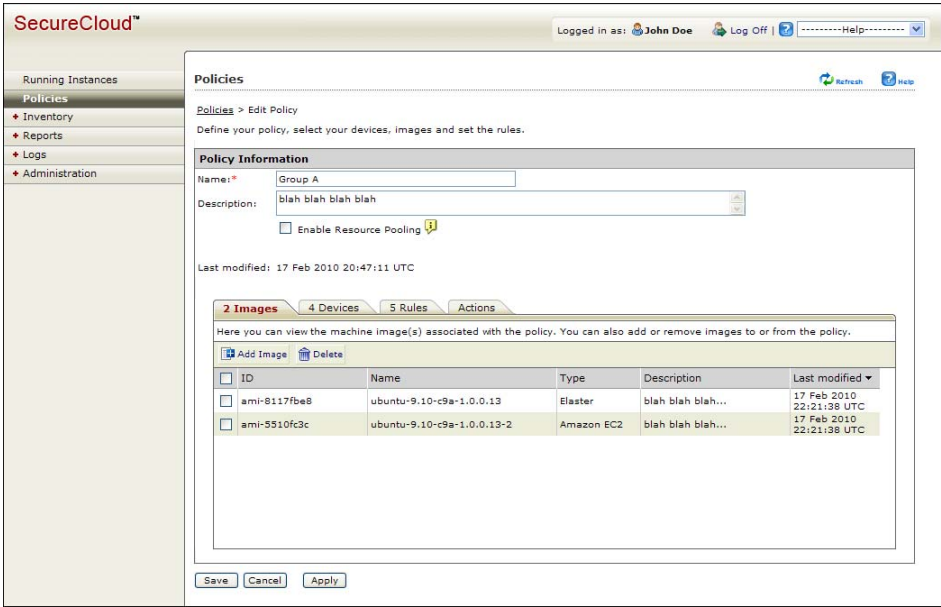


FIGURE 4-5. "Edit Policies" page displaying tabs

To add a machine image:

- Click **Add Image**.
- From the Available Image(s) dialog box, select the image(s) to add to the policy.
All machine images from your cloud service provider that are registered with SecureCloud are listed here. Those already in this policy are checked while all others are not.

- Click **Save** to add the new image(s) to the policy and return to the "Edit Policy" page.

To delete a machine image:

- Select the desired image(s).
 - Click **Delete**.
2. Click **Save** to save the policy and return to the "Policy" page.
Click **Apply** to apply changes and continue working in the "Edit Policy" page.

Adding or Removing a Data Storage Device

Procedure:

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

1. Click the **Devices** tab.

See [Figure 4-5](#).

To add a data storage device:

- Click **Add Device**.
- From the Available Device(s) dialog box, select the device(s) to add to the policy.
All data storage devices from your cloud service provider that are registered with SecureCloud are listed here. Those already in this policy are checked while all others are not.
- Click **Save** to add the new device(s) to the policy and return to the "Edit Policy" page.

To delete a data storage device:

- Select the desired data storage device(s).
 - Click **Delete**.
2. Click **Save** to save the policy and return to the "Policy" page.
Click **Apply** to apply changes and continue working in the "Edit Policy" page.

Adding or Removing Data Access 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 cloud environment checks. This criteria is expressed in SecureCloud as *rules*.

SecureCloud supports advanced policy fields where Boolean operators and compound rules are used. SecureCloud uses a set of basic and advanced rules that are evaluated against a subset of criteria to determine if the cloud environment is safe enough to receive the encryption key.

The following are the possible data types you can use in policy rules:

- String
- Number
- IP address
- IP address range
- Date

Procedure:

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

1. Click the **Rules** tab.

See [Figure 4-5](#).

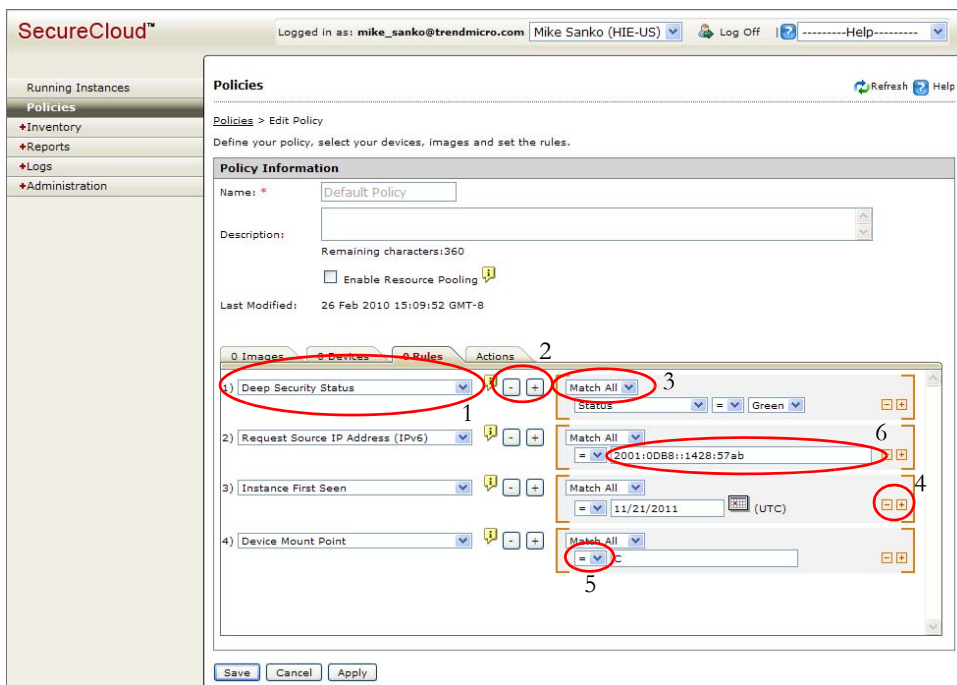


FIGURE 4-6. "Edit Policy" page showing the Rules tab

2. Specify the rules required to access an encrypted data storage device.
See [Figure 4-6](#) to complete the following steps.
 - a. Select the desired rule from the drop-down (see item-1).
 - b. For multiple conditions, specify if all or any of the conditions should be met by the requesting machine image (see item-3).

Since the "Trend Micro Software", "Trend Micro Virus Scan Engine", and "Trend Micro Virus Scan Pattern" rules do not require multiple conditions, the match drop-down list is not necessary.

For the "Device Access Type" rule you can only specify "Read Only" or "Read/Write", which is provided by a single condition. With only a single condition, the match drop-down list is not necessary.

- c. Specify the operator for the rule (see item-5).
- d. Specify the machine instance conditions for the rule (see item-6).

See [Table 4-3](#) for the possible encryption key approval rules.

TABLE 4-3. Rule information for encryption key approval

RULE	DESCRIPTION	EXAMPLE	MULTIPLE CONDITIONS
Deep Security Status	<p>The status of the key-requesting environment as determined by the Deep Security Management (DSM).</p> <p>Note: Should the environment integrity change based on a bad file being found, SecureCloud can revoke the encryption key, thus protecting the sensitive data.</p>	<ul style="list-style-type: none"> - Anti-Malware - Web reputation - Firewall - DPI - Integrity monitoring - Log inspection - Status 	No
Device Access Type	The requested access type, either read/write or read-only	read-only or read/write	Yes
Device Mount Point	The mounting point for the data storage device if keys are approved.	/mnt/secure or X	Yes
Guest OS Information	Operating system and architecture used by the machine image to run the Runtime Agent.	<p>OS: Linux or Windows</p> <p>Architecture: 32 bit or 64 bit</p>	Yes
Key Request Date	Date the key request was received.		Yes

TABLE 4-3. Rule information for encryption key approval (Continued)

RULE	DESCRIPTION	EXAMPLE	MULTIPLE CONDITIONS
Instance Last Seen	Date when SecureCloud last processed any data related to an instance. Based on this timestamp, SecureCloud can determine if the time period is too great to grant the instance encryption keys.		Yes
Instance User Data	Data packet provided to the instance at start up.	DataKey=MySecret-Key	Yes
Instance Location	Location of the server farm running the machine instance.	Us-east-1c	Yes
Network Services	Listening ports on the system running the SecureCloud Runtime Agent, both TCP and UDP ports are included.	80, 25, or 8080	Yes
OSSEC Version	The version of OSSEC that is presented in the machine instance.	2.5.1	Yes
Request Source IP Address (IPv4)	IP address the key request originates from.	192.168.1.1 -or- 192.168.0.0 /16	Yes

TABLE 4-3. Rule information for encryption key approval (Continued)

RULE	DESCRIPTION	EXAMPLE	MULTIPLE CONDITIONS
Request Source IP Address (IPv6)	IP address the key request originates from.	2001:0DB8: :1428:57ab - or - 2001:0DB8: :1428:57ab/ 96	Yes
Trend Micro Software	The Trend Micro security software installed on the machine instance.	Office Scan	No
Trend Micro Virus Scan Engine Version	The version of the Trend Micro virus scan engine running in your machine instance.	9.180.1104	No
Trend Micro Virus Scan Pattern Version	The version of the Trend Micro virus scan pattern running in your machine instance.	7.753.00	No

- e. To specify another machine instance condition for the rule, click the plus button (see item-4).

To remove a machine instance condition for a rule, click the minus button (see item-4).

- f. To add another rule, click the plus button (see item-2) and then repeat Step a through Step e.

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.

Specifying the Encryption Key Approval Process

SecureCloud provides an encryption and decryption key to a virtual machine image after its information has been evaluated against the policy rules. 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:

- Auto approve (immediately)
- Auto approval (within a certain period of time)
- Manual approval
- Deny

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.

As part of the device key request, the Runtime Agent sends the instance identity and integrity data to the Management Server. The Management Server then validates the data against the policies to determine whether the request has to be approved or not (see [Table 4-3](#)).

Procedure:

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

1. Click the **Actions** tab.

If there are no rules configured in a policy, the key approval action is set to Manual Approve. To change the key approval action, specify one or more rules in the policy.

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 request 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" from the **If all rules match** drop-down list, SecureCloud enables you to specify a time when automatic approval will occur if no manual approval is taken.

3. To enable scheduled integrity checking, select the check box by the same name.
With this featured enabled, scheduled integrity checking will be routinely performed on the cloud environment (see [Scheduling an Integrity Check](#) on page 4-4).
From the "Action Taken During Scheduled Integrity Checking" area, specify the action for if a rule fails. Complete the **Postpone revoke for** information to specify the amount of time that can pass before SecureCloud revokes the key. This can be thought of as a "grace period."

Note: If you select **Revoke encryption key** for the **If one or more rule fails** drop-down list and do not select the **Postpone revoke for** check box, the encryption key will be revoked immediately upon policy violation.

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.

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 images must belong to at least one policy and each device must belong to 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*
- *Changing Machine Image Information and Viewing Related Information*
- *Configuring a RAID Device*
- *Changing a Data Storage Device or RAID Device Assignment*
- *Configuring a Data Storage Device*
- *Unconfiguring a Data Storage Device or Device RAID*

Registering a Machine Image

After installing the Runtime Agent in the machine image, you need to register the machine image with the SecureCloud Management Server in order to see the machine 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.

Cloud credentials are stored in encrypted form in the image. The credentials keys are stored in the SecureCloud Management Server.

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 3-4).

Configuring a Data Storage Device

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

Specifying Device Configuration Information

If you did not wait for provisioning to complete when running the Configuration Tool, you will not be able to encrypt the device from the Web Console, but you can still configure the device.

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

This section describes how to do the following:

- Specify device information
- View instance details
- Specify the machine image to which to mount
- View policy information associated with the device

Prerequisites:

- Create a data storage device within the cloud provider (see [Creating a Data Storage Device in Your Virtualized or Cloud Service Provider Environment](#) on page 8-3).
- Configure the Runtime Agent in order to publish the data storage device in your CSP environment.

With the **update inventory** option set to "yes", configuring the Runtime Agent will make the devices in your CSP environment available in SecureCloud (see [Configuring the Runtime Agent](#) on page 8-6).

Procedure:

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

1. Click the link of the desired device with a "Not Configured" status.
2. From the "Device Information" area of the "Edit > Device" page, specify any desired information.

Access the appropriate fields to specify the device name and description. Your Cloud Service Provider (CSP) automatically generated the device identity and device name.

Information is any further information about the devices which has been sent from the Configuration Tool and depends on the cloud server provider plugin.

The **Platform/file system** is the operating system the device will be used by. The file name portion is the file system type by which you wish to format the device. SecureCloud supports the following file systems: Windows: FAT32 and NTFS; Linux: EXT3 and XFS.

The **mount point** is the drive letter you map to the data storage device.

The following are the possible device statuses:

- **Not configured** — Not currently in use and not yet encrypted. Essential configuration information such as operating system, file system, and mount point have not yet been specified.
- **Configured** — Attached to an instance but the encryption key has not yet been given to an application in order to access the encrypted data. Essential configuration information such as operating system, file system, and mount point have been specified.
- **Encryption pending** — Configured and attached to a virtual machine instance. SecureCloud is about to pass an application the device encryption key pending the validation of the application against the policy rules.
- **Encrypting** — Configured and attached to a virtual machine instance and SecureCloud is in the process of encrypting the requested data storage device.
- **Encrypted** — Configured, attached, encrypted and now ready to be accessed by the requesting instance of the machine image.
- **In-use** — Configured, attached, encrypted and being accessed by the requesting instance of the machine image.
- **Encryption error** — Configured and attached to a virtual machine instance and SecureCloud has encountered a problem while encrypting the data storage device.
- **Undetected** — Not available to the machine image instance and therefore no longer a part of the inventory in SecureCloud. (This status only applies to a data storage device, and not to a RAID.)

- **Device Missing** — Some RAID devices have the "Undetected" status. (This status only applies to a RAID, and not to a simple data storage device.)
3. From the "Instance(s)" area, click the link of any desired instance to see complete instance details.
 4. From the "Image" area, specify the machine image to which to mount the device.

Note: This step only applies to Amazon and Eucalyptus. These cloud server providers does not assign a default machine image to a device.

For vCloud and vSphere, the device is attached to a virtual machine and therefore has a default assignment which cannot be changed.

- Choose the desired machine image from the drop-down list in the "Image Identity" column.

A device must have the "Encrypted" status in order to be re-mapped to a different machine image (see [Changing a Data Storage Device or RAID Device Assignment](#) on page 5-10).

A device with a "Not Configured" status must be configured in order to be Encrypted.

Note: The actions available (encrypt, export, and delete) are only available for valid selections. For example, the **Encrypt** button will not be available for a "Not Configured" device.

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

See Chapter 4, [Managing Policies](#).

Using Configuration Information from Another Device

When you clone a device in your CSP environment, 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 encrypted device. Refer to your cloud service provider documentation for complete details.

Note: After cloning the device, the inventory should be re-published to SecureCloud using Configuration Tool.

- Run the Configuration Tool to report available data storage devices and machine images (see [Configuring the Runtime Agent](#) on page 8-6).

Procedure:

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

1. From the bottom of the page, click **Copy Configuration from Another Device**.
2. From the "Copying Device Configuration" page, select the desired device and then click **Copy**.

The "Devices - Edit device" page is populated with information from the selected device.

Only a device that has encryption key information can be the clone source.

3. If you are not satisfied with the machine image to which the source device is mounted, you can assign the device a different machine image.

See [Changing a Data Storage Device or RAID Device Assignment](#) on page 5-10.

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

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

Viewing and Changing Encryption Key Information

Procedure:

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

1. 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	Allows for 128, 192, and 256-bit encryption. Note: The key size is 256 bits if Key Server is used for encryption key storage.
Mode	The mode of operation for the AES cipher is Cipher Block Chaining (CBC).
Key management type	The key management type is the Trend Micro Encryption Module.
Hash	sha1 is always used. In cryptography, secure hash algorithm (sha1) is a cryptographic hash function.
Stored On	The encryption key location can be either SecureCloud Server or Key Server.

2. Click **Save** to save changes and return to the "Devices" page.
Click **Apply** to apply changes and continue working in the "Edit Device" page.

Configuring a RAID Device

From the "Devices" page, you can add, change, and view device RAID information. Data storage devices in a RAID are added or removed from SecureCloud in your Cloud Service Provider (CSP) environment. See your CSP documentation for details.

Note: A device RAID cannot be configured from RightScale.

Table 5-4 describes the disk limitations when creating a dynamic disk in Windows. For additional information on RAID storage limits, see the posting at the following Microsoft location:

[http://technet.microsoft.com/en-us/library/cc773268\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc773268(WS.10).aspx)

TABLE 5-4. Dynamic disk limitations in Windows

STORAGE CAPABILITIES	DYNAMIC DISKS
Volume size (maximum)	2 TB for simple and mirrored volumes. Up to 64 TB for spanned and striped volumes. (2 TB per disk with a maximum of 32 disks per volume.)
Supported RAID implementation	Hardware or software RAID
Storage of boot and system volumes	Simple or mirrored volumes only
Shared cluster storage in server clusters	Not supported

Specifying RAID Device Configuration Information

SecureCloud supports software RAID for the RAID 0 level.

Prerequisites:

- Create within your CSP the data storage devices for the RAID.

See [Creating a Data Storage Device in Your Virtualized or Cloud Service Provider Environment](#) on page 8-3.

- Configure the Runtime Agent in order to publish the data storage device in your CSP environment.

With the **update inventory** option set to "yes", configuring the Runtime Agent will make the devices in your CSP environment available in SecureCloud (see [Configuring the Runtime Agent](#) on page 8-6).

Procedure:

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

1. Click **Create RAID Array**.
2. From the "RAID Array Information" area, specify all the necessary information for the RAID.

The RAID Array ID is any unique name that does not contain any special characters (!@#\$(%^&*+).

The mount point is the drive letter you map to the RAID.

The image is the machine image accessing the RAID.

The key size determines the block size used in encryption (either 128, 192, or 256-bits).

The Provider, Region/Zone, and Image determine which device will be available for selection in the "Available Devices" area.

3. From the "Available Devices" area, select the data storage devices you want to add to the RAID.

You must select at least two devices.

4. Click **Create RAID Array**.

You must encrypt the RAID before you can use it (see [Encrypting a Data Storage Device or Device RAID](#) on page 8-7).

Viewing and Changing RAID Device Information

For a RAID with a status of "Not configured", "Configured", or "Encryption error", you can edit the devices in the array.

Prerequisites:

- Create within your CSP the data storage devices for the RAID.
See [Creating a Data Storage Device in Your Virtualized or Cloud Service Provider Environment](#) on page 8-3.
- Configure the Runtime Agent in order to publish the data storage device in your CSP environment.
With the **update inventory** option set to "yes", configuring the Runtime Agent will make the devices in your CSP environment available in SecureCloud (see [Configuring the Runtime Agent](#) on page 8-6).

Procedure:

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

1. Click the link of the desired RAID.
2. From the "RAID ID" page, make the desired changes.
See [Specifying RAID Device Configuration Information](#) on page 5-8 starting with Step 2.
3. Click **Save**.

Changing a Data Storage Device or RAID Device Assignment

At device creation, the CSP automatically generates the device identity. A device must have the "Encrypted" status in order to be re-mapped to a different machine image.

Note: This section applies to Amazon and Eucalyptus cloud environments. For vCloud and vSphere (with Native plugin), the data storage device assignment process is done at the time of machine image creation.

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

- Configuration Tool
 - User data
 - Resource pools on the Management Server
- See [About the Resource Pool](#) on page 4-3.

Note: User data can only be used by Amazon EC2:

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 Runtime 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 the Runtime Agent configuration. The Configuration Tool writes this information to the configuration file.

The Runtime 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.

Procedure:

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

1. From the "Image" area, choose the desired machine image from the drop-down list in the "Image Identity" column.

This is the machine image to which to mount the device or RAID.

2. Click **Save**.

3. Run the Configuration Tool on the Runtime Agent and then select **Update Device List** when prompted.

It is necessary to first run the Configuration Tool in order that the Runtime Agent passes SecureCloud an accurate inventory listing. Likewise during this process, the Management Server passes the Runtime Agent a list of assigned devices (see [Configuring the Runtime Agent](#) on page 8-6).

Unconfiguring a Data Storage Device or Device RAID

If you miss-configure a data storage device or RAID, or configure one of these so that it causes a configuration error, SecureCloud gives you the ability to reconfigure.

Note: You can unconfigure a device or RAID with the status of "Configured" or "Encrypted". If a device has the "Encrypting" status, wait for the status to change to "Encrypted" before unconfiguring.

Procedure:

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

1. Click the link of the desired device or RAID.
2. From the "Devices > Edit device" page, click **Unconfigure** and then **Save**.

Once a device or RAID is unconfigured, it can be reconfigured (see [Specifying RAID Device Configuration Information](#) on page 5-8 and [Specifying Device Configuration Information](#) on page 5-3).

WARNING! SecureCloud removes all key information and you cannot decrypt the device or RAID anymore.



Chapter 6

Reports and Logs

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

Topics in this chapter include the following:

- *Creating a Report Template and Generating a Report*
- *Understanding Generated Reports*
- *Querying Logs*
- *Understanding Archived Logs*

Reports

SecureCloud enables you to generate a one-time report or a scheduled report that is produced either daily, weekly, or monthly. All of these reports are based on a specified time range.

Also part of the report functionality is the ability to delete reports after a certain amount of time and to then email a report link so users can download the report.

Finally, you can generate a report either in PDF or Microsoft Excel (XLS) format, or both. But you must specify at least one format.

SecureCloud provides the following types of report criteria:

- **Key Reports**
Number of keys that have been requested, denied and approved. Time lapse between a key request and manual approval.
- **Inventory Reports**
Total number of machine instances that have been spun off, total number of machine images, total number of data storage devices.
- **Audit Reports**
Who accessed the Web Console, who and at what time a user created and/or deleted a policy, and who approves manual key requests.
- **Usage Reports**
The run time of the SecureCloud Runtime Agent in machine instances.

The different types of report criteria can be combined to create a unique report that fits your exact needs.

Creating a Report Template and Generating a Report

Procedure:

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

1. Specify the report name in the **Name** field.
The **Name** field is required. This field accepts up to 255 characters.

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

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 at least one format in which to view the composite report.

3. Specify when you want to delete the report.

See [Performing Report Maintenance](#) on page 6-3.

4. Specify any email recipients of the report.

See [Emailing a Report Notification](#) on page 6-3.

5. Click **Save** or **Save and Generate**.

Since a one-time report is saved and generated at the same time, the **Save and Generate** button is available for this type of report.

Scheduled reports are saved and then generated at a specified time. Therefore, the **Preview Report** button and **Save** button are available for these type of reports.

See [Understanding Generated Reports](#) on page 6-5.

Performing Report Maintenance

Report maintenance involves deleting unwanted reports.

Prerequisite:

Create a report (see [Creating a Report Template and Generating a Report](#) on page 6-2).

Procedure:

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

- Type the desired value in the **Delete this report after** field.

The field accepts values from 1 to 365. Thirty (30) is the default value.

Emailing a Report Notification

For a generated report, you can choose to issue an email notification alerting users that the report is available for viewing.

Prerequisite:

Create a report (see [Creating a Report Template and Generating a Report](#) on page 6-2).

Procedure:

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

- Select the **Email Report** check box and then specify an email address or email addresses.

If you de-select the check box, the specified address or addresses will remain, but will not be used.

See Also:

- [Creating a Web Console Notification](#) on page 7-6

Changing a Report Template

Procedure:

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

1. Click the link of the desired report template.
2. From the "Generate Report" page, make all the desired changes.
See [Creating a Report Template and Generating a Report](#).
3. Click **Save**.

The updated report template appears in the "Report Templates" page.

Deleting a Report Template

Procedure:

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

- Click the check box of the desired report template and then click **Delete**.

Downloading an Archived Report

Archived reports are either in PDF or Microsoft Excel (XLS) format, or both.

Prerequisites:

- Adobe Reader 9 or later
- Microsoft Excel

Procedure:

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

- Click the check box of the desired report and then click **Download Report(s)**.
In the "Output" column, you can also click the PDF or Excel icon of the desired report to download the report.

Deleting an Archived Report

Procedure:

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

- Click the check box of the desired report and then click **Delete**.

Understanding Generated Reports

SecureCloud generates a composite report that includes data for all the criteria 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.

Note: For a report that includes keys-requested information, the total number of key requests reported may be more than the combined number of approved and denied key requests due to several scenarios. For example, one scenario is where not all key requests are actioned before the instance is terminated. (If a key request errors, it does not require actioning.)

Logs

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

As part of the audit trail, SecureCloud logs system events from the Management Server and events sent to the Management Server from the Runtime Agent.

System events from the Management Server:

- Date and time of the Management Server start-up
- Date and time of the Management Server shutdown
- Date and time of account creation
- Record of machine image group creation, removal, modification
- Record of successful user account login
- Record of failed user account login attempts
- User activity in the Management Server Web Console (date, time, and user)
- Policy creation/deletion/edits.
- Key actions (approval [Manual/auto]/deny/pending)
- Report actions (generate/configuration/deletion)
- Agent actions (register/delete instance)
- Device actions (register/delete/clone)
- System settings changed

System events sent to the Management Server from the Runtime Agent:

- Agent ID, volume ID, date & time of device key request and resulting action.
- Agent ID, date & time of Agent image boot-up and shutdown
- Date & time of virtual image's boot-up and shutdown

Archived logs are stored in the CSV format.

Procedure:

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

- Click the hyperlink of the desired archived log.

From the "Size" column, you can also click the CSV icon of the desired log to download the log.

Because SecureCloud purges the log data after 12 months, you can save this data in an application that is able to read the CSV format, such as Microsoft Excel.



Chapter 7

Administration

Topics in this chapter include the following:

- *User Roles*
- *Managing Profile Information*
- *Web Console Notifications*
- *Authentication Methods in SecureCloud*
- *Product License*
- *Data Recovery*

Managing Users in the Web Console

This section describes the following:

- *Adding a New User to the Web Console* on page 7-1
- *Changing Web Console User Information* on page 7-2
- *Deleting a Web Console User* on page 7-2

Adding a New User to the Web Console

You can add users to SecureCloud using either the application's user interface or using Active Directory, if you are using this feature.

Procedure:

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

1. Click **Add User**.
2. From the "User Information" area, complete all the required fields.
See [User Roles](#) on page 7-3 for a description of each possible role.
3. Click **Save**.

The new user appears in the "Account Management" page.

Changing Web Console User Information

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

Procedure:

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

1. Click the link of the desired user.
2. From the "User Information" area, change the desired field(s).
See [User Roles](#) on page 7-3 for a description of each possible role.
3. Click **Save**.

Deleting a Web Console User

SecureCloud enables you to remove a user you no longer want accessing the Web Console.

Procedure:

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

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

User Roles

About User Roles

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

[Table 7-5](#) details the Web Console user roles.

TABLE 7-5. SecureCloud functionality based on user roles

ROLE	DESCRIPTION
Account Administrator	Manages a group account, which includes assigning users to an account based on various roles, controls device encryption keys, and has full functionality for all other Web Console operations, except for log deletion, device key export and generate report with device key information.
Security Administrator	Provides the ability to audit and manage device key information, which includes device key export and generate reports for device key information.
Data Analyst	Provides full report functionality with log functionality limited to read-only access. No other functionality is supported.
Auditor	Provides full report and log functionality, including log deletion. All other functionality is limited to read-only access. 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 User Role Permissions in the Web Console

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

Procedure:

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

From the "Account Management (Roles tab)" page, you can learn the capabilities of user each role.

Managing Profile Information

The account manager has the ability to specify the corporate time zone and the format for this time. This time in the format specified will be used by all other account members when generating reports and notifications, no matter what time zone in which they are working.

The Password option is for all account users. Using this option, you can change your login password.

Changing the Log In Password

SecureCloud enables you to change your log-in password. The Web Console password was originally set during product registration.

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**.

Specifying the Time Zone Used for Notifications and Reports

SecureCloud time stamps notifications and reports. These time stamps can be based on a specific location, such as your organization's corporate location.

From the "Time Information" page, you can specify a time zone used in the time stamping of notifications and reports. From this same page, you can specify the format in which you want the time stamp to appear.

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | ADMINISTRATION > TIME INFORMATION > TIME INFORMATION PAGE

- Specify the time zone and date format from the appropriate drop-down list and then click **Save**.

Web Console Notifications

SecureCloud can issue Web Console-based notifications for the following system events:

- A key request for device access requires manual approval.
- A key request for device access was automatically denied.
- A key request for device access was automatically approved.
- A key request was automatically approved after no action was taken for a device.
- A key request for a device that is not a member of the same policy as the machine image.
- An error occurs while provisioning a device.
- Device provisioning has completed.
- Device provisioning remains idle longer than the allotted time.
- Report generation has completed and is ready for viewing.

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

Creating a Web Console Notification

Procedure:

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

1. Click **Add Notification**.

The "Notifications Settings" page opens.

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

The **Name** field is required.

3. 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.

4. 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.

5. 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.

6. Click **Save**.

The new notification appears in the "Notifications" page.

Changing an Existing Web Console Notification

Procedure:

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

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

See [Creating a Web Console Notification](#) on page 7-6.

Deleting a Web Console 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**.

Specifying Deep Security Settings

In order to establish a connection between SecureCloud and the Deep Security Manager (DSM) server, you need to specify the DSM settings.

Procedure:

LOCATION: WEB CONSOLE MAIN MENU | ADMINISTRATION > DEEP SECURITY SETTINGS > DEEP SECURITY SETTINGS PAGE

- From the "Connection Information" area, specify all the necessary information for the DMS server.

The **Enable connection** check box enables you to connect to the DSM server for an additional layer of security. Deselecting this check box has a two-fold result:

- SecureCloud does not contact the DSM server for the additional security.
- SecureCloud does not use any DSM-related policies.

The username and password are for the DSM server and used by SecureCloud to gain access to this server.

Authentication Methods in SecureCloud

SecureCloud enables to you to log on to the system using of the following means:

- Local (SecureCloud password)

Using Local Authentication

The SecureCloud log on password is the default method for logging on to SecureCloud. The password is establish at product registration (see [Changing the Log In Password](#) on page 7-4).

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.

Specifying the Product License Activation Code

Note: If you are using SecureCloud from a provider other than Trend Micro, your activation code will not come from your product license. The activation code will be entered by your Managed Service Provider.

Specifying the activation code is necessary for the following scenarios:

- Activate the license for a new installation
- Renewing or updating your license with more or less seats
- Updating your license 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 "Enter A New Code" 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 contact your reseller for a license and then register online with your registration code for a valid activation code.

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

Rotating Amazon Credential Keys

In an effort to optimize security, Amazon allows you to create a new pair of credential keys (access key ID and secret access key). While Amazon does not enforce the use of this key pair, it does recommend that you replace your old key pair with a new one every 90 days. In doing so, SecureCloud provides additional security and clearly separates the duties between the Cloud Service Provider (CSP) administrator and your SecureCloud administrator.

Procedure:

1. Log on to an Amazon EC2 instance where SecureCloud Runtime Agent is installed.
2. Use the Configuration Tool to rotate old credential keys with new ones.

See *[Specifying Amazon Credential Keys Rotation](#)* on page F-7.

Rotate the credential keys for each account you have. The Runtime Agent reports credential information to the SecureCloud Server for each account you have.

The SecureCloud server stores credential rotation information.

The Runtime Agent queries credential information from the Management Server each time that it needs to query Amazon EC2 information.

The Runtime Agent derives the new credentials from the information received from the Management Server.

Note: To rotate the credential keys for multiple Amazon Machine Images (AMIs) using the same credential keys, rotate the credential keys for just one of these AMIs. This will result in credential key rotation for all the AMIs using the same credential keys. This is possible because while the key rotation is initiated from the Runtime Agent, the management of the credential keys is done from the SecureCloud Server.

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 device encryption keys available to you.

Exporting an Encryption Key to Restore an Encrypted Data Storage Device or RAID

Note: Only the Security Administrator has permission to export the device or RAID encryption key.

For each encrypted data storage device, you can export the encryption key to a specified location. An exported device encryption key is stored in a zip file. If you select more than one device for encryption key export, all the keys are stored in a single zip file.

An exported device encryption key is retrieved from the database and decrypted using the database encryption key. Each decrypted device encryption key is stored in a text file named `<device-id>.xml`. All device key files are compressed into a zip file with a name similar to `SecureCloudDeviceKeys-<timestamp>.zip`.

Note: The zip file itself is not protected by a password. Instead, the XML contents are encrypted using a user-specified passphrase.

Note: The exported device encryption key cannot be imported back into SecureCloud. To use the encryption key for data retrieval, you have to apply `keyexporter.sh` to the data storage device in question and then use the exported key for decryption.

Basic Steps:

Step 1. Export the encryption key from the Web Console.

See *Exporting the Encryption Key* on page 7-11.

Step 2. Decrypt the encryption key file and mount the device with the key.

See *Decrypting the Encryption Key File and Mounting the Device with the Key* on page 7-12.

Exporting the Encryption Key

Each encryption key is an encrypted XML file. You can export the encryption key for an individual data storage device or the keys for multiple devices. In the latter case, this could include any combination of individual devices, RAIDS, and individual devices plus RAIDS. For multiple key exports, the key for each device is stored in a zip file. Note that because a RAID has multiple devices by nature, selecting a RAID for encryption-key export will result in a zip file containing a key for each device in the RAID.

Prerequisite:

Logon to the Web Console using the Security Administrator role.

Procedure:

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

1. Select the desired data storage device, RAID, or any combination of these for which you want to export the encryption keys.

The desired volume(s) must have a status of "Encrypted" or "In-use".

An exported encryption key is stored in a zip file. If you select more than one device for encryption key export, all the keys are stored in a single zip file.

2. Click **Export**.
3. Enter the passphrase when prompted.

This passphrase, along with the random salt, is used to cipher/encrypt the device key when it is deciphered from the database. This ensures that the key is extracted securely.

4. Click **Save** to save the zip file.

Decrypting the Encryption Key File and Mounting the Device with the Key

Prerequisite:

- Logon to the Web Console using the Security Administrator role.
- Runtime Agent must be installed in order to make the key exporter utility function properly
- Export the device key zip file.

See [Exporting the Encryption Key](#) on page 7-11.

Procedure:

1. Extract the key file (in XML format) from the zip file that you saved earlier (see [Exporting the Encryption Key](#) on page 7-11).

vol1-e64a8f86.xml is the typical format of an extracted encryption key.

2. Change the working directory to the Runtime Agent installation directory.
/var/lib/securecloud is a typical example of the installation directory.
 - For Linux::

```
$ ./keyexporter.sh <key file.xml path>
```

- For Windows:

```
Run key_exporter.exe <key file.xml path>
```




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 Configuration Tool. Next, from the SecureCloud Web Console you specify which device(s) you want the Configuration Tool to encrypt.

Topics in this chapter include the following:

- *About the Configuration Tool*
- *Creating a Data Storage Device in Your Virtualized or Cloud Service Provider Environment*
- *Native on NFS and iSCSI*
- *Configuring the Runtime Agent*
- *Starting the Runtime Agent*
- *Encrypting a Data Storage Device or Device RAID*
- *Deleting a Data Storage Device From the Inventory*

About the Configuration Tool

When you run the Configuration Tool, it starts to configure the Runtime Agent and then prompts you to provision a device for encryption. If you accept the prompt, the Configuration Tool will provision the device that you configured from the SecureCloud Web Console.

Whenever there is a change to the devices inventory in your Cloud Service Provider (CSP), you need to run Configuration Tool to update the inventory to SecureCloud Management Server (see [Configuring the Runtime Agent](#) on page 8-6).

The Configuration Tool connects to SecureCloud and does the following:

- Reports to SecureCloud all available devices in your account for a given region or organization. These devices can be either active and inactive.

The Configuration Tool passes the SecureCloud Management Server a list of active devices. The Management Server then "cross references" this list to see which devices are already encrypted. From SecureCloud Web Console, you can view the results of this "cross reference" and direct the Configuration Tool to encrypt any un-encrypted devices.

The SecureCloud Management Server passes the list of assigned devices to the Configuration Tool. The Management Server generates this list based on the data storage device assignments.

- Encrypts and registers the device

The Configuration Tool encrypts your specified devices using the device encryption keys generated by the SecureCloud Management Server. Furthermore, when the Configuration Tool 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.

- Rotates the credential keys for an Amazon environment.

The Configuration Tool can rotate out old credential keys (access and secret access keys) for new ones. You can do this for each Amazon account you have, anytime after the Runtime Agent is installed.

See [Rotating Amazon Credential Keys](#) on page 7-9.

Note: The Configuration Tool functions listed above can also be achieved by using the optional SecureCloud RightScripts for RightScale. See Appendix E, [Managing SecureCloud Using RightScale](#) and your RightScale documentation for complete details.

Creating a Data Storage Device in Your Virtualized or Cloud Service Provider Environment

After SecureCloud confirms your registration, you need to create a data storage device for encryption. You can either create a new device or depending on your cloud service provider, clone an existing one.

The following are the basic steps to provision a device for encryption in SecureCloud:

Procedure:

1. Create a data storage device in your cloud service provider's environment.
See [Creating a Device in Amazon EC2](#) on page 8-4.
See [Creating a Device in vCloud](#) on page 8-4.
See [Creating a Data Storage Device in Eucalyptus](#) on page 8-4.
See [Creating a Device in vSphere](#) on page 8-5.
2. Install the Runtime Agent in the cloud VM.
See [Installing the SecureCloud Runtime Agent](#) on page A-3.
3. Run the Configuration Tool.
See [Configuring the Runtime Agent](#) on page 8-6.
 - a. Specify the required information.
 - b. Publish the device inventory to SecureCloud.
4. From the Web Console, specify a new key size if you are not satisfied with the default value.
See [Viewing and Changing Encryption Key Information](#) on page 5-7.

Note: When installing the Runtime Agent on Windows, use the Runtime Agent/Configuration Tool to provision the device.

Creating a Device in Amazon EC2

Procedure:

1. From your Amazon AWS console, create a new volume to encrypt.
Choose **Amazon AWS console > Amazon EC2 > Volumes**
2. Click **Create Volumes** and specify the necessary information in the "Create Volume" page.

See your Amazon documentation for complete details.

Creating a Device in vCloud

WARNING! When adding a data disk to a vCloud vApp, the disk must be attached to a free, logical unit number (LUN) on the first controller which is in use. Additionally, the use of mixed type of SCSI controllers are not supported and may result in failure to encrypt the disk, or unwanted loss of data.

1. From your vCloud Director console, add a disk to the VM.
Go to My Cloud > VMS, right click on the VM to which you want to add a disk, and then select **Properties** from the drop-down menu.
2. Click the "Hardware" tab and then click **Add**.
3. Click **OK**.

See your vCloud documentation for additional details.

Creating a Data Storage Device in Eucalyptus

1. Use the following command to list the availability zones:
`euca-describe-availability-zones`
2. Use the following command to create a device:
`euca-create-volume -size 1 -z myzone`

Creating a Device in vSphere

1. From vSphere client tool, select the VM to which you want to add a disk and right click.
2. From the menu, select **Edit Settings**.
3. From the Hardware tab, click **Add** and then select **Hard Disk** from the **Choose the type of device you wish to add** box.
4. Click **Next**.
5. Select **Create a new virtual disk** and then specify the size.
6. Follow the prompts and instruction to finish the settings.

Native on NFS and iSCSI

iSCSI works just like SCSI. You must attach the iSCSI target prior to provisioning

The NFS volume must be mounted prior to provisioning. SecureCloud will create a file inside the NFS as the secure storage. It will occupy the remaining space on the NFS at the time of provisioning.

NFS:

In Centos:

1. Mount the disk.

```
mount -t nfs 172.17.0.245:/cloud9 /emma-nfs
```
2. Then use `df -k`

iSCSI:

In Centos:

1. Install the iSCSI initiator.

```
yum -y install iscsi-initiator-utils
```
2. Start the service.
 The iSCSI service starts.
3. Search for the target.

```
iscsiadm -m discovery -type sendtargets -portal 172.17.0.245:3260
```
4. Login to the target.

```
iscsiadm -m node -T iqn.2011-04:ncsg-storage.target4 -p  
172.17.0.245:3260 -l
```

Then you can see it like `/dev/sdb`

In Windows 7:

1. Open iSCSI initiator.
2. Discover the target
3. Connect to the target

Configuring the Runtime Agent

Before the Configuration Tool can provision and encrypt a data storage device, you must use the Configuration Tool to configure the Runtime Agent.

Note: In order to setup the SecureCloud Runtime Agent or run the Configuration Tool shortcut on Windows 2008 successfully, you need to run the installer as administrator.

Procedure:

1. Launch the Configuration Tool.
 - For the Linux platform, execute the configuration script:
`/var/lib/securecloud/scconfig.sh`
 - For the Windows platform, click the Configuration Tool short cut.
2. Select the cloud service provider plug-in.
3. Specify the cloud service provider's credentials.
4. Input your SecureCloud Account ID.
5. Specify the URL of the Management Server Web services.
 - For Trend Micro SaaS customers, leave this prompt blank and press **Enter**.
The Web Service URL can be found at the "SecureCloud Web Console |Administration > User Management" page.
 - For customers receiving SecureCloud service from a Managed Service Provider, enter `https://sp-ms.securecloud.com` as the Web Service URL. Otherwise, accept the default of `https://ms.securecloud.com`.
6. Enter your passphrase for device provisioning.

7. Type "yes" to update inventory.
8. Type "yes" to wait for provisioning.
From the Web Console, you can now configure and then encrypt the device in question.
Type "no" if you are not provisioning a data storage device at this time.
9. If you want to use this instance to mount the device you want to encrypt, type "yes".
If you want to encrypt a device for some other instance, type "no".
10. Press **Enter** to accept the default timeout setting.

Note: The Configuration Tool can be automated and ran with command-line parameters. For the command line reference, start the Configuration Tool with the `--help` parameter specified for a list of options and their meaning.

Encrypting a Data Storage Device or Device RAID

WARNING! Selecting the primary (root) disk for encryption will result in an encryption error.

WARNING! Encrypting a data storage device will destroy any existing data on the device. Ensure that no valuable data is on the device before encrypting.

Prerequisites:

- Create within your CSP the data storage device.
See [Creating a Data Storage Device in Your Virtualized or Cloud Service Provider Environment](#) on page 8-3.
- Configure the Runtime Agent in order to publish the data storage devices in your CSP environment.

With the **update inventory** option set to "yes", configuring the Runtime Agent will make the devices in your CSP environment available in SecureCloud (see [Configuring the Runtime Agent](#) on page 8-6).

- Configure the data storage device.

See [Specifying Device Configuration Information](#) on page 5-3.

Procedure:

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

1. Select the desired device or RAID with a status of "Configured".
2. Click **Encrypt**.

The status of your selection changes from "Encryption Pending" to "Encrypted" after the encryption process finishes in the Runtime Agent.

Note: If the `scconfig.sh` file finishes executing in the provisioning loop before you click **Encrypt**, execute the `scconfig.sh` file again.

Deleting a Data Storage Device From the Inventory

In order to remove an encrypted device from SecureCloud, you must delete the device from your cloud service provider first. Next, update the inventory by running the Configuration Tool (see [Configuring the Runtime Agent](#) on page 8-6). This process will cause the device to have an "Undetected" status and can therefore be removed.

Deleting an encrypted device is basically a threefold process: (1) remove the device from your CSP, (2) update the SecureCloud inventory, and (3) delete the device entry from the Web Console.

Note: Only devices with the "Undetected" status can be deleted from the SecureCloud Web Console.

Procedure:

1. Log on to the virtual machine running the SecureCloud Runtime Agent and then stop the agent.
The status of the device changes from "In Use" to "Encrypted".
2. Delete the desired device in your CSP.
See your CSP documentation for complete details.
3. Run the Configuration Tool to report the current CSP inventory back to the SecureCloud Management Server.
See *Configuring the Runtime Agent* on page 8-6.
The device status is now "Undetected".
4. From the "Devices" page (Web Console main menu | Inventory > Devices), select the desired device having the "Undetected" status and then click **Delete**.

Deleting a RAID from the Inventory

In a RAID configuration, the data is distributed across the member volumes. If you delete a RAID, the distributed data is no longer accessible. The member volumes are now available as individual volumes or to be used in a RAID again.

Procedure:

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

- Select the desired RAID and then click **Delete**.
You can delete a RAID only when the RAID status is "Not Configured" or "Device Missing".

Starting the Runtime Agent

If you are operating in a bare metal, virtualized environment such as vSphere or you are operating in a cloud environment and do not want to bundle your data before executing it, you may want to start the Runtime Agent after running the Configuration Tool.

Start the Runtime Agent in Linux:

```
/etc/init.d/scagentd start
```

Start the Runtime Agent in Windows:

1. Click the **Start** menu and choose **Run**.
2. From the "Run" window, type `services.msc` and then click **OK**.
3. Right-mouse click **Trend Micro SecureCloud Agent** and then choose **Start**.

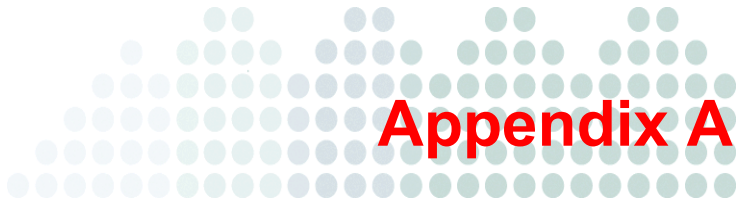
Stopping the Runtime Agent

Stop the Runtime Agent in Linux:

```
/etc/init.d/scagentd stop
```

Stop the Runtime Agent in Windows:

1. Click the **Start** menu and choose **Run**.
2. From the "Run" window, type `services.msc` and then click **OK**.
3. Right-mouse click **Trend Micro SecureCloud Agent** and then choose **Stop**.



Installing and Uninstalling SecureCloud

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:

- *Specifying Application Start Up After Encrypted Device Mount*
- *Installing the SecureCloud Runtime Agent*
- *Starting and Stopping a Dependent Service*
- *Uninstalling the Runtime Agent*
- *Migrating Data from SecureCloud 1.x to SecureCloud 2.0*

Installation Summary

The following are the basic steps of the SecureCloud installation process.

Step 1. Modify the config.xml file so an application starts after the data storage device is mounted

If an application attempts to access a data storage device before the device is mounted, the application will freeze and require rebooting.

See *Specifying Application Start Up After Encrypted Device Mount* on page A-2.

Step 2. Install the SecureCloud Runtime Agent.

- If your environment is Linux, install accordingly.
See *Installing the Runtime Agent in a Linux Environment* on page A-7.
The Linux agent installer requires several pre-installation preparations if you use a custom kernel—not the official Linux released kernel. In this case, you have to provide the corresponding kernel source and set up the installation environment manually prior to launching the Runtime Agent installer.
See *Preparing to Install with a Custom Linux Kernel* on page A-9.
- If your environment is Windows, install accordingly.
See *Installing the Runtime Agent in a Windows Environment* on page A-10.

Step 3. Modify the config.xml file to start and stop a dependent service

To ensure the smooth operation of a dependent service, it is a good practice to start your dependant service after the data storage device is mounted and then stop it before the device is dismounted.

See *Starting and Stopping a Dependent Service* on page A-12.

Specifying Application Start Up After Encrypted Device Mount

Before an application can start up and access an encrypted data storage device, the device must be mounted. If this is not the case, then the application attempting to access the device will freeze and require rebooting. For example, if SQL starts before the device containing the SQL database is mounted, the SQL application may not function properly.

Procedure:

1. Create the script file.

To start the service mysqld:

```
vim /root/start.sh  
  
#!/bin/sh
```

To stop the service mysqld:

```
vim /root/stop.sh
```

```
#!/bin/sh
```

2. Make the scripts executable.

```
chmod 755 /root/start.sh
```

```
chmod 755 /root/stop.sh
```

3. Specify in the `config.xml` file that an application should start after the data storage device is mounted:

```
:  
<agent version="2.0">  
  
<devices/>  
  
<userScripts mountComplete="/root/start.sh"  
teardown="/root/stop.sh"/>  
  
</agent>  
:
```

For the `mountComplete` attribute, specify the start up script for the application.
For the `teardown` attribute, specify the shut down script for the application.
SecureCloud executes the script file once all devices are successfully mounted.

Note: SecureCloud executes the script file after all devices are successfully mounted.
For example, SecureCloud would not execute the script file if there are
key-pending devices or mounting-failed devices.

Installing the SecureCloud Runtime Agent

If you have a RightScale account, you can use RightScript to install the Runtime Agent
(see *Installing the Runtime Agent and Provisioning a Data Storage Device* on page E-3).

Note: SecureCloud 2.0 Runtime Agent does not support an upgrade from a 1.x version of the product. Also, it cannot access volumes encrypted with SecureCloud 1.x Runtime Agent. Therefore, you need to do a manual migration of any SecureCloud 1.x data before it can be accessed using SecureCloud 2.0 Runtime Agent. (see [Migrating Data from SecureCloud 1.x to SecureCloud 2.0](#) on page A-14).

Prerequisites:

- Create a data storage device in your cloud environment.
See [Creating a Data Storage Device in Your Virtualized or Cloud Service Provider Environment](#) on page 8-3 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 Chapter 8, [Provisioning for Data Storage Encryption](#).

- For the Amazon environment, if you are using the Amazon Identity Manager (AIM) then you need to setup certain EC2 privileges in order to install and run the Runtime Agent.

The following AIM policy contains the necessary EC2 privileges:

```
{
  "Statement": [
    {
      "Sid": "Stmt1307660106106",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
```

```

        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume"
    ],
    "Effect": "Allow",
    "Resource": "*"
}
]
}
```

Procedure:

- To install the Runtime Agent in a Linux environment, see [Installing the Runtime Agent in a Linux Environment](#) on page A-7.
Refer to [Supported Kernels for Amazon EC2](#) on page A-6 if you are installing in an Amazon EC2 cloud environment.
- To install the Runtime Agent in a Windows environment, see [Installing the Runtime Agent in a Windows Environment](#) on page A-10.
Refer to [Supported Kernels for Amazon EC2](#) on page A-6 if you are installing in an Amazon EC2 cloud environment.

Supported Kernels for Amazon EC2

Use [Table A-6](#) below to install the Runtime Agent in the Amazon EC2 cloud environment.

TABLE A-6. Supported Kernels for Amazon EC2

OS VERSION	ARCH	KERNEL	DISTRIBUTION	EC2 AKI
CentOS 5.4	x86	2.6.18	Linux 2.6.18-128.1.6.el5xen i686	
CentOS 5.5	x86	2.6.18	Linux 2.6.18-128.1.6.el5xen i686	
CentOS 5.6	x86 x64	2.6.18	Linux 2.6.18-238.19.1.el5.centos.plusxen x86_64 Linux 2.6.18-238.19.1.el5.centos.plusxen i686 Linux 2.6.18-274.7.1.el5 i686 Linux 2.6.18-274.7.1.el5-x86_64	aki-a4225af6 aki-ee5df7ef
CentOS 6.0	x86 x64	2.6.32	Linux 2.6.32-71.29.1.el6.i686 i686 Linux 2.6.32-71.29.1.el6.x86_64 x86_64	aki-d209a2d3 aki-11d5aa43
RHEL 5.5	x86 x64	2.6.18	Linux 2.6.18-194.32.1.el5xen i686 Linux 2.6.18-194.32.1.el5xen x86_64	aki-9c235ace aki-82235ad0
RHEL 6.0	x86 x64	2.6.32	Linux 2.6.32-71.29.1.el6.i686 i686 Linux 2.6.32-71.29.1.el6.x86_64 x86_64	aki-9c235ace aki-11d5aa43
Ubuntu 10.10	x86	2.6.35	Linux 2.6.35-22-generic-pae i686	

TABLE A-6. Supported Kernels for Amazon EC2 (Continued)

OS VERSION	ARCH	KERNEL	DISTRIBUTION	EC2 AKI
Ubuntu 11.4	x64 x86	2.6.38	Linux ubuntu1104x642 2.6.38-8-server x86_64 Linux Ubuntu1104-cm 2.6.38-8-generic-pae i686	
CentOS 5.4	x86 x64	2.6.21	Linux 2.6.21.7-2.fc8xen i686 Linux 2.6.21.7-2.fc8xen x86_64	aki-15f58 a47 aki-1df58 a4f
Ubuntu 9.10	x86 x64	2.6.31	Linux 2.6.31-302-ec2 i686 Linux 2.6.31-302-ec2 x86_64	aki-87f38 cd5 aki-83f38 cd1
Ubuntu 10.10	x86	2.6.35	Linux 2.6.35-19-virtual i686	aki-13d5a a41
SUSE 11	x86	2.6.32	Linux 2.6.32.46-0.3-ec2 i686	aki-83396 bc6
Ubuntu 10.4	x64	2.6.32	Linux 2.6.32-308-ec2 x86_64	aki-20354 b72

Installing the Runtime Agent in a Linux Environment

Note: In the vCloud environment, you have to provide the SecureCloud account ID and vCloud organization.

Procedure:

1. Download the appropriate agent build for your cloud instance from the Trend Micro portal:
<http://downloadcenter.trendmicro.com/>

2. Install the package management system.

CentOS/RHEL/SUSE:

Use RPM to install the RPM package by executing the following command:

```
rpm -ivh <scagent.rpm>
```

where <scagent.rpm> is the name of the installation package downloaded in step 1.

Ubuntu:

Install Gdebi to then install the DEB package by executing the following command:

```
gdebi <scagent.deb>
```

where <scagent.deb> is the name of the installation package download in step 1.

3. Launch the SecureCloud Configuration Tool by executing the following command:

```
/var/lib/securecloud/scconfig.sh
```

4. Accept the license agreement.
5. When prompted, select the appropriate option for your cloud service provider.
6. Enter your Cloud Service Provider (CSP) credentials as prompted.

These credentials will differ depending on your Cloud Service Provider.

Note: Not all Cloud Service Provider environments require credentials.

7. Enter your SecureCloud Account ID when prompted.

The SecureCloud Account ID can be found at the "SecureCloud Web console | Administration > User Management" page.

8. Enter your provision passphrase when prompted.

9. Specify the URL of the Management Server Web services.

- For Trend Micro SaaS customers, leave this prompt blank and press **Enter**.

The Web Service URL can be found at the "SecureCloud Web Console | Administration > User Management" page.

- For customers receiving SecureCloud service from a Managed Service Provider, enter `https://sp-ms.securecloud.com` as the Web Service URL.

10. Follow the prompts as they appear.

The provisioning passphrase can be found and set at the "SecureCloud Web Console | Administration > User Management" page.

Preparing to Install with a Custom Linux Kernel

The Linux agent installer can automatically download required dependent packages from the online repository (package storage location) which is defined in your running instance. The repository settings are varied among the Linux distributions. Usually, once the operating system is installed, some default repositories will be included in the system and you need not configure it unless an additional repository is used.

The Linux agent installer uses a different package management system on different distributions. For example, on CentOS and RHEL, the yum tool is used where on Ubuntu the apt-get tool is used.

Prerequisites:

- The Linux agent installer requires all dependent packages to be present in the system before continuing the installation of the SecureCloud Runtime Agent. If the Linux agent installer cannot download all the dependent packages from the repository, you are then required to provide them by either downloading the package manually from Internet or somewhere else.

The following comprise the dependant packages for Linux:

- Common dependency : gcc, python (2.4.3 or greater), curl, make, gawk
- CentOS /RHEL 5.x:
 - Amazon EC2 or Xen based : kernel-headers, kernel-xen-devel
 - Others: kernel-headers, kernel-devel
- CentOS /RHEL 6.x : kernel-headers, kernel-devel
- Ubuntu: linux-headers
- Suse 11: Kernel source

SUSE 11 requires that you specify the information below. (This information is based on the 2.6.32.46 version of the Linux kernel.)

```
$yast --install kernel-source
$cp /boot/symvers-2.6.32.46-0.3-ec2.gz
/usr/src/linux/Module.symvers.gz
```



```
$gunzip /usr/src/linux/Module.symvers.gz
$cd /usr/src/linux
$make cloneconfig
$make modules_prepare
$ln -s /usr/src/linux
/lib/modules/2.6.32.46-0.3-ec2/build rpm -ivh
scagent-2.0.0.xxx.rpm
```

- If you are using a custom Linux kernel, the complete kernel source is required because the Trend Micro Encryption Module driver cannot build without the proper kernel source. (To compile the kernel, refer to your Linux user guide.) Also, ensure there is a soft link, `/lib/modules/<kernel version>/build` which links to the kernel source path.
- In the Linux environment, you are able to customize your kernels. The kernel source must be provided and the path should be set using one of the following commands:

```
$ln -s /usr/src/linux /lib/modules/<kernel-version>/build
#SUSE

$ln -s /usr/src/kernels/<kernel-version>
/lib/modules/<kernel-version>/build #CentOS/RHEL

$ln -s /usr/src/linux-source-<kernel-version>
/lib/modules/<kernel-version>/build #Ubuntu
```

To check the kernel version, use command `uname -r`.

Procedure:

- Launch the Linux agent installer.
`./<scagent_installer_name>.bin`

Installing the Runtime Agent in a Windows Environment

Note: In order to setup the SecureCloud Runtime Agent or run the Configuration Tool shortcut on Windows 2008, you need to run the installer as Administrator.

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 portal:
`http://downloadcenter.trendmicro.com/`
3. Extract the installation package and run `SecureCloudInstaller.exe` and then follow the on-screen instructions.
4. Launch the SecureCloud Configuration Tool from the Start Menu by choosing **All Programs > Trend Micro SecureCloud Agent > Configuration tool**
5. When prompted, select the appropriate option for your CSP.
6. Enter the credentials of your CSP as prompted.
The credentials will vary depending on your CSP.

Note: Not all CSP environments require credentials.

7. Enter your SecureCloud Account ID when prompted.
The SecureCloud Account ID can be found on SecureCloud at **Web Console main menu | Administration > User Management**.
8. Specify the URL of the Management Server Web services.
 - For Trend Micro SaaS customers, leave this prompt blank and press **Enter**.
The Web Service URL can be found at the "SecureCloud Web Console | Administration > User Management" page.
 - For customers receiving SecureCloud service from a Managed Service Provider, enter `https://sp-ms.securecloud.com` as the Web Service URL.
9. Follow the prompts as they appear.
The provisioning passphrase can be found and set at **Web Console main menu | Administration > User Management**.
10. When prompted, reboot the VM.
This reboot is necessary in order to update the Windows Runtime Agent with the FIPS 140-2 certified crypto engine driver. Without this driver, SecureCloud cannot function.

When installing the Runtime Agent, you can reboot at any time.

Maintenance Install for the Runtime Agent in a 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://downloadcenter.trendmicro.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.

Starting and Stopping a Dependent Service

To ensure the smooth operation of a dependent service, it is a good practice to start your dependant service after the data storage device is mounted and then stop it before the device is dismounted.

To implement this functionality, you have to modify the `config.xml` file.

Procedure:

Update the `config.xml` file under the Runtime Agent folder by adding the following:

```
<userScripts mountComplete="" teardown=""/>
```

Also, set the correct script path for `mountComplete` and `teardown`.

Uninstalling the Runtime Agent

You can uninstall the SecureCloud Runtime Agent from one machine image and then install it on another. Uninstalling the SecureCloud Runtime Agent does not remove your data from the encrypted data storage device(s). If you choose to uninstall the SecureCloud Runtime 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 the Runtime Agent from a Linux Environment

Procedure

- From a command shell, execute the following command:
`rpm -ev scagent`

For the Ubuntu operating system, execute the following command:
`dpkg -r scagent`

Uninstalling the Runtime Agent 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://downloadcenter.trendmicro.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.

Migrating Data from SecureCloud 1.x to SecureCloud 2.0

SecureCloud 2.0 Runtime Agent does not support an upgrade from a 1.x version of the product. Also, it cannot access volumes encrypted with SecureCloud 1.x Runtime Agent. Therefore, you need to do a manual migration of any SecureCloud 1.x data before it can be accessed using the SecureCloud 2.0 Runtime Agent.

This section describes how to migrate the data protected by SecureCloud 1.x to SecureCloud 2.0.

Migrating Data from a Public Cloud

1. Launch a new, temporary instance and install the SecureCloud 2.0 Runtime Agent.
2. In the temporary instance, run the Configuration Tool to provision a new device with the same SecureCloud 1.2 source device size.
3. Copy the data securely from the SecureCloud 1.2 instance to the temporary instance.

In Linux use Secure Copy (SCP) and in Windows, setup a SFTP server.

4. After the copy finishes, stop the SecureCloud Runtime Agent in the temporary instance.

See [Stopping the Runtime Agent](#) on page 8-10.

5. Login to the SecureCloud Web Console and from the main menu choose **Inventory > Devices**.
6. From the "Devices" page, click the new device and change the image identity from the temporary instance to the original SecureCloud 1.2 instance.
7. Remove the SecureCloud 1.2 Runtime Agent in the original instance and install the SecureCloud 2.0 Runtime Agent.
8. In the original instance, run the Configuration Tool and then specify "no" to the prompt to update the inventory and "no" to the prompt to get the mount device list.
9. Start the SecureCloud 2.0 Runtime Agent.

The newly provisioned device is mounted and the SecureCloud 1.2 data is migrated.

See [Starting the Runtime Agent](#) on page 8-9.

10. After verification, delete the temporary instance and the SecureCloud 1.2 encrypted disk if necessary.

Migrating Data from a Private Cloud

Basic Steps:

- Step 1. Restore encrypted data to clear-text format on a separate, temporary disk.**

See [Restoring Encrypted Data to Cleat-text Format](#) on page A-15.

- Step 2. Uninstall the SecureCloud 1.x Runtime Agent.**

See [Uninstalling the SecureCloud 1.x Runtime Agent](#) on page A-16.

- Step 3. Install the SecureCloud 2.0 Runtime Agent and do disk provisioning on another disk.**

See [Installing the SecureCloud 2.0 Runtime Agent and Provision the Disk](#) on page A-17.

- Step 4. Copy clear-text data to the new provisioned/encrypted device.**

See [Copying Clear-text Data to the Newly Provisioned Device](#) on page A-17.

- Step 5. Optionally, remove the temporary disk you created in step 1.**

The data on the temporary disk is not encrypted and therefore not secure.

Restoring Encrypted Data to Cleat-text Format

In the machine image that has the SecureCloud 1.x Runtime Agent installed, add two new devices (dev-X, dev-Y) with the same capacity as the encrypted (by SecureCloud 1.x) device (dev-E).

Restart the machine image that has SecureCloud 1.x Runtime Agent installed.

After the machine image starts up, go to the Web Console to approve the key request if it is configured as manual approval.

Procedure:

Restore protected data to unprotected device (clear-text):

Windows platform

1. Go to **Computer Management > Disk Management**.
2. Select the first new disk (dev-X).
3. Initialize the disk to **Basic** and create a data storage device that occupies the whole space on it.
4. Format the disk and assign a drive letter to this new data storage device.
5. Copy all files/folders from the protected drive (on dev-E) to the new assigned drive (on dev-X).

Linux platform

1. Format the new disk (dev-X) using tools (such as mkfs).
2. Create a mount point for the 1st new disk (dev-X) added.
3. Mount the first new disk (dev-X) to the mount point just created.
4. Copy all files/folders from the protected mount point (on dev-E) to the new unprotected mount point (on dev-X).

Uninstalling the SecureCloud 1.x Runtime Agent

Procedure:*Windows platform*

1. Close all windows.
2. Uninstall SecureCloud 1.x Runtime Agent.
3. Uninstall FreeOTFE.

Linux platform

1. Uninstall the SecureCloud 1.x Runtime Agent.
2. Delete the `/var/lib/securecloud` folder.

Installing the SecureCloud 2.0 Runtime Agent and Provision the Disk

Procedure:

1. Install SecureCloud 2.0 Runtime Agent.
2. Restart the machine image that has SecureCloud 2.0 agent installed.
3. After the machine image is started, stop SecureCloud 2.0 Runtime Agent service/daemon.
4. Launch the Configuration Tool.
Follow the instructions to do provisioning on the second new disk (dev-Y).
Remember to upload inventory and get the new device list.

Copying Clear-text Data to the Newly Provisioned Device

Procedure:

1. Start SecureCloud 2.0 Runtime Agent service/daemon.
2. After the machine image starts, go to the Web Console to approve the key request if it is configured for manual approval.
3. Copy clear-text data to new provisioned/encrypted device, based on your platform:

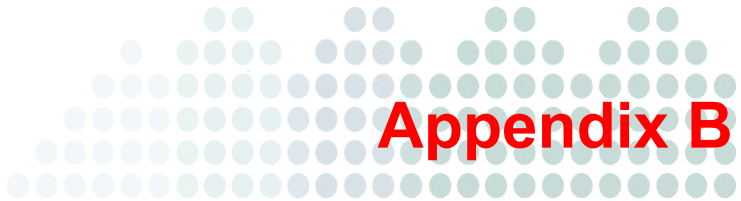
Windows platform

- a. Copy all files/folders from the unprotected drive (on dev-X) to the new provisioned drive (on dev-Y).
- b. Close all windows.
- c. Go to **Computer Management > Disk Management** and remove the drive letter assigned to the unprotected drive (on dev-X).

Linux platform

- a. Copy all files/folders from the unprotected mount point (on dev-X) to the new protected mount point (on dev-Y).
- b. Dismount the mount point for the 1st new disk (on dev-X).
- c. Delete the mount point for the 1st new disk (on dev-X).
 - i. Restart the machine image and approve the key request.
 - ii. Verify if the system works as expected.

- iii. Delete the first new disk (dev-X) if you do not need it anymore.



Appendix B

Frequently Asked Questions

This appendix describes questions that may arise when using SecureCloud.

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.

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.

What Certifications Does SecureCloud Hold?

SecureCloud SaaS data centers are ISO27001 certified.

How are All Communications 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-the-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.

How do I Acquire the Installation Log File for Installation Debugging?

In order to generate a debug log file during a manual installation of the Management Server, run the following command from the command prompt:

```
msiexec /i <msi path> /lv*x install.log
```

Note: Please substitute the <msi path> with the path of the SecureCloud MSI file.

How do I Restore My Device Encryption Key on the Runtime Agent?

You can only export the data storage device encryption key from the Web Console.

Procedure:

1. Extract your backed up device key.
2. Decrypt your device key.
See [Decrypting the Encryption Key File and Mounting the Device with the Key](#) on page 7-12.
3. Mount your data storage device using the device encryption key.
See [Decrypting the Encryption Key File and Mounting the Device with the Key](#) on page 7-12.



Contact Information and Web-based Resources

Note: If you are using SecureCloud from a provider other than Trend Micro, this appendix does not apply to you. Your contact and means of support is your Managed Service Provider.

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 should encounter problems while using SecureCloud, please use the following email address to contact Trend Micro and report your problem:

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

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:

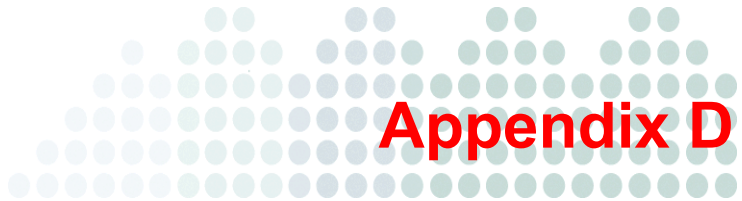
<http://kb.trendmicro.com/solutions/includes2/ContactTechSupport.asp>

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.



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 Configuration Tool 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 Configuration Tool utilize log files to record runtime and detailed error information. The log files for the SecureCloud Runtime Agent and Configuration Tool can be found at the following locations:

- Linux:

```
/var/lib/securecloud/logfiles/
```

- Windows:

```
C:\Program Files\Trend Micro\SecureCloud\Agent\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 `logger.ini` in the SecureCloud installation folder (`/var/lib/securecloud/logger.ini` on Linux, or `C:\Program Files\Trend Micro\SecureCloud\Agent\logger.ini` on Windows) named `logger.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.

SSL Configuration and Troubleshooting

SecureCloud utilizes SSL to establish a secure connection between the Management Server and the Runtime Agent and Configuration Tool. The validity of the SSL certificates installed on the Management Server are verified by the Runtime Agent and Configuration Tool prior to establishing a communications protocol. If you are experiencing SSL certificate validation issues, there are two methods to resolve this. These are described below.

1. Install the Issuer Certificate files on the Runtime Agent and Configuration Tool machine images.

The Runtime Agent and Configuration Tool provide a mechanism for users to upload their own certificate issuer files in order to establish a trust relationship with the Management Server. These certificates should be in PEM (base64 encoded DER) format and placed in the appropriate folder:

Runtime Agent:

`/var/lib/securecloud/certs` (Linux)

`C:\Program Files\Trend Micro\SecureCloud\Agent\bin\certs\`
(Windows)

2. Disable SSL certification validation in the Runtime Agent and Configuration Tool machine images

In the event of using a Self Signed certificate, or a certificate whose common name doesn't match the hostname which the Runtime Agent and Configuration Tool use to connect to the Management Server, SSL certificate validation can be disabled.

Edit the `config.xml` file and set the `ignore_errors` attribute to `True` on the `openssl` element:

```
<openssl certTimeout="60" ignore_errors='True'/>
```

The `config.xml` file is located in the following location:

Runtime Agent:

`/var/lib/securecloud/config.xml` (Linux)

`C:\Program Files\Trend
Micro\SecureCloud\Agent\bin\config.xml` (Windows)



Managing SecureCloud Using RightScale

The enhanced RightScale scripts give you the ability to separate the Runtime Agent installation and device provisioning operations. These do not have to be performed as a single operation. The enhanced RightScale script automatically detect the guest operating system for Runtime Agent installation. Only devices on the device list will be part of your environment.

The enhanced RightScale scripts also support installing and uninstalling the Runtime Agent, provisioning a device, and rotating Amazon credential keys.

Note: When Amazon periodically refreshes your access and secret access keys, the enhanced RightScale scripts will not automatically deploy the new Amazon credential keys to the Runtime Agent. You have to manually run the script, provide required parameters (old credential, new credential, and provision passphrase) and then SecureCloud will replace the old credential keys with the new ones.

The Trend Micro RightScript takes Amazon Web Services (AWS) credentials and device configuration information as input and then performs provisioning.

Possible RightScript Commands

The following are the possible SecureCloud operations you can do in RightScale:

- Install the Runtime Agent and provision the data storage device
- Provision the data storage device
- Uninstall the Runtime Agent
- Rotate the Amazon credential keys

Table E-7 describes the RightScript commands used in these operations.

TABLE E-7. SecureCloud RightScript Parameters

PARAMETER	DESCRIPTION
INSTALL_OPTION	<ul style="list-style-type: none">• Install the Runtime Agent and/or Provision Device• Uninstall
AWS_ACCESS_ID	Amazon AWS access key ID
AWS_SECRET_KEY	Amazon AWS secret access key
DEVICES_CONF	<p>Device list to provision</p> <p>Format: <DEVICES_CONF> ::= <DEVICE> <DEVICE> <DEVICE_CONF> <DEVICE> ::= id=<DEVICE_ID>, mountpoint=<MOUNTPOINT>,os=[linux windows], filesystem=[ntfs fat32 ext3 xfs], keysize=[128 192 256],access=[readOnly readWrite];</p> <p>Example: id=vol-09657866,mountpoint=/mnt/testsc, os=linux,filesystem=ext3,keysize=128, access=readWrite;</p>
PROV_PASSWORD	Provisioning password

TABLE E-7. SecureCloud RightScript Parameters (Continued)

PARAMETER	DESCRIPTION
SC_ACCOUNT_ID	SecureCloud account ID
ORIGINAL_AWS_ACCESS_ID	Original Amazon AWS access key ID
ORIGINAL_AWS_SECRET_KEY	Original Amazon AWS secret access key

Installing the Runtime Agent and Provisioning a Data Storage Device

To locate and install the SecureCloud RightScripts in your RightScale account, go to MultiCloud Marketplace RightScripts, search on "SecureCloud" and then locate the SecureCloud scripts. Finally, import them into your account.

Prerequisites:

- Create the multi-cloud image from the RightScale console (See RightScale documentation).
- Go to the "Scripts" tab and locate the SecureCloud script from the published scripts.

Procedure:

1. Go to the "Inputs" tab and specify the following:
 - `INSTALL_OPTION`
Select **Install Runtime Agent**.
 - `AWS_ACCESS_ID`
 - `AWS_SECRET_KEY`
 - `DEVICES_CONF`
 - `PROV_PASSWORD`
 - `SC_ACCOUNT_ID`

See *Possible RightScript Commands* on page E-2.
2. View the monitor to see the status of the script.

At the end of the process, the new data storage device will be added to the SecureCloud inventory and appear with a status of "Encrypted" in the "Devices" page.

Uninstalling the Runtime Agent

Prerequisites:

- Create the multi-cloud image from the RightScale console (See RightScale documentation).
- Go to the "Scripts" tab and locate the SecureCloud script from the published scripts.

Procedure:

- Go to the "Inputs" tab and specify the following:
 - `INSTALL_OPTION`
Select **Uninstall** to uninstall the Runtime Agent.
- See [Possible RightScript Commands](#) on page E-2.

Rotating Amazon Credential Keys

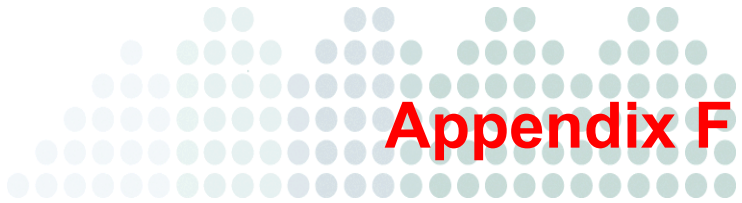
Prerequisites:

- Ensure that the Runtime Agent is installed.
See [Installing the Runtime Agent and Provisioning a Data Storage Device](#) on page E-3 or [Installing the SecureCloud Runtime Agent](#) on page A-3.
- Go to the "Scripts" tab and locate the SecureCloud script from the published scripts.

Procedure:

- Go to the "Inputs" tab and specify the following parameters:
 - `ORIGINAL_AWS_ACCESS_ID`
 - `ORIGINAL_AWS_SECRET_KEY`
 - `AWS_ACCESS_ID`
 - `AWS_SECRET_KEY`
 - `PROV_PASSWORD`

See *Possible RightScript Commands* on page E-2.



Configuration Tool Scripts

The Configuration Tool scripts are available to do the following:

- Rotate Amazon credential keys
- Update the SecureCloud inventory with the list of data storage devices in your Cloud Service Provider's environment
- Configure the Runtime Agent
- Provision a data storage device
- Support proxy server functions

Configuration Tool Commands

Table F-8 list all the Configuration Tool commands that are used in the functions performed by this tool.

TABLE F-8. Configuration Tool Commands

OPTION	ARGUMENTS	FUNCTION	EXAMPLE	COMMENT
-h --help	None	Displays the options and help messages		
-d -- devices	<CSP_ID>	Specifies a Cloud Provider to activate	Amazon-AWS vCloud Native	This option can be used along with other commands. If the plugin is not installed, it will install it (-p) The CSP Id is defined in the plugin
-e --ignore-ssl-error	None	Ignore any SSL errors (certificate verification)		This should be used if the instance has Python2.4 and proxy is enabled
-g --guid	<ACCOUNT_ID>	Specifies the Account ID	BF2CE005-F482-4d95-AA2A-6A3E94D4780C	Can be obtained from the Management Server, Web Console Administration > User Management

TABLE F-8. Configuration Tool Commands (Continued)

OPTION	ARGUMENTS	FUNCTION	EXAMPLE	COMMENT
-i --publish-inventory	None	Read the CSP inventory and update the KMS	./scconfig.sh -i -g BF2CE005-F482-4d95-AA2A-6A3E94D4780C -x eeruzswRi9V-c Native -s -q	This command depends on other options. This option can be run in -q (quiet) mode where the default values are used for skipped inputs
-l --list-plugins	None	Displays the bundled plugins		
-k --get-device-list	None	Fetch the list of devices that are assigned to this agent		Useful in CSPs with detachable storage Its is a good idea to run this command 1)after provisioning 2)After device re-assignment 3)After staring a new instance with agent in it This command sync's up the KMS and the agent on the device list assignment

TABLE F-8. Configuration Tool Commands (Continued)

OPTION	ARGUMENTS	FUNCTION	EXAMPLE	COMMENT
-m --original-credentials	<OPTIONS>	Specifies the OLD credential fields when you perform credential	"access_id=XXXXXXXXXX, secret_key=YYYYYY"	In 2.0 this is applicable only to Amazon EC2. But it can be used on any supported cloud
-n --new-credentials	<OPTIONS>	Specifies the NEW credential fields when you perform credential rotation	"access_id=XXXXXXXXXX, secret_key=YYYYYY"	Same as above
-o --options	<OPTIONS>	This is a generic string to specify any custom options.	"access_id=XXXXXXXXXX, secret_key=YYYYYY"	<p>This has a "key=value,key=value" format. Any module that accepts custom inputs can be passed in using this option.</p> <p>For example</p> <p>1)auto configuration in EC2 takes the amazon access id and secret key in this form</p> <p>2)The plugin registration module takes custom credential input using this option as well</p>

TABLE F-8. Configuration Tool Commands (Continued)

OPTION	ARGUMENTS	FUNCTION	EXAMPLE	COMMENT
-p --plugin	PLUGIN FILE NAME	Specifies the plugin file that need to be installed		
-q --quiet	None	Quiet mode, assumes defaults		
-r --register	None	Command to register the current image with KMS		Registering image will require inputs such as the CSP_ID, ACCOUNT_ID, URL, CSP creden- tials etc. These inputs can be passed using other options
-s --saas	None	Using Trend Micro SaaS server		Overrides any urls provided using -u option
-t --timeout	Time in min- utes	Provision- ing Timeout in minutes		How long should the tool wait to receive the list of devices to be pro- visioned (default 720)
-u --url	<URL>	Specifies the URL of the manage- ment server's Web service		Can be obtained from the Web Con- sole, Administra- tion > User Management

TABLE F-8. Configuration Tool Commands (Continued)

OPTION	ARGUMENTS	FUNCTION	EXAMPLE	COMMENT
-w --with-provisioning	None	Do provisioning		The toll will request Management Server for any devices that need to be provisioned. If there are devices to be provisioned, it will provision them (Refer to -d option for overriding)
-x --passphrase	PASSWORD	Specifies the provisioning password		Can be obtained from the Web Console, Administration > User Management
-z --update-credentials	None	Command to rotate		Works with -n and -m options. Currently used by the Amazon credentials rotation
-y --proxy-settings	show, -show test, -test remove, -remove	Displays, updates, tests, or removes proxy settings	<code>./scconfig -y show</code> <code>./scconfig -y http://1.2.3.4:3128</code> <code>./scconfig -y -test</code> <code>./scconfig -y -remove</code>	Test option will test the connectivity through proxy to the Management Server.

Specifying Amazon Credential Keys Rotation

Use the following script to rotate the old credential keys with new ones.

```
$ scconfig.sh -z -m
access_id=<OLD_ACCESS_ID>,secret_key=<OLD_SECRET_KEY> -n
access_id=<NEW_ACCESS_ID>,secret_key=<NEW_SECRET_KEY> -x
<PASSPHRASE>
```

For Windows, use `scconfig.exe` instead of `scconfig.sh` in the above script.

Updating the Volume List

Execute the command below to update the Web Console "Devices" page with the current list of data storage devices in your CSP environment (see [Configuring a Data Storage Device](#) on page 5-3).

```
scconfig -k
```

Auto-configuring the Runtime Agent

To auto-configure the Runtime Agent, run the following script:

```
./scconfig.sh -c Amazon-AWS -o
"access_id=<AWS_ACCESS_ID>,secret_key=<AWS_SECRET_KEY>" -g
$SC_ACCOUNT_ID -s -x $PROV_PASSWORD -q
```

Performing an Auto Batch Provision of Devices

Using the following Configuration Tool script, you can provision multiple devices at the same time:

```
[device1]
id=vol-xxxxxx
mountpoint=/mnt/sc_test1
filesystem=ext3
access=readWrite
```

```
os=linux
keysize=128
[device2]
id=vol-yyyyyyyyy
mountpoint=/mnt/sc_test2
filesystem=ext3
access=readWrite
os=linux
keysize=128
..
..
..
```

Under each device [deviceN] where N is the sequence number, create a section for each device.

Next, run the following Configuration Tool script:

```
./scconfig.sh -o
"access_id=<AWS_ACCESS_ID>,secret_key=<AWS_SECRET_KEY>" -d
devices.conf -x $PROV_PASSWORD -q
```

Proxy Server Support for the Runtime Agent

SecureCloud enables you to setup a proxy server for the Runtime Agent, either on an authenticated or unauthenticated connection. SecureCloud also supports both the HTTP and HTTPS protocols for a proxy server.

Using the Configuration Tool, you can add and show the proxy server settings. You can also test the proxy server connection. Finally, you can remove the proxy server from the Runtime Agent.

Note: Proxy support is only available for a Runtime Agent built upon Python 2.6.

When the Runtime Agent is running in either of the following guest operating systems (32- and 64-bit versions), proxy server for the Runtime Agent is supported:

- Windows 7 Ultimate
- Windows Server 2003 R2 Datacenter SP2
- Windows Server 2008 R2 Datacenter SP2
- Windows Server 2008 Datacenter SP2
- Ubuntu 10
- Ubuntu 11
- Centos 6
- RHEL 6
- SUSE 11

Adding a Proxy Server

At Runtime Agent installation, there is no option to configure a proxy server. Therefore, adding a proxy server is done after Runtime Agent installation using the Configuration Tool.

Procedure:

- To add a proxy server using an authenticated connection, use the following Configuration Tool command with either the http or https protocol:

```
scconfig -y <proxy setting>  
https:\\<username>:<password>@<hostname>:port
```
- To add a proxy server using an unauthenticated connection, use the following Configuration Tool command with either the http or https protocol:

```
scconfig -y <proxy setting> https:\\<hostname>:port
```

Note: Set the `https_proxy` environment variable in the `.bashrc` file in the Linux system.

You can also configure the proxy settings using the `https_proxy` environment variable, with the same values and in the same format as the above two scenarios. For example:

```
export
https_proxy='https://<username>:<password>@<hostname>:port%root
/.bashrc
```

Viewing the Proxy Server Settings

Use the following Configuration Tool command to view the proxy server settings specified when adding a proxy server:

```
scconfig -y show
```

Note: The `scconfig -y show` command cannot be used on the proxy server configured with the `https_proxy` environment variable.

Testing the Proxy Server Connection

Use the following Configuration Tool command to test the proxy server connection:

```
scconfig -y test
```

Note: The proxy server configured with the `https_proxy` environment variable cannot be tested using the `scconfig -y test` command.

If the proxy server test fails, check your proxy settings, `scconfig.log`, or the proxy server log.

Removing Proxy Information from the Runtime Agent

Use the following Configure Tool command to remove the proxy server information from the Runtime Agent:

```
scconfig -y remove
```

Note: The proxy server configured with the `https_proxy` environment variable cannot be removed using the `scconfig -y remove` command.

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.

Configuration Tool

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

Device 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.

ICM

Integrity Check Module (ICM) is a module running inside the Runtime Agent that checks the integrity of security products within a machine instance.

See Also:

- [Scheduling an Integrity Check](#) on page 4-4

Instance

A running machine image in the cloud service provider environment.

IPv4

IPv4 is a connectionless protocol for use on packet-switched Link Layer networks (e.g., Ethernet). It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).

IPv6

IPv6 is an Internet layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks. IPv6 simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers. Network security is also integrated into the design of the IPv6 architecture, and the IPv6 specification mandates support for IPsec as a fundamental interoperability requirement.

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), Eucalyptus Machine Image (EMI), and vCloud Machine Image. 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.

Configuration Tool

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.

RAID

SecureCloud supports the Redundant Array of Inexpensive Disks (RAID) for the RAID 0 level. With this support, you can have multiple encrypted devices in a RAID controlled by a single encryption key.

RAID 0—Provides block-level striping without parity or mirroring. This RAID level splits data evenly across two or more disks (striped) with no parity information for redundancy. RAID 0 was not one of the original RAID levels and provides no (or zero) data redundancy. It provides improved performance and additional storage, but no fault tolerance.

A RAID 0 can be created with disks of differing sizes, but the storage space added to the array by each disk is limited to the size of the smallest disk. For example, if a 120 GB disk is striped together with a 100 GB disk, the size of the array will be 200 GB.

Runtime Agent

This agent is installed inside the production virtual machines 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 (ICM) and 3) credential validation and key acquisition module.

Salt (cryptography)

A salt is used in cryptography to make decryption less efficient for attackers by adding another hashing layer on top of an encryption algorithm. When a passphrase is used to encrypt data, a salt can be additional data that gets concatenated to the passphrase or key. This means that the attacker's dictionary now needs to contain many more entries, one for each possible salt value for each probable passphrase.

Salts are implemented as random bits. They are used as a second argument along with the passphrase in a function that is used to derive a decryption key.

SecureCloud Web Console

The Web-based user interface to the Management Server.

Index

Symbols

"Password Reset Verification" email B-3

A

account ID 1-11

account name, definition of G-1

activation code 7-8, B-1

administrator user role 7-3

Adobe Reader 6-5

Advanced Encryption Standard (AES) 5-7

AES 5-7

AES 256 B-4

AES 256 encryption B-2

AES encryption 1-3

agent build A-7

agent events 6-6

AIM A-4

Amazon EC2 1-2

Amazon environment 5-10

Amazon Identity Manager (AIM) A-4

Amazon Web Services (AWS) E-1

API B-2

apt-get tool A-9

auditor user role 7-3

AWS E-1

B

beta license B-2

bundling, definition of G-1

C

catastrophic failure 7-10

CBC 5-7

CentOS 5.4 1-3

Cipher 5-7

Cipher Block Chaining (CBC) 5-7

Click here link 2-2

Cloud providers

 Amazon EC2 1-2

 Eucalyptus 1.6 1-2

 Eucalyptus 2.0 1-2

 VMware vCloud 1-2

cloud service provider documentation 5-6

command shell A-13

command-line parameters 5-2

configuration file 5-11

Configuration Tool 1-11, 5-2, 5-10, A-4

Configuration Tool, definition of G-1

contact

 general information C-3

CPU 1-2

crypto engine 1-5

CSV file 6-6

D

data analyst user role 7-3

data center B-3

data storage device statuses 5-4

decryption key 4-15

Deep Security Manager (DSM) 1-5

device statuses 5-4

DSM 1-5, 4-1

E

email 2-2

email Technical Support C-2

encryption key 2-9, 4-15

encryption key statuses 3-2

encryption key, credential information 4-12

encryption key, definition of G-1

Enter a new code link 7-9, B-1

Eucalyptus 1.6 1-2

Eucalyptus 2.0 1-2

Eucalyptus environment 5-10

Events

- agent 6-6

- key action 6-6

- policy 6-6

- user 6-6

Excel 6-2, 6-4

Excel icon 6-5

export log data 6-6

EXT3 5-4

F

FAQs C-2

FAT32 5-4

FDE 1-5

FIPS 140-2 1-5

Firefox 1-2

Forgot your password? link B-3

Full Disk Encryption (FDE) 1-5

G

guest operating systems 1-3

H

Hash 5-7

hot tips C-2

HTTP D-1

HTTPS B-2, D-1

hypervisor B-2

hypervisor, definition of G-2

I

ICM 4-2

icons

- Excel 6-5

- PDF 6-5

Installation Wizard A-12—A-13

installation wizard 1-11

Instance types 1-2

instance, definition of G-2

Integrity Check Module (ICM) 4-2

integrity ratings 3-3

Internet Explorer 1-2

IPv6 1-5

J

JavaScript 1-2

K

key action events 6-6

key approver user role 7-3

key exporter utility 7-12

key management 1-4, B-4

key request 2-10

keys

- decryption 4-15

- encryption 4-15

Knowledge Base xii, C-2

Knowledge Base URL C-3

L

links

- Click here 2-2

- Enter a new code 7-9, B-1

- Forgot your password? B-3

- Pending 3-3

log-level verbosity D-2

lower-case character 2-2

M

machine image, definition of G-3

main menu 2-3

Management Server 1-12, 2-8, 4-3, 4-15, 5-2,
5-10—5-11, 8-2

Management Server, definition of G-3

Microsoft Excel 6-7

Microsoft Excel (XLS) 6-2, 6-4

Minimum password criteria validation indicator 2-2

MSI file B-4

MultiCloud Marketplace RightScripts E-3

N

NTFS 5-4

O

online help xii

operating systems 1-3

P

password 2-2

password requirements 7-4

password reset B-3

PDF 6-2, 6-4

PDF icon 6-5

Pending link 3-3

policy events 6-6

policy, definition of 2-9

preventive antivirus advice C-2

private key and certificate files, definition of G-3

production license B-2

product-registration process 2-2

Q

Quick Reference Guide xii

R

RAID Array ID 5-9

RAID, definition of G-3

readme xii

reseller B-2

resource pooling 4-5

resource pools 5-10

role-based management 1-3

rules 3-5

Deep Security Status rule 4-12

Device Access Type rule 4-12

Device Mount Point rule 4-12

rules for encryption key approval 4-1

Runtime Agent 1-2, 2-9, A-1

Configuration Tool G-1

encryption key approval process 4-15

heartbeat 3-1

installing in machine image 5-2

log files location D-2

log recording level D-2

Resource Pool 4-3

vCloud Director D-1

vCloud log recording level D-2

Windows environment A-13

runtime agent, definition of G-4

S

SaaS 1-2, 1-8, 1-12

SaaS solution B-3

scan engine refinements C-3

scconfig.sh 8-6

SecureCloud installation folder D-2

SecureCloud Key Manager 1-7

SecureCloud RightScripts E-3

SecureCloud Web console, definition of G-4

Security Administrator 7-12

security administrator user role 7-3

server farm 4-13

sha1 5-7

special characters 2-2

SSL 1-4, B-4

Support

 contacting C-2

support by email C-2

T

TCP ports D-1

Technical Support A-13

 contacting C-2

Trend Micro

 contact information C-3

Trend Micro Encryption Module 1-5

TrendEdge C-2

TrendLabs C-3

trial license B-1

U

Ubuntu 9.10 1-3

upper-case character 2-2

user events 6-6

user roles 2-4

 administrator 7-3

 auditor 7-3

 data analyst 7-3

 key approver 7-3

 security administrator 7-3

UTC time zone B-2

V

vApps D-1

vCD D-1

vCD IP address D-1

vCloud Director D-1

virtual-core processor 1-2

Virus Doctor. See TrendLabs

virus pattern file updates C-3

VMware vCloud 1-2

W

Windows Server 2003 1-3

Windows Server 2008 1-3

X

XFS 5-4

XLS 6-2, 6-4

Y

yum tool A-9