TREND MICRO™

SecureCloud™ 1.1

Private Security for the Public and Private Clouds

SaaS

Quick Reference 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 - 2011 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. APEM14801/110224

Release Date: February, 2011

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* in the Administrator's Guide.

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

Welcome to the *Trend Micro™ SecureCloud™ Quick Reference Guide* for the 1.1 release of SecureCloud SaaS. This guide provides high-level procedures describing how to upgrade to SecureCloud 1.1 and how to perform the basic product operations.

Note: Because of the high-level nature of the document, refer to the Administrator's Guide for complete details when instructed.

This guide contains the following sections:

- *Upgrading to SecureCloud 1.1*
- *Summary of Operations*

Upgrading to SecureCloud 1.1

Upgrading from a Trial License

If you want to continue using SecureCloud after your trial license has expired, you need to get a standard license from your reseller and from this license, specify the activation code in the License page. See *How do I Upgrade from a Trial License?* in the Administrator's Guide.

Upgrading from SecureCloud 1.0 (Windows Environment)

1. Remove SecureCloud 1.0 Runtime Agent.

   See *Uninstalling the Runtime Agent from a Windows Environment* in the Administration's Guide.

2. Install SecureCloud 1.1 Runtime Agent.

   See *Installing the Runtime Agent in a Windows Environment* in the Administration's Guide.

Upgrading from SecureCloud 1.0 (Linux Environment)

Run the SecureCloud 1.1 Runtime Agent installation wizard. See *Installing the Runtime Agent in a Linux Environment* in the Administrator's Guide. The wizard upgrades SecureCloud 1.0 to the 1.1 version.

Upgrading from a Beta License

There is no migration between the SecureCloud SaaS Beta and SecureCloud SaaS Production. Trend Micro recommends that you only use test data while testing the SecureCloud SaaS Beta product, as the SecureCloud SaaS product receives more frequent updates during Beta than the On-Premise product.

To start using the SecureCloud SaaS Production product, complete the following steps:

1. Remove SecureCloud Beta Runtime Agent.

   See *Uninstalling the Runtime Agent from a Windows Environment* in the Administration's Guide.

2. Install SecureCloud Production Runtime Agent.

   See *Installing the Runtime Agent in a Windows Environment* in the Administration's Guide.

Summary of Operations

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

Step 1. Register your SecureCloud product with Trend Micro.

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

See *Registering the SecureCloud Product* in the Administrator's Guide.

Step 2. Create a data storage device.

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

See *Creating a Data Storage Device in Your Cloud Service Provider Environment* in the Administrator's Guide and your cloud service provider documentation for details.

Step 3. For vCloud, complete the following steps for the machine image, Runtime Agent, and data storage device:

a. Prepare a machine image.

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

Note: You need to add an additional data storage device for encryption. 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.

c. Encrypt and register the data storage device with SecureCloud.

This is done by the Provisioning Service. From the SecureCloud Web Console, the application uses the Provisioning Service to encrypt and register selected data storage devices using the device key issued from SecureCloud Management Server. This process will not complete until you restart the SecureCloud service in the exact machine image. Once complete, machine images registered with the SecureCloud Management Server can access encrypted data.

See Chapter 8, *Provisioning for Data Storage Encryption* in the Administrator's Guide.

Continue with *Step, 6 Create policies.* on page 5.

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

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

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

Step 5. Prepare a machine image.

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

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

a. Install SecureCloud Runtime Agent in the machine image.

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

b. Register the machine image.

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

See *Registering a Machine Image* in the Administrator's Guide.

Note: The SecureCloud Configuration Tool is only used for machine images in the Amazon and Eucalyptus environments.

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

---

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

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

See your cloud service provider 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* in the Administrator's Guide.

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* and *User Role Management* in the Administrator's Guide.

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* in the Administrator's Guide.

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 *Viewing and Changing Data Storage Device Information* in the Administrator's Guide 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* in the Administrator's Guide.

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* in the Administrator's Guide.

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* in the Administrator's Guide.

Note: To obtain trouble-shooting information regarding log-management issues, see Appendix D, Basic *Troubleshooting Information* in the Administrator's Guide.