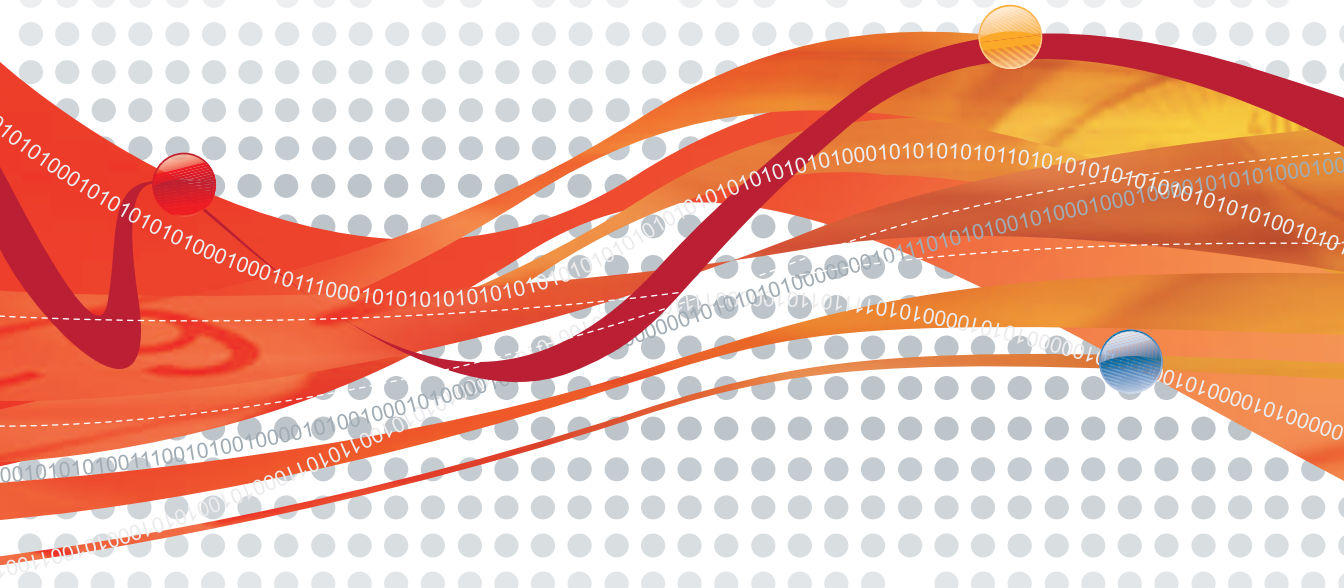
TREND MICRO

Trend Micro Security[1]

For Enterprise and Medium Business

for Mac

Installation and Configuration Worksheet



Endpoint Security

Document Part No.: TSEM14894/110621

Release Date: June 2011

The user documentation for Trend Micro Security *for Mac* introduces the main features of the software and installation instructions for your production environment. Read through it before installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Please evaluate this documentation on the following site:
http://www.trendmicro.com/download/documentation/rating.asp

Introduction

This document provides a checklist of items to guide you in setting up and configuring Trend Micro™ Security *for Mac*. See the *Administrator's Guide* for detailed information on setup and configuration tasks.

Server Installation

Before installing the Trend Micro Security server, carefully review the items in this worksheet to speed up the installation of the server and avoid installation issues.

TABLE 1-1. Server installation worksheet

INSTALLATION ITEM	REQUIREMENTS/ RECOMMENDATIONS/NOTES	YOUR INFORMATION
Computer name or IP address	--	
RAM	512MB minimum, 1GB recommended	
Available disk space	1.5GB minimum if the OfficeScan™ server is installed on the system drive (usually, C: drive) If the OfficeScan server is not installed on the system drive: • 600MB minimum on the drive where the OfficeScan server is installed. The Trend Micro Security server will be installed on this drive. • 900MB minimum on the system drive. Third-party programs used by Trend Micro Security server will be installed on this drive.	

TABLE 1-1. Server installation worksheet

INSTALLATION ITEM	REQUIREMENTS/ RECOMMENDATIONS/NOTES	YOUR INFORMATION
Other system requirements	• Microsoft™ .NET Framework 2.0 SP2 • Java runtime environment™ (JRE) 1.6 Update 14 or above on computers running Windows Server 2008	
OfficeScan server	• 10.6 • 10.5 • 10.0 • 8.0 Service Pack 1	
User name and password used to log on to the OfficeScan server Web console	Open the Web console on the computer where the OfficeScan server is installed. Trend Micro Security server will not be installed successfully if you open the console on another computer and run the Trend Micro Security server installation from there. If you are running OfficeScan 10 or later, use any of the following accounts to log on to the console: • root account • built-in administrator account • custom user account with "configure" access to Plug-in Manager Use an account with administrator privileges when logging on to the computer.	

TABLE 1-1. Server installation worksheet

INSTALLATION ITEM	REQUIREMENTS/ RECOMMENDATIONS/NOTES	YOUR INFORMATION
OfficeScan server installation folder	The default folder is C:\Program Files\Trend Micro\OfficeScan. Trend Micro Security installation files will be copied to C:\Program Files\Trend Micro\OfficeScan\Addon\TMSM. You cannot specify a different folder to which to copy the files.	
Plug-in Manager	• 2.0 • 1.0 with the latest patch	

Update source (Trend Micro ActiveUpdate server or custom update source)	• Internet connection is required if the update source is the Trend Micro ActiveUpdate server. Include proxy settings if connecting through a proxy server.
	• The following items are required if the update source is a custom update source:
	  • Latest version of OSCE_AOS_COMP_LIST.xml
	  • Trend Micro Security installation package	

Activation Code for an evaluation or full version license	Valid Activation Code with 31 alphanumeric characters specified in the following format: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX	
Number of seats for the Activation Code	--	

Client Installation

Before installing the Trend Micro Security client, carefully review the items in this worksheet to speed up the installation of the client and avoid installation issues.

TABLE 1-2. Client installation worksheet

INSTALLATION ITEM	REQUIREMENTS/ RECOMMENDATIONS/NOTES	YOUR INFORMATION
Computer name or IP address	--	
Operating system	• Mac OS™ X Lion 10.7 or later • Mac OS X Snow Leopard™ 10.6 or later • Mac OS X version 10.5.7 (Leopard™) or later • Mac OS X version 10.4.11 (Tiger™) or later	
Processor	PowerPC™ or Intel™ core processor	
RAM	256MB minimum	
Available disk space	30MB minimum	
Others	• Java for Mac OS X 10.7 • Java for Mac OS X 10.4, Release 9 • Java for Mac OS X 10.5, Update 4	
Client-server communication settings (configured on the Trend Micro Security server Web console)	• Trend Micro Security server name or IP address • Listening port (the default port is 61617) • (Optional) Proxy settings	

TABLE 1-2. Client installation worksheet

INSTALLATION ITEM	REQUIREMENTS/ RECOMMENDATIONS/NOTES	YOUR INFORMATION
Client installation package	To obtain the package, open the Trend Micro Security Server Web console, navigate to **Administration > Client Setup Files**, and click the link under **Client Installation File**.	
Launching the installation package	The files on the package may become corrupted if users launch the package using archiving tools not built-in on the Mac. Instruct users to launch the package using built-in archiving tools, such as Archive Utility.	
Firewall in use in the server computer	The firewall should not block client-server communication through the listening port.	
Personal firewall in Mac OS X	If the personal firewall option **Set access for specific services and applications** is enabled, instruct users to allow connections to **icorepluginMgr** when prompted by the system. icorepluginMgr is used to register the client to the server.	

Server Configuration

The default settings that ship with this product should be able to provide adequate protection on client computers. Use the information below as an additional reference to enhance security or achieve better performance. Some of the recommendations provided below are the default settings for the product.

TABLE 1-3. Server configuration worksheet

CONFIGURATION ITEM	RECOMMENDATIONS	YOUR INFORMATION
Manual Scan Settings		
Scan compressed files	Enabled Add compressed files or file extentions you do not want scanned to the scan exclusion list.	
CPU usage	Low This setting helps minimize computer slowdown when scanning occurs during peak hours. To improve performance, consider running Manual Scan during off-peak hours.	
Action	Use ActiveAction	
Real-time Scan Settings		
Real-time Scan	Enabled	
User activity on files	Scan files being created/modified and retrieved/executed This option ensures that files introduced to and originating from the computer are safe to access.	

TABLE 1-3. Server configuration worksheet

CONFIGURATION ITEM	RECOMMENDATIONS	YOUR INFORMATION
Scan compressed files	Enabled Add compressed files or file extentions you do not want scanned to the scan exclusion list.	
Action	Use ActiveAction	
Display a notification message when a security risk is detected	Enabled Notifications allow users to take immediate action. Consider disabling only if the notifications are generating a large number of support calls.	
Scheduled Scan Settings		
Scheduled Scan	Enabled	
Schedule	Weekly Schedule the scan during off-peak hours to improve the scanning performance and avoid potential computer slowdown.	
Scan target	File types scanned by IntelliScan IntelliScan improves performance by only scanning types known to potentially carry malicious code. Using this setting also allows you to utilize true file-type scanning.	
Scan compressed files	Enabled Add compressed files or file extentions you do not want scanned to the scan exclusion list.	

TABLE 1-3. Server configuration worksheet

CONFIGURATION ITEM	RECOMMENDATIONS	YOUR INFORMATION
CPU usage	Low This setting helps minimize computer slowdown when scanning occurs during peak hours.	
Action	Use ActiveAction	
Allow users to postpone or cancel Scheduled Scan	Disabled Users may cancel the scan if this setting is enabled. Consider enabling only on selected computers. For example, enable the option on a shared computer used for presentations. This allows the user to cancel the scan if scanning will occur during a presentation.	
Scan Exclusion Settings		
Scan exclusions	Enabled Database and encrypted files should generally be excluded from scanning to avoid performance and functionality issues. Also add files that are causing false-positives and files that many users are reporting as safe.	
Web Reputation Settings for External Clients		
Web Reputation policy	Enabled This setting ensures that clients are protected from Web-based threats even if they are outside the corporate network.	
Security level	Medium	

TABLE 1-3. Server configuration worksheet

CONFIGURATION ITEM	RECOMMENDATIONS	YOUR INFORMATION
Web Reputation Settings for Internal Clients		
Web Reputation policy	Enabled	
Security level	Medium or Low	
Allow clients to send logs to the Trend Micro Security server	Enabled if you want to monitor Web sites that users are accessing. This setting generates traffic between the server and clients.	
Web Reputation Approved URL List		
Approved URL list	Add URLs that you or users think are safe to access. Also access the following page if you think a URL has been misclassified: http://reclassify.wrs.trendmicro.com/wrsonlinequery.aspx	
Server Updates		
Update schedule	Daily or Hourly	
Update source	Trend Micro ActiveUpdate server Setting up and maintaining a custom update source may be a tedious process and requires additional computing resources.	
Standard Notifications		

TABLE 1-3. Server configuration worksheet

CONFIGURATION ITEM	RECOMMENDATIONS	YOUR INFORMATION
Criteria	Send a notification only when the scan action was not performed successfully Select this option to limit the amount of email notifications you receive and focus only on security events that require your attention.	
Email	Add all Trend Micro Security and OfficeScan administrators in your organization as email recipients.	
Outbreak Notifications		
Criteria	Use the default settings: • Unique sources: 1 • Detections: 100 • Time period: 24 hours	
Email	Add all Trend Micro Security and OfficeScan administrators in your organization as email recipients.	
Client-Server Communication		
Server name and listening port	Avoid changing when clients have been registered to the server or clients will have to be re-deployed.	

TABLE 1-3. Server configuration worksheet

CONFIGURATION ITEM	RECOMMENDATIONS	YOUR INFORMATION
Proxy settings	Disabled Clients do not typically communicate with the server through an intranet proxy. Also avoid changing when clients have been registered to the server or clients will have to be re-deployed.	
External Proxy Settings		
Proxy settings	Enabled if the Trend Micro Security server connects to the Trend Micro ActiveUpdate server through a proxy server	
Log Maintenance		
Scheduled deletion of logs	Enabled	
Logs to delete	Logs older than 7 days	
Log deletion schedule	Weekly Schedule the deletion during off-peak hours.	