Configuration Guide

SmartConnector for Symantec Gateway Security/Enterprise Firewall NG File

November 15, 2013

ArcSight
An HP Company

Configuration Guide

SmartConnector for Symantec Gateway Security/Enterprise Firewall NG File

November 15, 2013

Copyright © 2006 – 2013 Hewlett-Packard Development Company, L.P.Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks and acknowledgements: http://www.hpenterprisesecurity.com/copyright.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is confidential.

Revision History

Date	Description
11/15/2013	Added that Solaris 11 x86 operating system is not supported by this connector.
05/15/2012	Added new installation procedure.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Global update to installation procedure.
06/25/2008	Created this configuration guide.

SmartConnector for Symantec Gateway Security/Enterprise Firewall NG File

This guide provides information for Installing the SmartConnector for Symantec Gateway Security/Enterprise Firewall NG File and configuring the device for log file event collection. Symantec Gateway Security 5000 Series v3.0, appliance 5620, is supported. Solaris 11 x86 is not a supported platform for this connector.

See the section "Device Event Mapping to ArcSight Data Fields" later in this document for the specific events mapped to fields in the ArcSight database.

Product Overview

The Symantec Gateway Security appliances, running Symantec Gateway Security software, is a fully integrated appliance with firewall, VPN, antivirus, intrusion detection and prevention, content filtering, anti-spam, and high availability/load balancing.

The appliance provides access control and security enforcement on passing traffic. The rack-mountable, plug-and-protect appliances control information entering and leaving networks.

Symantec Gateway Security appliances are managed using the Security Gateway Management Interface (SGMI), which is a Web-based graphical user interface for managing and monitoring all security gateway functions.

Configuration

Configuring a Machine Account

Before installing the SmartConnector, create a new account for the machine that will host the connector. The **Machine Account** window lets you define computers other than administrator workstations and authorize them to automatically retrieve or update information on the security gateway. Depending upon the privileges you assign to the machine account, the computer represented by the account can be used to remotely view or manage log files, or to manage the security gateway's blacklist.

Perform the following steps to create an account using the Symantec Security Gateway Management Interface(SGMI):

1. In the SGMI, in the left pane, under **System**, click **Administration**.
2. In the right pane, on the **Machine Accounts** tab, click **New**.
3. In the **Machine Account Properties** dialog box, on the **General** tab, do the following:

   Enable
   To enable the machine account, check **Enable**.

   IP address
   Enter the IP address of the machine account in dotted quad format.

Password Type
Enter the password for the machine account. The password must be at least 10 characters long, contain both upper and lower case letters, at least one numeric digit, and a punctuation character. The password is encrypted and appears as a string of asterisk (*) characters.

Verify Password Type
The machine account password again for confirmation.

Last password change
The Last Password Change text box is read only; it displays the date of the most recent password change.

Caption Type
A brief description of the machine account.

View log
Check to let the remote computer view security gateway log files.

Manage log
Check to let the remote computer access and manage security gateway log files.

Provide IDS blacklist entries
Check to let the remote computer add or change entries in the Blacklist file. If you check this entry, complete the following fields:

Pass entries on port: Enter the port number to be used to connect to the blacklist.

Entry lifetime (minutes): Enter the length of time the blacklist entries are valid.

4 On the **Privileges** tab, do the following:

View log
Check to let the remote computer view security gateway log files.

Manage log
Check to let the remote computer access and manage security gateway log files.

Provide IDS blacklist entries
Check to let the remote computer add or change entries in the Blacklist file. If you check this entry, complete the following fields:

Pass entries on port: Enter the port number to be used to connect to the blacklist.

Entry lifetime (minutes): Enter the length of time the blacklist entries are valid.

5 Optionally, on the **Description** tab, enter a more detailed description than you typed in the Caption text box.

6 Click **OK**.

7 To activate your configuration, select **Activate** from the **System** menu. When prompted to save your changes, click **Yes**.

The Activation Wizard then guides you through the process of activating your changes.

Install the SmartConnector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger). This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the Connector Appliance, see the *ArcSight Connector Appliance Administrator's Guide* for instructions, and start the installation procedure at step 3.

Before installing the SmartConnector, be sure the following are available:

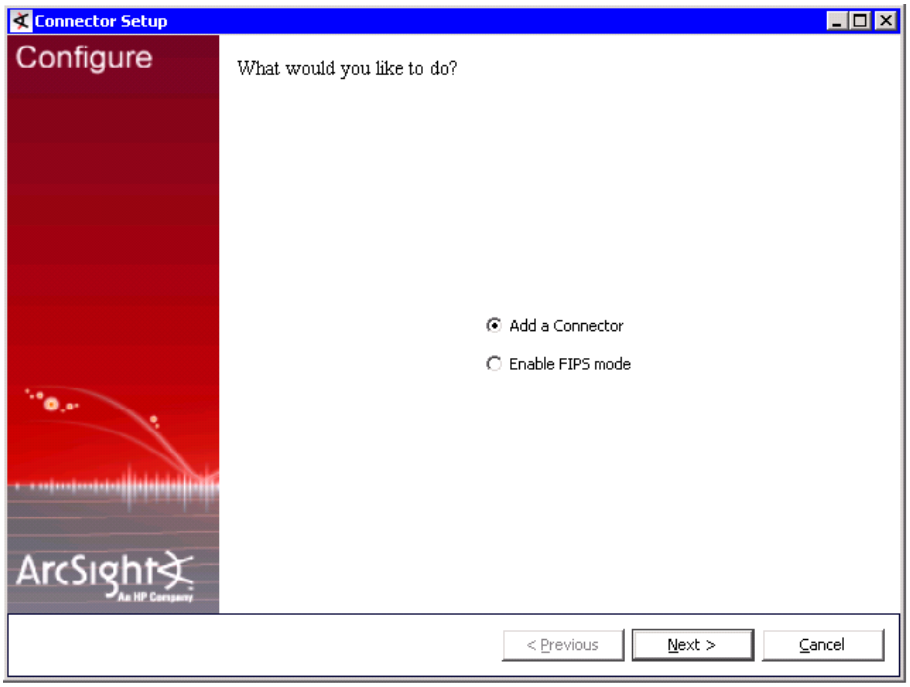
- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HP SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the HP SSO site.
2. Start the SmartConnector Installer by running the executable.

   Follow the installation wizard through the following folder selection tasks and installation of the core connector software:

   Introduction
   Choose Install Folder
   Choose Install Set
   Choose Shortcut Folder
   Pre-Installation Summary
   Installing...
3. When the installation of SmartConnector core component software is finished, the following window is displayed.



A Leave the installation wizard open. On the machine on which you are installing the connector, run the `clienrempass` utility to generate a key on the client machine.

B The passphrase is stored on the SmartConnector host in `raptor\firewall\sg\remkeys` on Windows, `/usr/adm/sg/remkeys` on Solaris, and `var/lib/sg/remkeys` on Linux. If this directory does not yet exist, create it before running `clientrempass`.

C Find the `clientrempass` utility. Open a command window in the directory `$ARCSIGHT_HOME\current\bin\agent\symantec\symantec_gs_ef__ng_file\[platform]` (where `platform` depends upon the OS, such as Win32). Run `clientrempass`.

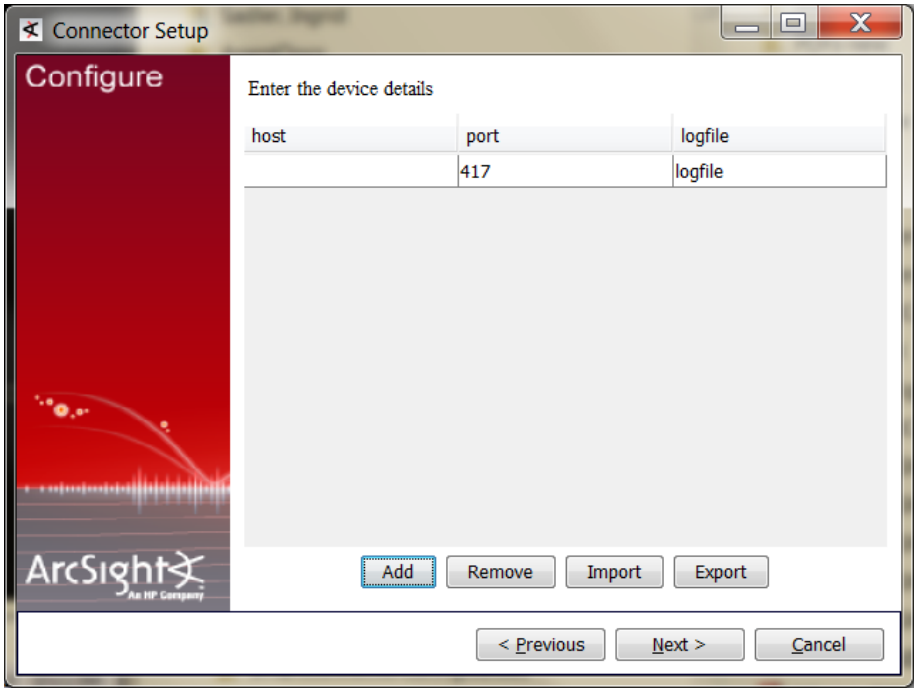
D Select option **A** to add a new host configuration and then enter the IP address of the firewall or appliance. Select option **1**, for Logfile Retrieval, and enter the port number and the exact passphrase that you entered for the client using SGMI.

E Select option **Q** to exit `clientrempass`.

4 Select **Add a Connector** and click **Next**.

5 Select **Symantec Gateway Security/Enterprise Firewall NG File** and click **Next**.

6 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

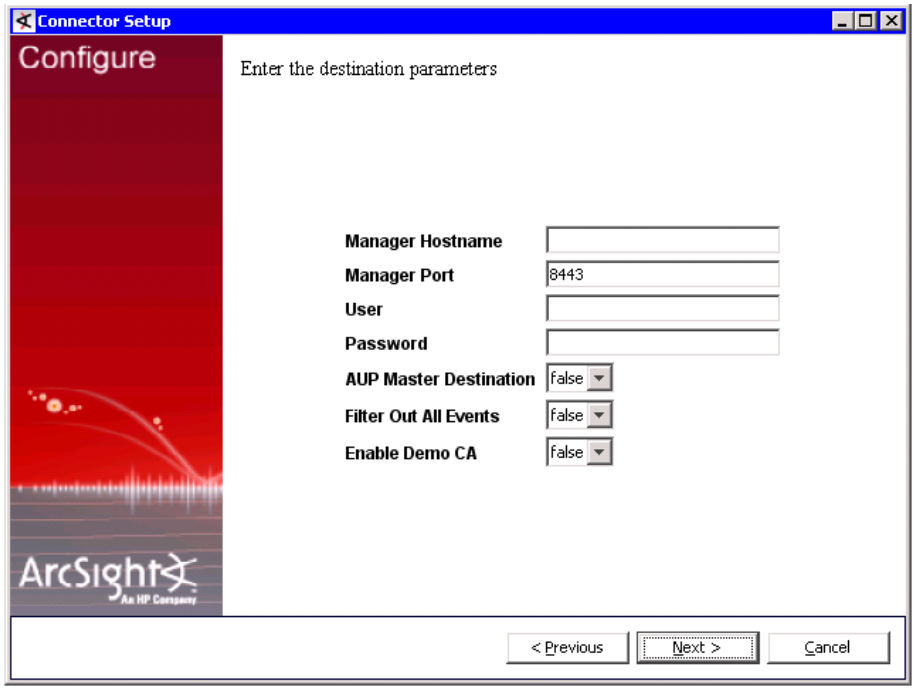


Parameter	Description
Host or IP Address	Symantec Gateway Security Appliance or Enterprise Firewall Host or IP Address.
Port	Symantec Gateway Security Appliance or Enterprise Firewall Listening Port.
Logfile	Complete path to Symantec Gateway Security Appliance or Enterprise Firewall Log Files.

You can click the 'Export' button to export the data you have entered into the table into a CSV file; you can click the 'Import' button to select a CSV file to import into the table rather than add the data manually.

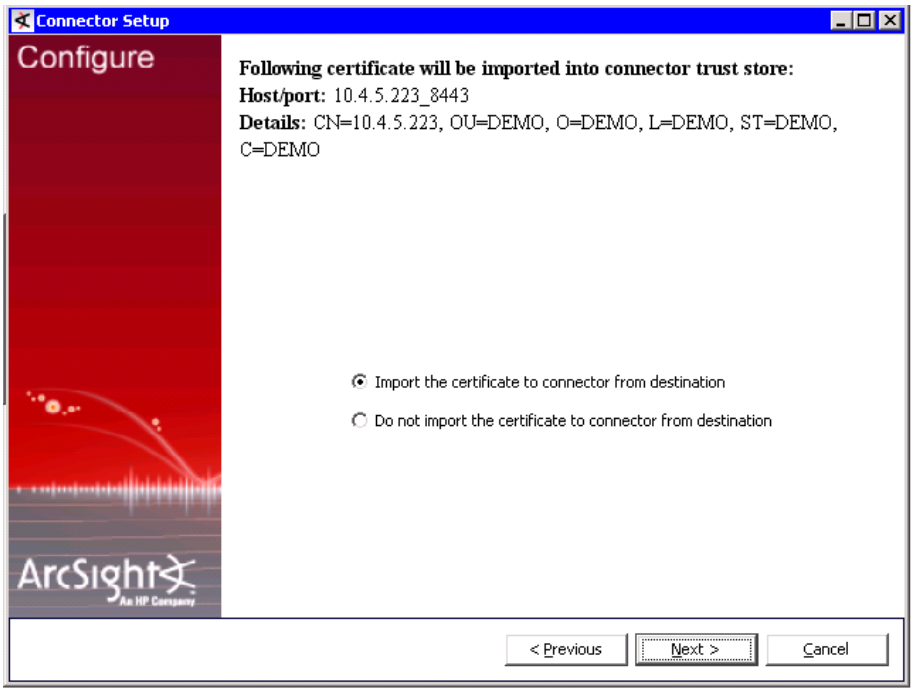
7 Make sure **ArcSight Manager (encrypted)** is selected and click **Next**. For information about the other destinations listed, see the *ArcSight SmartConnector User's Guide* as well as the Administrator's Guide for your ArcSight product.

8 Enter the **Manager Host Name**, **Manager Port**, and a valid ArcSight **User Name** and **Password**. This is the same user name and password you created during the ArcSight Manager installation. Click **Next**.



9 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**; the connector starts the registration process.

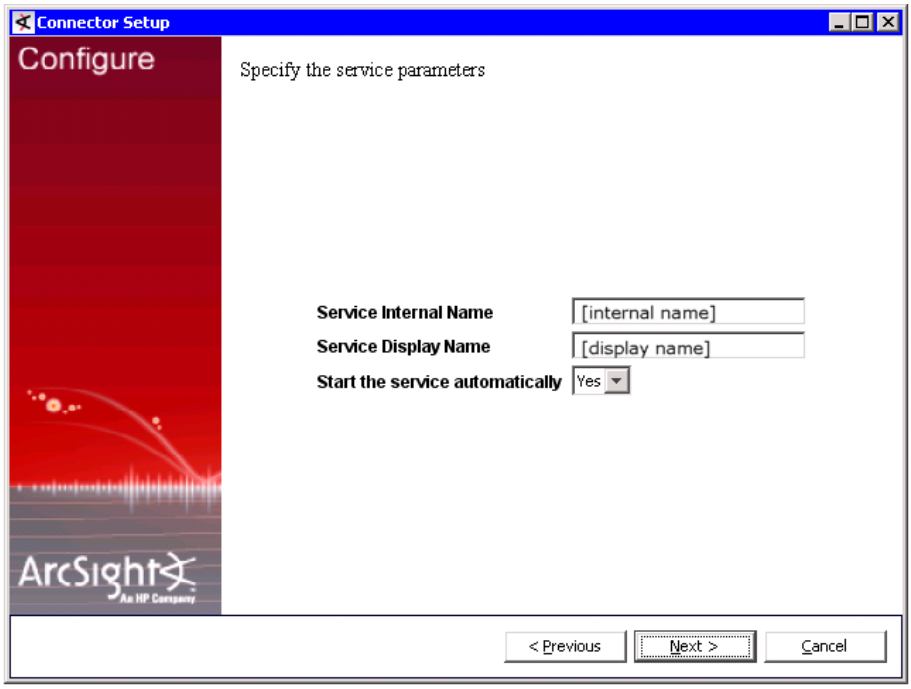
10 The certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. If you select **Do not import the certificate to connector from destination**, the connector installation will end.



The certificate is imported and the **Add connector Summary** window is displayed.

11 Review the **Add connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

12 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, skip step 13. If you choose to run the connector as a service, the wizard prompts you to define service parameters. See "Run the SmartConnector" later in this guide for more information.



13 Enter the service parameters and click **Next**. The **Install Service Summary** window is displayed.

14 Click **Next**.

To complete the installation, choose **Exit** and click **Next**. To enable FIPS-compliant mode, choose **Continue**, click **Next**, and continue with "Enable FIPS Mode."

Enable FIPS Mode

15 After choosing **Continue** and clicking **Next** after connector installation, choose **Enable FIPS Mode** and click **Next**. A confirmation window is displayed when FIPS mode is enabled.

16 Click **Next**. To complete installation of FIPS support, click **Exit**. To enable FIPS Suite B mode, click **Continue**.

17 On the window displayed, select **Modify Connector**.

18 Select **Add, Modify, or remove destinations** and click **Next**.

19 Select the destination for which you want to enable FIPS Suite B mode and click **Next**.

20 Select **Modify destination parameters** and click **Next**.

21 When the parameter window is displayed, select **FIPS with Suite B 128 bits** or **FIPS with Suite B 192 bits** for the **FIPS Cipher Suites** parameter. Click **Next**.

22 The window displayed shows the editing changes to be made. Confirm and click **Next** to continue. (To adjust changes before confirming, click **Previous**.)

23 A summary of the configuration changes made is displayed. Click **Next** to continue.

24 Click **Exit** to exit the configuration wizard.

For some SmartConnectors, a system restart is required before the configuration settings you made take effect. If a **System Restart** window is displayed, read the information and initiate the system restart operation.

Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

Complete any **Additional Configuration** required, then continue with the "Run the SmartConnector."

For connector upgrade or uninstall instructions, see the *SmartConnector User's Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *HP ArcSight SmartConnector User's Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Symantec Gateway Security Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	Protocol
Base Event Count	Message Count
Bytes In	Received
Bytes Out	Sent
Destination Address	Destination IP

ArcSight ESM Field	Device-Specific Field
Destination Host Name	Destination Name
Destination Port	Destination Port
Destination User Name	User
Device Action	Operation
Device Custom Date 1	Date
Device Custom String 1	Rule or Rule ID
Device Custom String 2	Feature ID
Device Custom String 3	Key
Device Custom String 4	Rule
Device Custom String 5	Result
Device Event Class Id	Message Reference
Device Host Name	Source Host
Device Inbound Interface	Source Interface
Device Outbound Interface	Destination Interface
Device Process Name	Program Name or Module
Device Product	'Symantec Gateway Security/Enterprise Firewall'
Device Receipt Time	DateTime
Device Severity	Priority
Device Vendor	'Symantec'
Device Version	Version
Message	Detail or Authentication Result or Consolidated Message or Status
Name	Message Text
Raw Event	Parameters
Request URL Query	Argument
Source Address	Source Ip
Source Host Name	Source Name
Source Port	Source Port
Transport Protocol	IP Code

Tips

Make sure the necessary ***.so** files are installed when the agent is installed on Linux and Solaris platforms.

Solaris

If the following *.so files are not in **/usr/lib**, copy them from the related agent installation folder as follows:

Copy **libSesaXmlPardser.so** and **libxerces-c.so.25** to **/usr/lib** from `<arcsight_home>/current/bin/agent/symantec/symantec_gs_ef_ng_file/solaris`

You also must create the directory **/var/lib/sg** if it does not exist.

Linux

If the following *.so libraries are not in **/lib**, copy them from the related agent installation folder as follows:

Copy **libSesaXmlParser.so** and **libxerces-c.so.24** to **/usr/lib** from `<arcsight_home>/current/bin/agent/symantec/symantec_gs_ef_ng_file/linux`

Make sure the binaries **clientrempass**, **remotelogdir**, and **remotelogfile** are executable under:

`<arcsight_home>/current/bin/agent/symantec/symantec_gs_ef_ng_file/solaris or linux`