

Security Threat Response Manager

Adaptive Log Exporter Users Guide

Release 2009.1

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Published: 2010-02-15

Copyright Notice

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense. The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Consult the dealer or an experienced radio/TV technician for help. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Configuring DSMs
Release 2009.1

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

November 2009—Revision 3

The information in this document is current as of the date listed in the revision history.

CONTENTS

ABOUT THIS GUIDE

Conventions 5
Technical Documentation 5
Contacting Customer Support 6

1 OVERVIEW

Integrating Device Support Modules (DSMs) with STRM 7
Using the Adaptive Log Exporter 8
- Using the Menu 8
- Using the Toolbar 8

Deploying Changes 9

2 INSTALLING THE ADAPTIVE LOG EXPORTER

Before You Begin 11
Installing the Adaptive Log Exporter 11
Un-installing the Adaptive Log Exporter 16

3 SETTING UP THE ADAPTIVE LOG EXPORTER

Using the Preferences Window 17
Managing Updates 18
- Configuring Adaptive Log Exporter Updates 18
- Scheduling Automatic Updates 21
- Configuring the Update Site 23
- Configuring Updates for Off-line Sites 24

4 MANAGING DEVICES

Installing Device Types 25
Updating Devices 28
Configuring Devices 30
- Adding a Device 30
- Editing a Device 32
- Deleting a Device 33

5 MANAGING DESTINATIONS

Configuring Destinations 35

Adding a Destination 35
Editing a Destination 37
Deleting a Destination 39
Mapping to a Destination 40
Creating a Mapping 40
Removing a Mapping 41

6 CONFIGURING THE CISCO ACS DEVICE

7 CONFIGURING THE CISCO CSA DEVICE

8 CONFIGURING THE FILE FORWARDER DEVICE

9 CONFIGURING THE XML FILE FORWARDER DEVICE

10 CONFIGURING THE JUNIPER SBR DEVICE

11 CONFIGURING THE WINDOWS EVENT LOG DEVICE

12 CONFIGURING THE MICROSOFT DHCP DEVICE

13 CONFIGURING THE TREND MICRO INTERSCAN VIRUSWALL DEVICE

14 CONFIGURING THE MICROSOFT EXCHANGE SERVER DEVICE
Forwarding OWA Logs 59
Forwarding SMTP Logs 60

15 CONFIGURING THE MICROSOFT SQL SERVER DEVICE

16 CONFIGURING THE MICROSOFT IIS DEVICE

17 CONFIGURING THE MICROSOFT WINDOWS IAS DEVICE

18 CONFIGURING THE MICROSOFT ISA DEVICE

A COLLECTING WINDOWS EVENT LOGS
Collecting Logs Without an Agent 70
Configuring the Adaptive Log Exporter 71
Collecting Logs With an Agent 74
Configuring the Adaptive Log Exporter 74

B ADAPTIVE LOG EXPORTER QUICK START

ABOUT THIS GUIDE

The *STRM Adaptive Log Exporter Users Guide* provides you with information for integrating Device Support Modules (DSMs) with STRM or STRM Log Manager using the Adaptive Log Exporter.

Conventions

Table 1 lists conventions that are used throughout this guide.

Table 1 Icons

Icon	Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, device, or network.
	Warning	Information that alerts you to potential personal injury.

Technical Documentation

You can access technical documentation, technical notes, and release notes directly from the Juniper Customer Support web site at https://www.juniper.net/support/. Once you access the Juniper Customer Support web site, locate the product and software release for which you require documentation.

Your comments are important to us. Please send your e-mail comments about this guide or any of the Juniper Networks documentation to:

techpubs-comments@juniper.net.

Include the following information with your comments:

- Document title
- Page number

Contacting Customer Support

To help you resolve any issues that you may encounter when installing or maintaining STRM, you can contact Customer Support as follows:

- Open a support case using the Case Management link at http://www.juniper.net/support/
- Call 1-888-314-JTAC (from the United States,Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

1 OVERVIEW

The Adaptive Log Exporter is a stand-alone application that allows you to integrate devices/applications with STRM or STRM Log Manager. This chapter includes:

- Integrating Device Support Modules (DSMs) with STRM
- Using the Adaptive Log Exporter
- Deploying Changes



Note: *Unless otherwise noted, all references to STRM refer to both STRM and STRM Log Manager.*

Integrating Device Support Modules (DSMs) with STRM

STRM can log and correlate events received from external sources such as security equipment and network equipment. The Adaptive Log Exporter enables you to forward data from Windows-based devices and applications to STRM for processing. Using the Adaptive Log Exporter, you can easily integrate Windows-based devices with STRM.

To integrate devices/applications with STRM:

Step 1 Install available device types.

For more information, see Chapter 4 Managing Devices, Installing Device Types.

Step 2 Add and configure the required devices.

For more information, see Chapter 4 Managing Devices, Configuring Devices.



Note: *Each instance of Adaptive Log Exporter can support a maximum of 20 devices.*

Step 3 Add and configure the required device destinations.

For more information, see Chapter 5 Managing Destinations, Configuring Destinations.

Step 4 Map the device to the desired destination, such as syslog or a log file.

For more information, see Chapter 5 Managing Destinations, Mapping to a Destination.

Step 5 Deploy all changes.

Using the Adaptive Log Exporter

The Adaptive Log Exporter provides menu and tool bar options. This section provides information on the available options including:

- Using the Menu
- Using the Toolbar

Using the Menu

The menu options include:

Table 1-1 Adaptive Log Exporter Menu Options

Menu	Sub-Menu	Description
File	Save	Allows you to save current changes.
	Save All	Allows you to save all changes made during the current session.
	Deploy	Allows you to deploy all changes made during the current session.
	Preferences	Allows you to configure Adaptive Log Exporter preferences. For more information, see. Chapter 3 Setting Up the Adaptive Log Exporter.
	Exit	Allows you to exit the application.
Edit	Edit Device	Allows you to edit the settings for a currently saved device. For more information, see Chapter 4 Managing Devices.
	Edit Destination	Allows you to edit the mapping destination for a device. For more information, see Chapter 4 Managing Devices.
Window	Show Views	Allows you to view the Destination or Devices tabs.
Help	Software Updates	Allows you to check for software updates. For more information, see Chapter 4 Managing Devices.
	About	Allows you to access information about the version of Adaptive Log Exporter you are using.

Using the Toolbar

The toolbar options include:

Table 1-2 Toolbar Options

Icon	Description
	Allows you to save current changes.
	Allows you to save all changes made during the current session.

Table 1-2 Toolbar Options (continued)

Icon	Description
	Allows you to edit the settings for a currently saved device.
	Allows you to edit the mapping destination for a device.
	Allows you to deploy all changes made during the current session.
	Allows you to install all available devices.

Deploying Changes

Once you configure your devices using the Adaptive Log Exporter, you must save your changes to the staging area using the Save or Save All option. Then, you must either manually deploy all changes using the Deploy menu option or, upon exit, a window appears prompting you to deploy changes before you exit. All deployed changes are then enforced.

2 INSTALLING THE ADAPTIVE LOG EXPORTER

This chapter provides information on installing and uninstalling your Adaptive Log Exporter including:

- Before You Begin
- Installing the Adaptive Log Exporter
- Un-installing the Adaptive Log Exporter

Before You Begin

Before you install the Adaptive Log Exporter, make sure you have the following:

- Windows 2000, Windows 2003, or Windows 2008 server software installed. The Adaptive Log Exporter supports 32 or 64-bit systems.
- Your system includes at least 200 MB of disk space available.
- Appropriate access to STRM. For more information regarding STRM, see the *STRM Users Guide.*
- Appropriate access to all devices and servers you want to configure. For more information, see your vendor documentation.

Installing the Adaptive Log Exporter

To install the Adaptive Log Exporter:

Step 1 Download the Adaptive Log Exporter from the Juniper Customer Support web site: **http://www.juniper.net/support/**.

Step 2 Close all other active applications before installing the Adaptive Log Exporter.

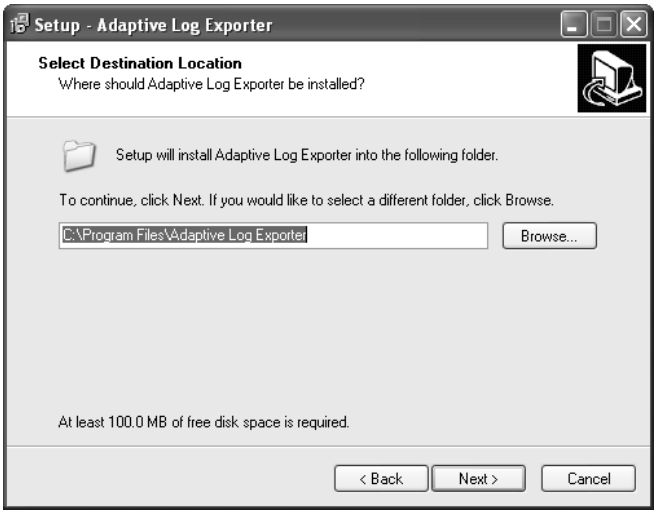
Step 3 Double-click the Adaptive Log Exporter executable.

The Welcome window appears.



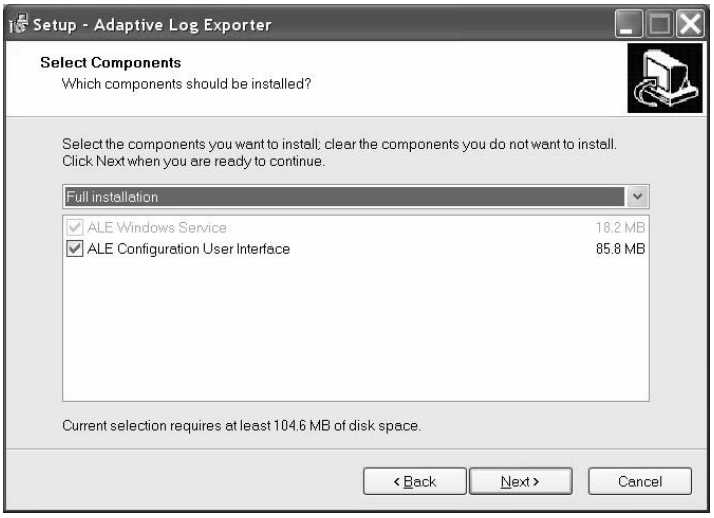
Step 4 Click **Next**.

The Select Destination Location window appears.



Step 5 Specify the location you want to install the Adaptive Log Exporter. To browse your system for a particular location, click **Browse**. Click **Next**.

The Select Components window appears.



Step 6 Using the drop-down list box, select the type of installation. The options are:

- **Full Installation** - Installs all components including the user interface and the Adaptive Log Exporter server.
- **Custom** - This option is automatically selected when any of the default check boxes are manually selected or cleared.

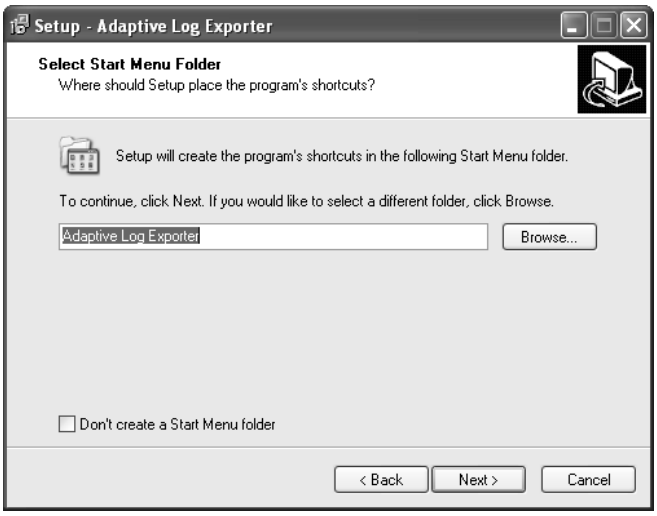
Step 7 Using the check boxes, select the desired options:

- **ALE Windows Service** - Mandatory. This option is not configurable and ensures the appropriate Adaptive Log Exporter options are installed.
- **ALE Configuration user Interface** - Installs the Java-based configuration user interface options for the Adaptive Log Exporter. Clearing this check box installs the Adaptive Log Exporter without the user interface and requires configuration using the text based configuration files.

Note: *We recommend that you install and configure the Adaptive Log Exporter using the user interface. Installing without the user interface is for advanced users only. For additional information, see Appendix B Installing and Configuring Without the Wizard.*

Step 8 Click **Next**.

The Start Menu Folder window appears.



Step 9 Specify the name of the menu option in your Start menu. If you do not want to include a menu option in your Start menu, select the **Don't create a Start Menu folder** check box. Click **Next**.

The Select Additional Tasks window appears.



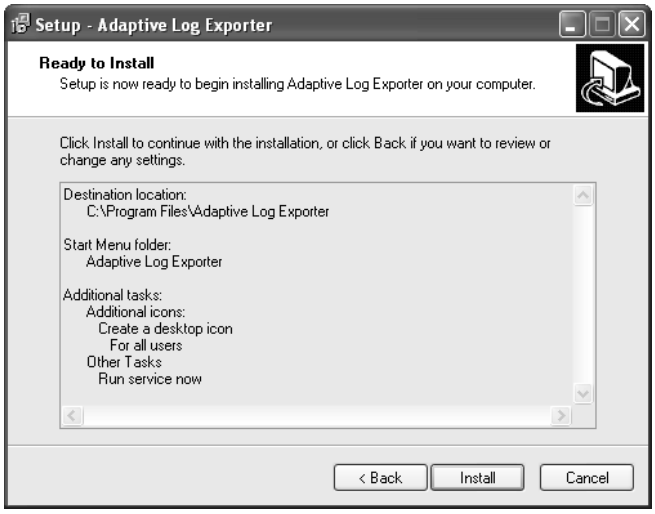
Step 10 Configure the available options:

- **Create a desktop icon** — Select the check box if you want to create an icon on your desktop for the Adaptive Log Exporter. You can also select one of the following options:
  - For all users
  - For the current user only
- **Create a Quick Launch icon** — Select the check box if you want to create an icon on your Quick Launch toolbar.

- **Run service now** — If you want to run the Adaptive Log Exporter immediately after installation, select the Run service now check box.

Step 11 Click **Next**.

The Ready to Install window appears.



Step 12 Click **Install**.

The Competing the Setup Wizard appears when the installation is complete.



Step 13 Click **Finish**.

The installation process is complete.

When the installation process completes, you must configure the location that the Adaptive Log Exporter uses for updates. For more information, see Configuring the Update Site.

Un-installing the Adaptive Log Exporter

To un-install the Adaptive Log Exporter:

Step 1 From your desktop, select **Start > Programs > AdaptiveLogExporter > Utility > Uninstall AdapterLogExporter.**

A confirmation messages appears.



Step 2 Click **Yes** to continue.

Once the process is complete, a message appears when the uninstall is complete.



Step 3 Click **Ok**.

3 SETTING UP THE ADAPTIVE LOG EXPORTER

This chapter provides information on setting up your Adaptive Log Exporter including:

- Using the Preferences Window
- Managing Updates

Using the Preferences Window

The Preferences window provides the following options:

Table 3-1 Preference Options

Menu	Sub-Menu	Description
Help		We recommend that you use the default values for the Help options.
Install/Update		Allows you to configure your update options. For more information, see Configuring Adaptive Log Exporter Updates.
	Automatic Updates	Allows you to schedule updates to your Adaptive Log Exporter. For more information, see Scheduling Automatic Updates.
	Update Site	Allows you to configure the location that the Adaptive Log Exporter uses for updates. For more information, see Configuring the Update Site.



***Note:** If you deviate from the default values of the Adaptive Log Exporter and you want to restore default values, click **Restore Defaults** in the Preferences window.*

Managing Updates

This section provides information on managing updates for your Adaptive Log Exporter including:

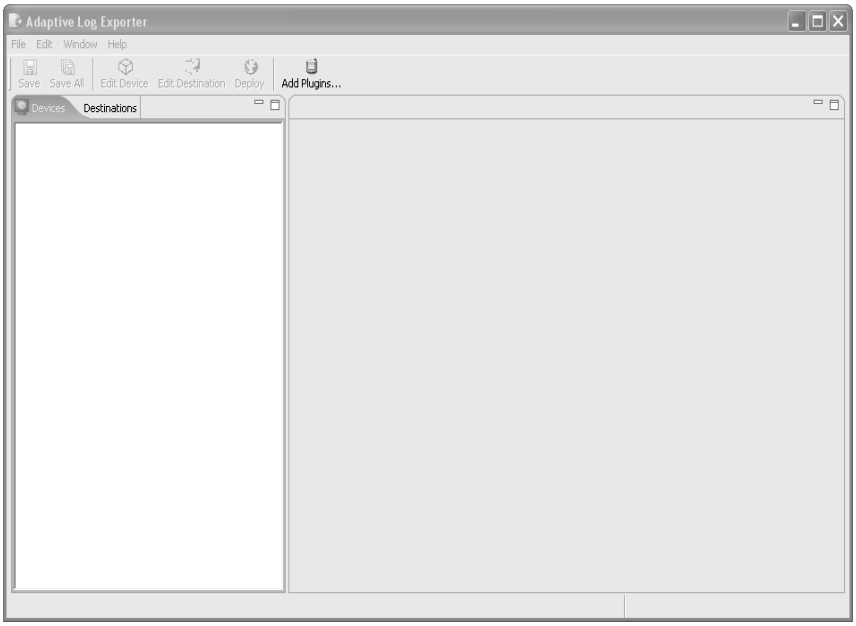
- Configuring Adaptive Log Exporter Updates
- Scheduling Automatic Updates
- Configuring the Update Site

Configuring Adaptive Log Exporter Updates

To configure the preferences for updates:

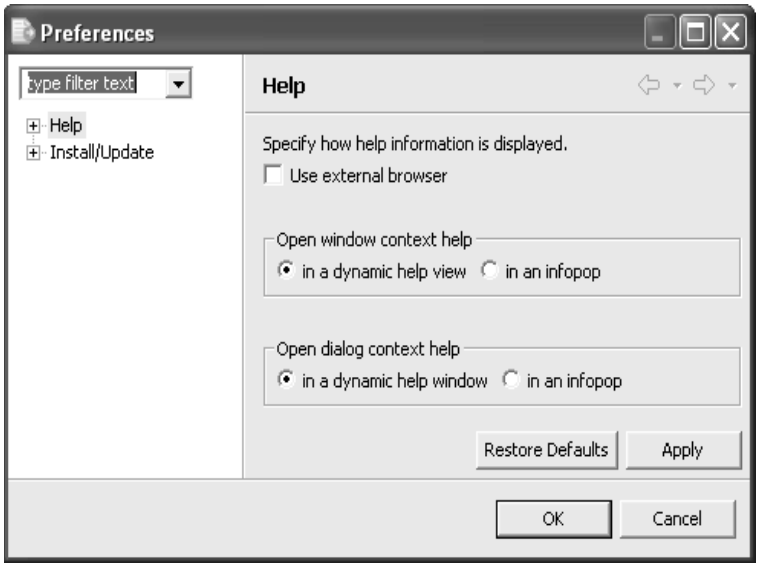
Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

The Adaptive Log Exporter appears.



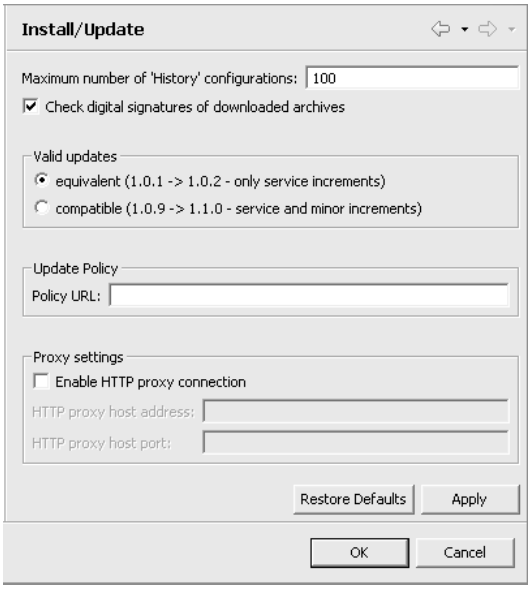
Step 2 From the menu, select **File > Preferences**.

The Preferences window appears.



Step 3 Click **Install/Update**.

The Install/Update parameters appear.



Step 4 In the Maximum number of History configurations field, enter the number of configuration changes you want the system to maintain. The default is 100.

Step 5 To ensure greater security for your downloaded archives, select the Check digital signatures of downloaded archives check box. By default, the check box is selected.

Step 6 To determine the updates you want your system to perform, choose one of the following options:

- **equivalent** — Includes updates that are equivalent with the other currently running version of the Adaptive Log Exporter. Typically, this includes plug-ins and updates.
- **compatible** — Includes updates that are available and include a new version of the application. Typically, this includes a new release of the Adaptive Log Exporter.

Step 7 To specify a specific update policy, specify a URL in the Policy URL field.

This update policy is useful if your deployment includes many Adaptive Log Exporters. If this is the case, you may need to schedule event uploads to minimize the potential high load on the network. For assistance creating a custom update policy, contact Juniper Networks Customer Support.

Step 8 To specify specific proxy settings for your updates:

a Select the Enable HTTP Proxy connection check box.

Additional fields are activated.

b In the HTTP proxy host address field, enter the IP address of the desired proxy host.

c In the HTTP proxy host port field, enter the port number of the proxy host.

Step 9 Click **Apply**.

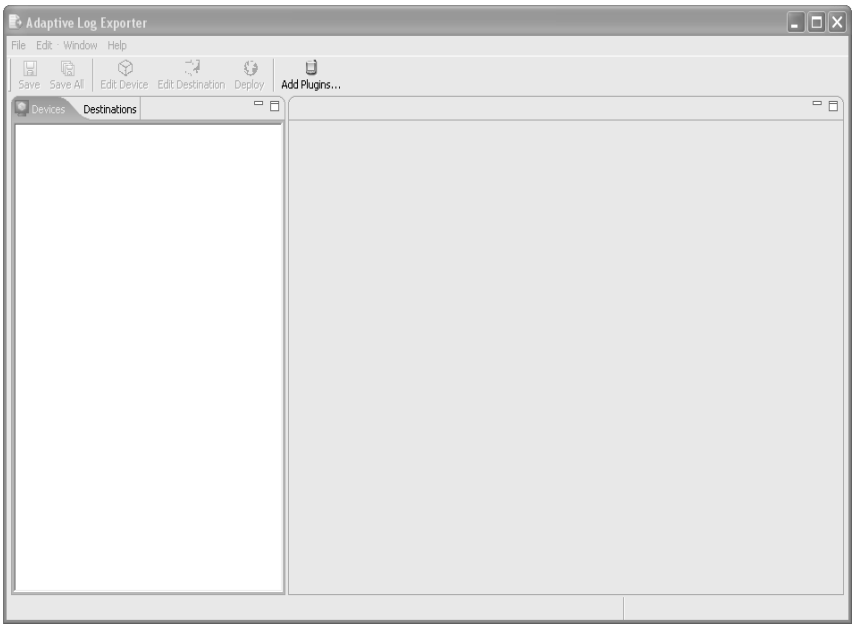
Step 10 Click **OK**.

Scheduling Automatic Updates

You can configure the Adaptive Log Exporter to automatically search for updates. To schedule updates:

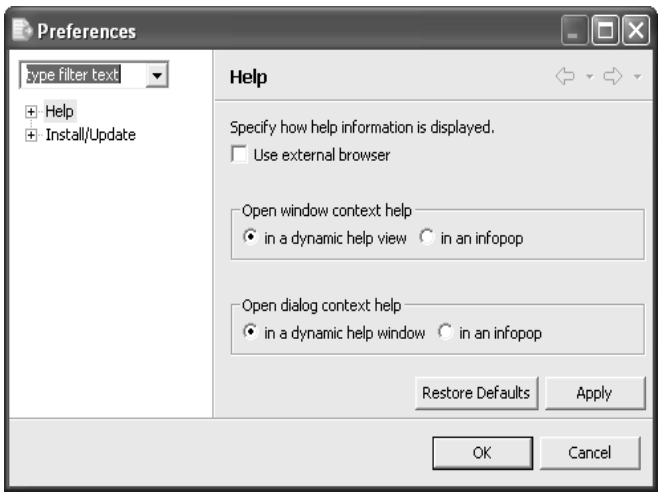
Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

The Adaptive Log Exporter appears.



Step 2 From the menu, select **File > Preferences**.

The Preferences window appears.

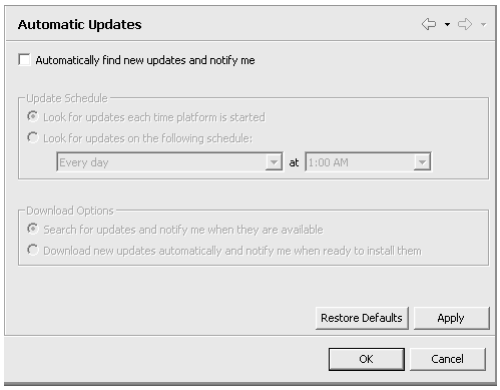


Step 3 In the left navigation pane, click the + sign next to Install/Update.

Additional menu options appear.

Step 4 Click **Automatic Updates**.

The Automatic Updates parameters appear.



Step 5 Select the Automatically find new updates and notify me check box.

Additional options become active. When updates are available, a message appears indicating the available updates.

Step 6 Select one of the following options to schedule automatic updates:

- **Look for updates each time platform is started** — Enables the system to search for updates each time you start your Adaptive Log Exporter. This is the default.
- **Look for updates on the following schedule:** — Allows you to use the drop-down list boxes to schedule a specific time for searching for updates.

Step 7 Select one of the following options for downloading updates:

- **Search for updates and notify me when they are available** — Enables the system to search for updates and provide notification when the updates are available before downloading.
- **Download new updates automatically and notify me when ready to install them** — Enables the system to search for new updates automatically and notifies you when they are ready to install.

Step 8 Click **Apply**.

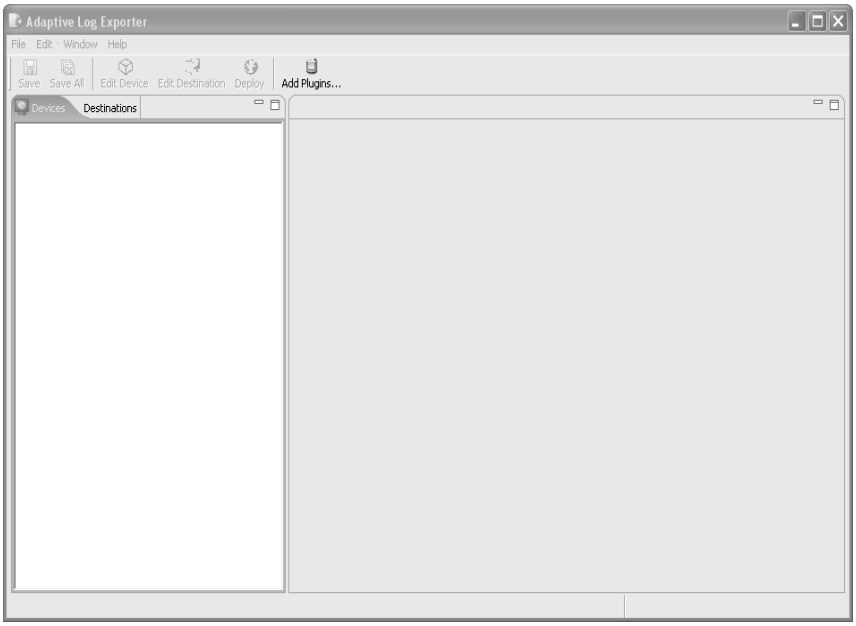
Step 9 Click **OK**.

Configuring the Update Site

To specify a specific location for the Adaptive Log Exporter to search for updates:

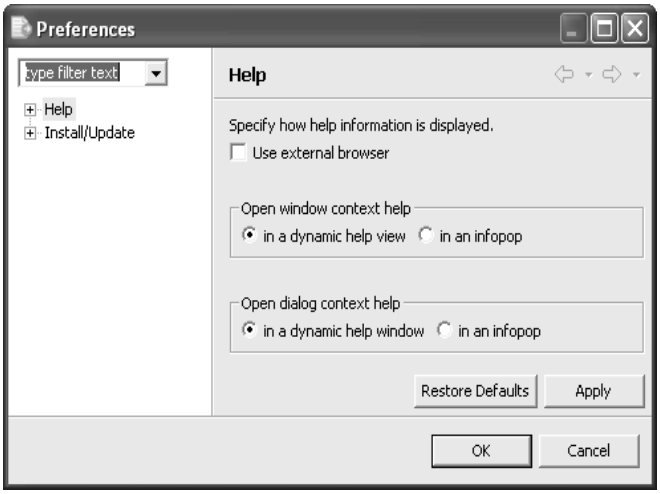
Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

The Adaptive Log Exporter appears.



Step 2 From the menu, select **File > Preferences**.

The Preferences window appears.

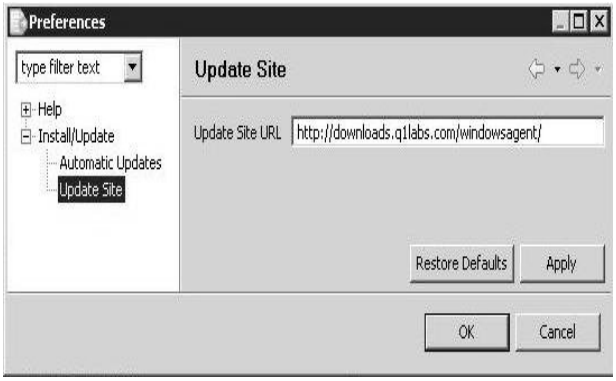


Step 3 In the left navigation pane, click the + sign next to Install/Update.

Additional menu options appear.

Step 4 Click **Update Site**.

Update Site parameters appear.



Step 5 Click **Apply**.

Step 6 Click **OK**.

Configuring Updates for Off-line Sites

To configure updates for a site that has no Internet connection:

Step 1 From a system with Internet connectivity, access the following web site.

`http://downloads.q1labs.com/windowsagent/`

Step 2 Download the following file:

`windowsagent.zip`

Step 3 Copy the file to your system without Internet connectivity on which you want to configure updates.

Step 4 Extract the file to your desired update site, for example:

`c:\updatesite`

Step 5 In the Update Site URL field, enter the location you want the Adaptive Log Exporter to use for searching for updates.

Note: *Adaptive Log Exporter supports both http and file protocols. For example, the following are valid locations:*

`http://<update.server.com>/UpdateSite`

On a Windows server:

`file:\\<SOMEWINDOWSSERVER>\ALE\UpdateSite`

A local file:

`file:///e:/UpdateSite`.

Step 6 Click **Apply**.

Step 7 Click **OK**.

4 MANAGING DEVICES

This chapter provides information on adding and managing devices using your Adaptive Log Exporter including:

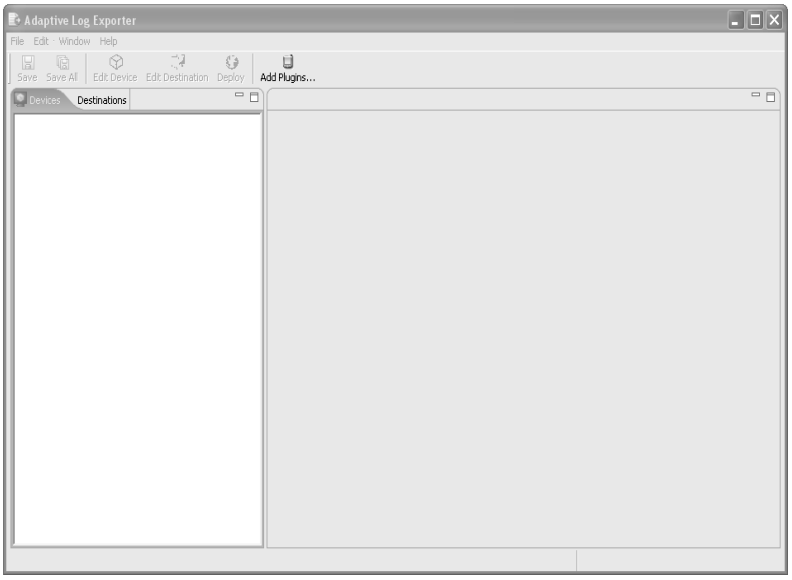
- Installing Device Types
- Updating Devices
- Configuring Devices

Installing Device Types

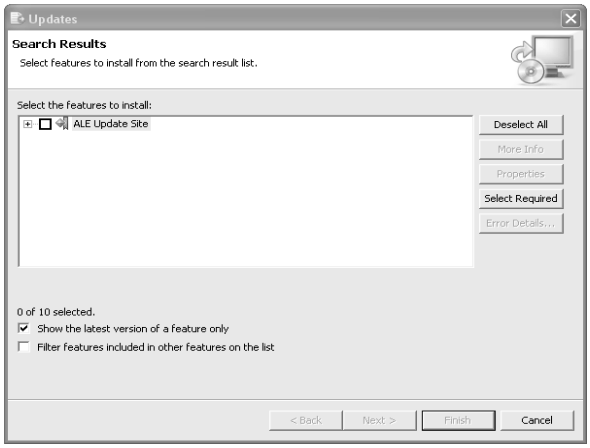
To install device types, such as a Cisco ACS, on your Adaptive Log Exporter:

Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

The Adaptive Log Exporter appears.

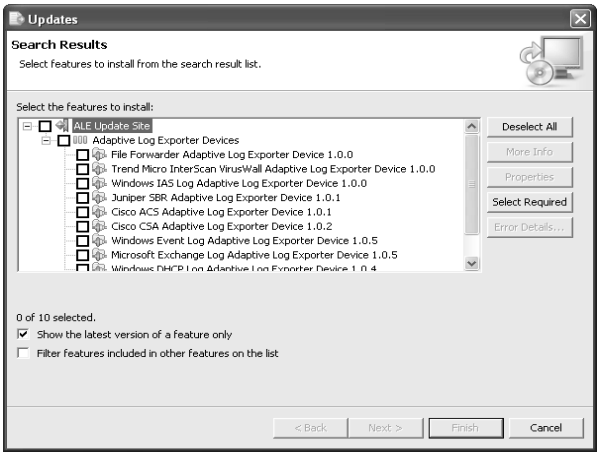


Step 2 From the menu, select **Help > Software Updates > Add Plugins**.



Step 3 Click the + sign to expand the menu tree.

The available devices appear.



Step 4 Choose one of the following options:

a If you want to install all available devices, select the check box of the top level menu option.

For example, in the above window, select the Adaptive Log Exporter Devices check box.

b If you want to install specific devices, select the check box(es) for all devices you want to add to your Adaptive Log Exporter.

Note: *The* ***Show the latest version of a feature only*** *and the* ***Filter features included in other features on the list*** *check boxes are for future development purposes only. We recommend that you use the default values for these check boxes.*

Step 5 To ensure that a selected plug-in installs any dependent plug-ins (if not already installed), click **Select Required**.

Note: *If you have selected device plug-ins that have required features but those required features have not been selected, click* ***Error Details*** *for additional information.*

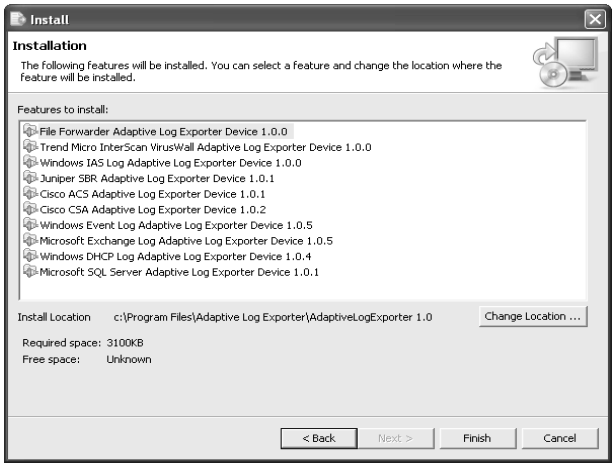
Step 6 Click **Next**.

The Feature License window appears.

Step 7 Read the license associated with the selected device. To continue, you must select the **I accept the terms of the license agreement** option.

Step 8 Click **Next**.

The Installation Window appears.



Note: *You must install your devices to the default location. Therefore, do not change the Install Location for your devices.*

Step 9 Click **Finish**.

The Feature Verification window appears.

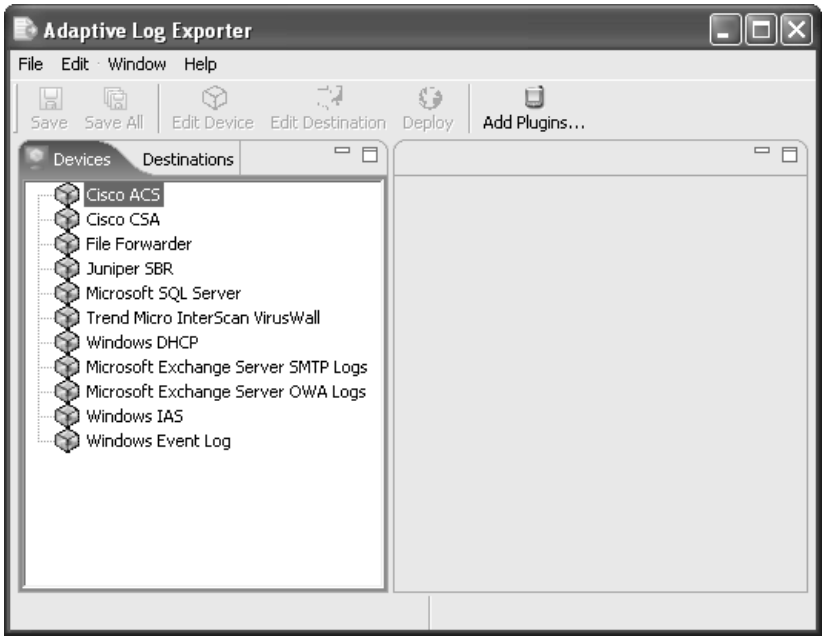
Step 10 Click **Install All** to install all chosen devices.

Updating Devices

To update your device configuration in the Adaptive Log Exporter:

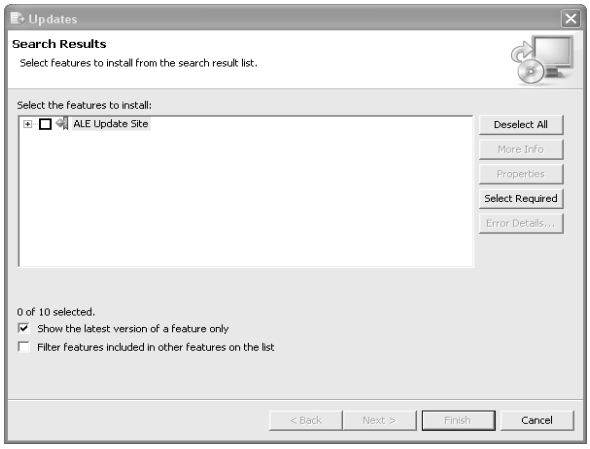
Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

The Adaptive Log Exporter appears.



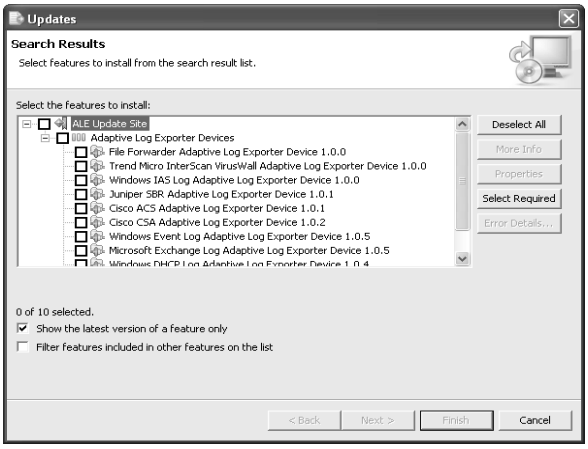
Step 2 From the menu, select **Help > Software Updates > Update Agent.**

If any updates are available, the Updates window appears. If no updates are available, a message appears.



Step 3 Click the + sign to expand the menu tree. .

The available devices appear.



Step 4 Choose one of the following options:

a If you want to install all available devices, select the check box of the top level menu option.

For example, in the above window, select the Adaptive Log Exporter Devices check box.

b If you want to install specific devices, select the check box(es) for all devices you want to add to your Adaptive Log Exporter.

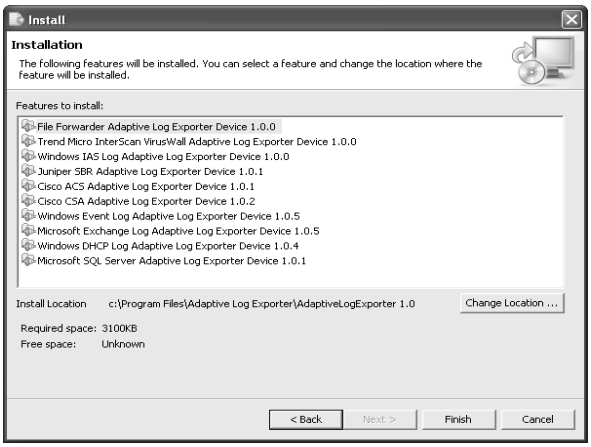
Step 5 Click **Next**.

The Feature License window appears.

Step 6 Read the license associated with the selected devices. To continue, you must select the **I accept the terms of the license agreement** option.

Step 7 Click **Next**.

The Installation Window appears.



Step 8 If you want to change the location to which the devices will be installed:

a Click **Change Location**.

b Click **Add Location**.

c Using the menu tree, select the location you want to install the devices.

d Click **OK**.

e Click **OK**.

Step 9 Click **Finish**.

The Feature Verification window appears.

Step 10 Click **Install All** to install all chosen devices.

Configuring Devices

Once you have installed the device types, such as Cisco ACS, to your Devices tab, you can add multiple devices to integrate with STRM. Each device you add to the device type must be configured and then mapped to a destination. For more information on configuring the destination, see Chapter 5 Managing Destinations.

Using the Adaptive Log Exporter, you can,

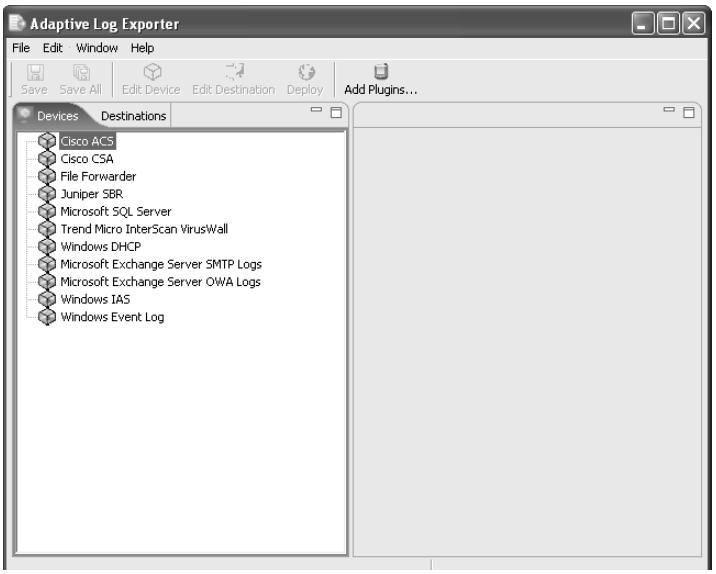
- Adding a Device
- Editing a Device
- Deleting a Device

Adding a Device

To add a device:

Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

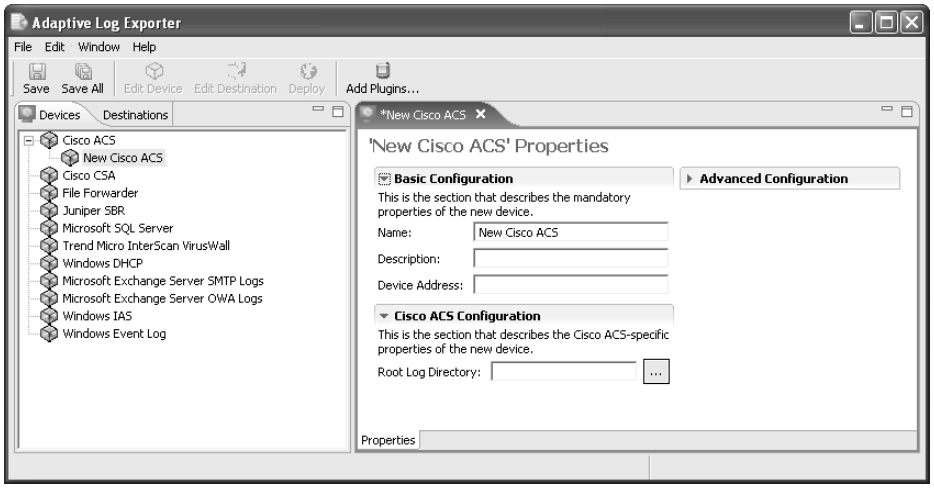
The Adaptive Log Exporter appears.



Step 2 Click the **Devices** tab.

Step 3 For the device type to which you want to add a device, use the right-mouse button (right-click) on the device name and select **Add Device**.

A new device appears below the main device name and configuration options appear. For example, if you add a new device to the Cisco ACS device, the following window appears:



Step 4 In the Basic Configuration area, enter values for the parameters:

- **Name** — Specify the name you want to assign this device. The name can be up to 50 characters in length, composed only of alphanumeric characters and the underscore (_).
- **Description** — Specify a description for this device. The description can be up to 100 characters in length.
- **Device Address** — Specify the IP address or hostname for this device. This is the IP address this DSM uses to communicate with STRM.

Step 5 Click the arrow next to Advanced Configuration to reveal the configuration parameters.

Step 6 For the Throttle Timeout parameter, specify the delay between polling events, in milliseconds, for a specific device. The higher the value, the less you want the Adaptive Log Exporter to check for device changes. The default is 500 and this value must be greater than 10 milliseconds.

Step 7 Configure the device specific parameters.

For more information, see the appropriate section for the device specific configuration.

Step 8 From the menu, select **File > Save**.

Step 9 Repeat for each device you want to configure.

Step 10 From the menu, select **File > Save All**.

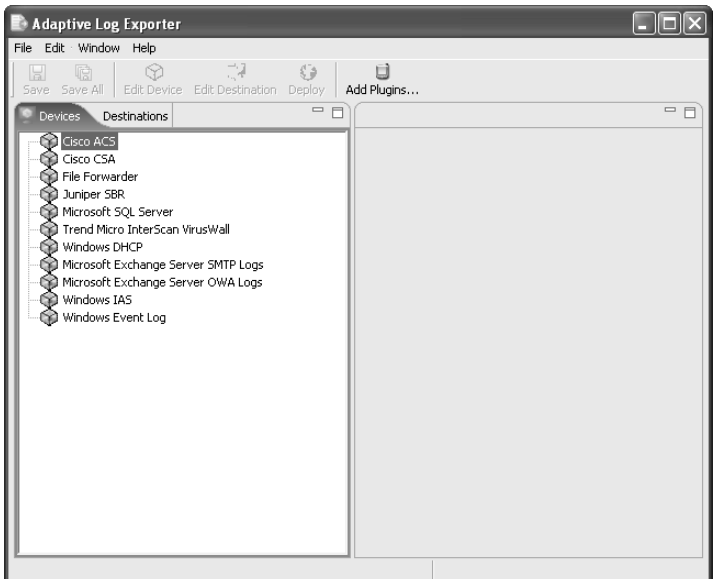
Step 11 From the menu, select **File > Deploy**.

Editing a Device

To edit a device:

Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

The Adaptive Log Exporter appears.



Step 2 Click the **Devices** tab.

Step 3 For the device type that includes the device you want to edit, click + to expand the menu tree.

Step 4 For the device you want to edit, use right-mouse button (right-click) on the device name and select **Edit Device**.

The configuration parameters for that device appears.

Step 5 Update the Basic Configuration, as necessary:

- **Name** — Specify the name you want to assign this device. The name can be up to 50 characters in length, composed only of alphanumeric characters and the underscore (_).
- **Description** — Specify a description for this device. The description can be up to 100 characters in length.
- **Device Address** — Specify the IP address or hostname for this device. This is the IP address with which you would like your device associated in STRM.

Step 6 Click the arrow next to Advanced Configuration to reveal the configuration parameters.

Step 7 For the Throttle Timeout parameter, specify the delay between polling events, in milliseconds, for a specific device. The higher the value, the less you want the Adaptive Log Exporter to check for device changes. The default is 500 and this value must be greater than 10 milliseconds.

Step 8 Configure the device specific parameters.

For more information, see the appropriate section for the device specific configuration.

Step 9 From the menu, select **File > Save**.

Step 10 Repeat for each device you want to edit.

Step 11 From the menu, select **File > Save All**.

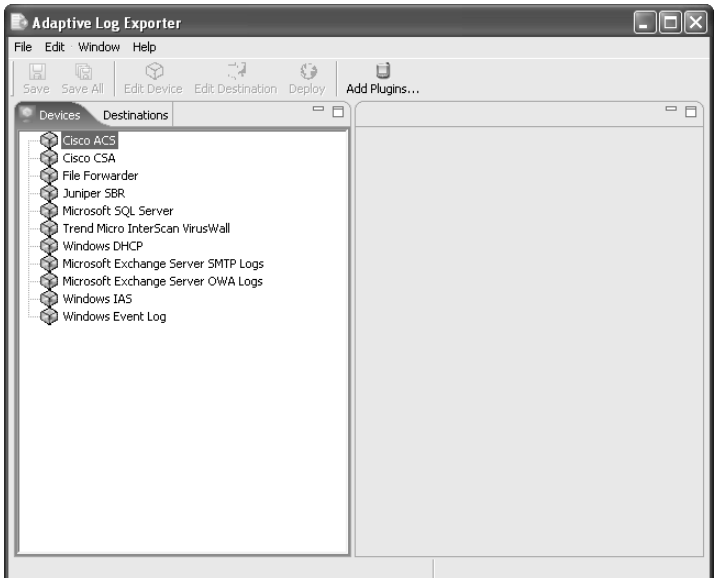
Step 12 From the menu, select **File > Deploy**.

Deleting a Device

To delete a device:

Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

The Adaptive Log Exporter appears.



Step 2 Click the **Devices** tab.

Step 3 For the device type that includes the device you want to delete, click + to expand the menu tree.

Step 4 For the device you want to delete, use right-mouse button (right-click) on the device name and select **Delete Device**.

A confirmation window appears.

Step 5 Click **Ok**.

Step 6 From the menu, select **File > Save**.

Step 7 Repeat for each device you want to delete.

Step 8 From the menu, select **File > Save All**.

Step 9 From the menu, select **File > Deploy**.

5 MANAGING DESTINATIONS

This chapter provides information on adding and managing your device destinations using your Adaptive Log Exporter including:

- Configuring Destinations
- Mapping to a Destination

Configuring Destinations

Using the Adaptive Log Exporter, you can,

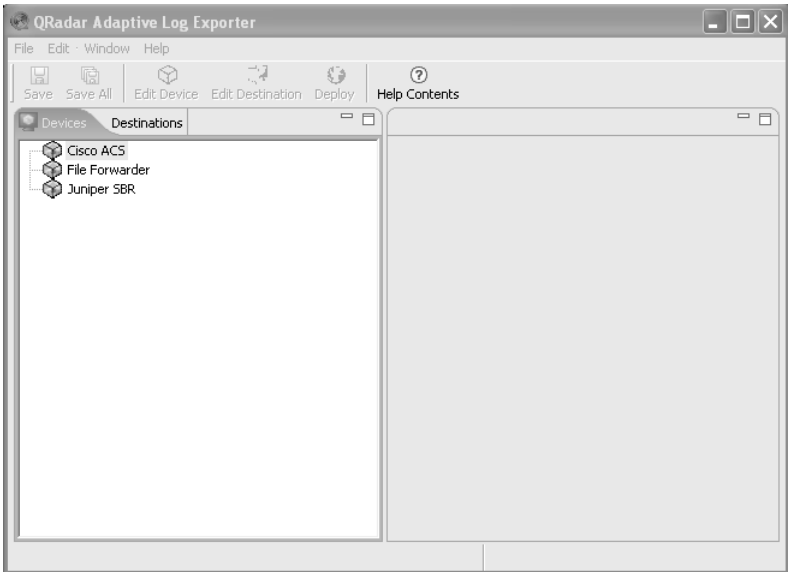
- Adding a Destination
- Editing a Destination
- Deleting a Destination

Adding a Destination

To add a destination:

Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

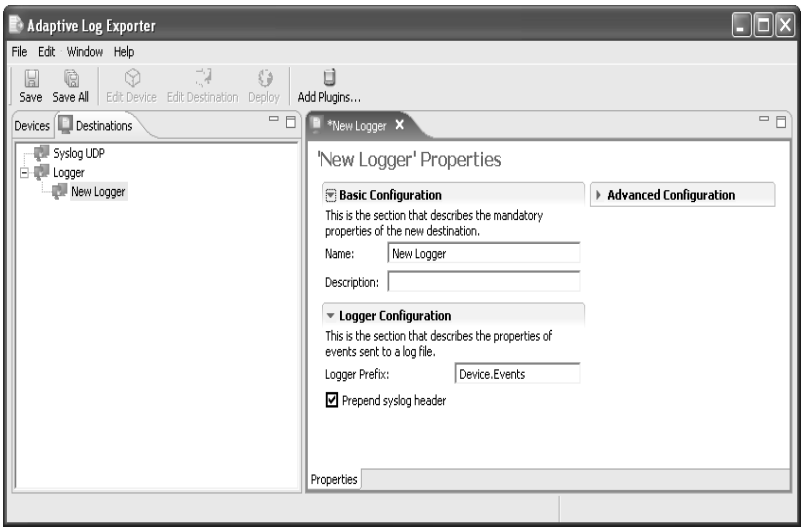
The Adaptive Log Exporter appears.



Step 2 Click the **Destination** tab.

Step 3 For the destination type to which you want to add a new device, use the right-mouse button (right-click) on the destination name and select **Add Destination**.

A new destination appears below the main destination name and configuration options appear. For example, if you add a new destination to the Syslog UDP destination, the following window appears:



Step 4 In the Basic Configuration area, enter values for the parameters:

- **Name** — Specify the name you want to assign this destination, composed only of alphanumeric characters and the underscore (_).
- **Description** — Specify a description for this device.

Step 5 Click the arrow next to Advanced Configuration to reveal the configuration parameters.

Step 6 For the Number of Threads parameter, specify the number of concurrent processing threads you want run in this destination. The default is 1.

Step 7 Choose one of the following options:

a If you are configuring a Syslog UDP or Syslog TCP destination:

- **Syslog Server Address** — Specify the IP address of your STRM system.
- **Syslog Server Port** — Specify the syslog port on your STRM system.

b If you are configuring a Logger destination:

- **Logger Prefix** — Specify the heading you want to assign to the logs. The Logger Prefix entry must start with **Device.Events** and may contain letters, numbers and periods.
- **Prepend Syslog Header** — Select the check box if you want the syslog header to be attached to the message in the logs.

Step 8 From the menu, select **File > Save**.

Step 9 Repeat for each destination you want to configure.

Step 10 From the menu, select **File > Save All**.

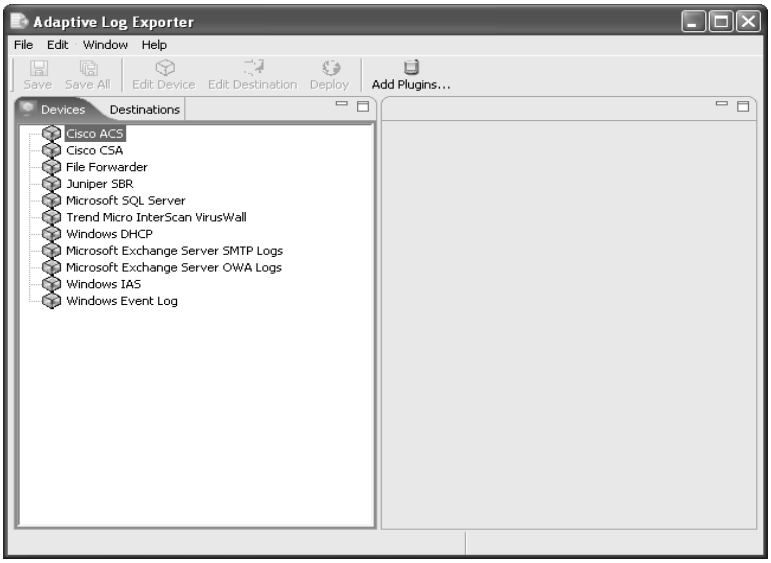
Step 11 From the menu, select **File > Deploy**.

Editing a Destination

To edit a destination:

Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

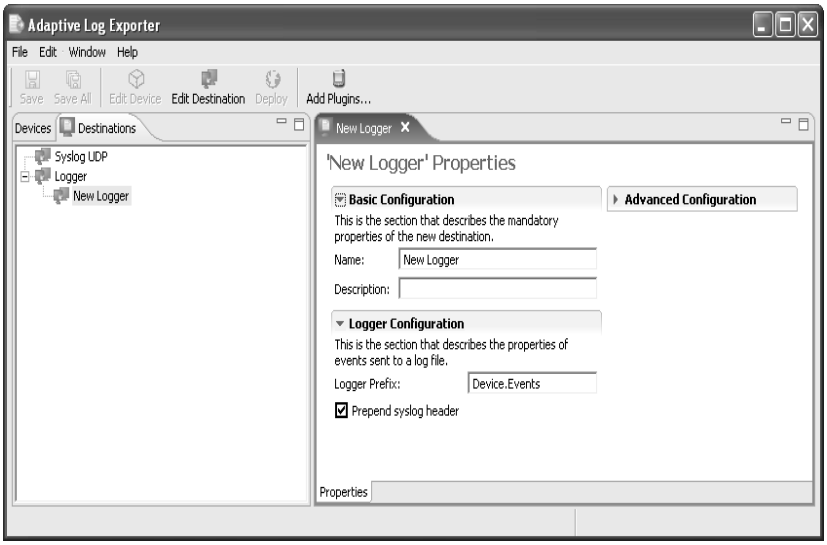
The Adaptive Log Exporter appears.



Step 2 Click the **Destination** tab.

Step 3 For the destination type that includes the destination that you want to edit, click the + sign to expand the menu tree.

Step 4 For the destination you want to edit, use the right-mouse button (right-click) on the destination name and select **Edit Destination**.



Step 5 In the Basic Configuration area, update the values, as necessary:

- **Name** — Specify the name you want to assign this destination, composed only of alphanumeric characters and the underscore (_).
- **Description** — Specify a description for this device.

Step 6 Click the arrow next to Advanced Configuration to reveal the configuration parameters.

Step 7 For the Number of Threads parameter, update the number of concurrent processing threads you want run in this destination.

Step 8 Choose one of the following options:

a If you are configuring a Syslog UDP or Syslog TCP destination:

- **Syslog Server Address** — Specify the IP address of your STRM system.
- **Syslog Server Port** — Specify the syslog port on your STRM system.

b If you are configuring a Logger destination:

- **Logger Prefix** — Specify the heading you want to assign to the logs. The Logger Prefix entry must start with **Device.Events** and may contain letters, numbers and periods.
- **Prepend Syslog Header** — Select the check box if you want the syslog header to be attached to the message in the logs.

Step 9 From the menu, select **File > Save**.

Step 10 Repeat for each destination you want to edit.

Step 11 From the menu, select **File > Save All**.

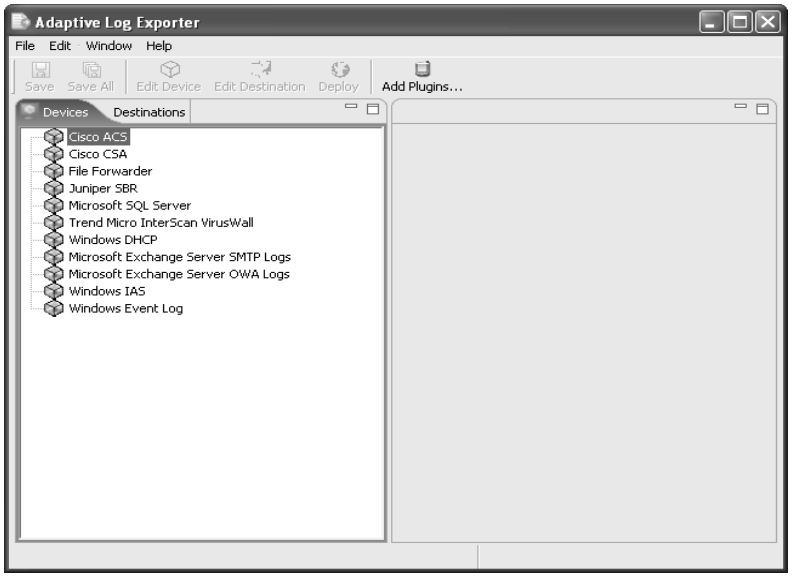
Step 12 From the menu, select **File > Deploy**.

Deleting a Destination

To delete a destination:

Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

The Adaptive Log Exporter appears.



Step 2 Click the **Destination** tab.

Step 3 For the destination type that includes the destination that you want to delete, click + to expand the menu tree.

Step 4 On the destination you want to delete, use the right-mouse button (right-click) on the destination name and select **Delete Destination**.

A confirmation window appears.

Step 5 Click **Ok**.

Step 6 From the menu, select **File > Save**.

Step 7 Repeat for each device you want to delete.

Step 8 From the menu, select **File > Save All**.

Step 9 From the menu, select **File > Deploy**.

Mapping to a Destination

Once you have configured your devices and destinations, you must map your device to a destination. This section provides information on mapping a destination to a device including:

- Creating a Mapping
- Removing a Mapping

Creating a Mapping

To map a device to a destination:

Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

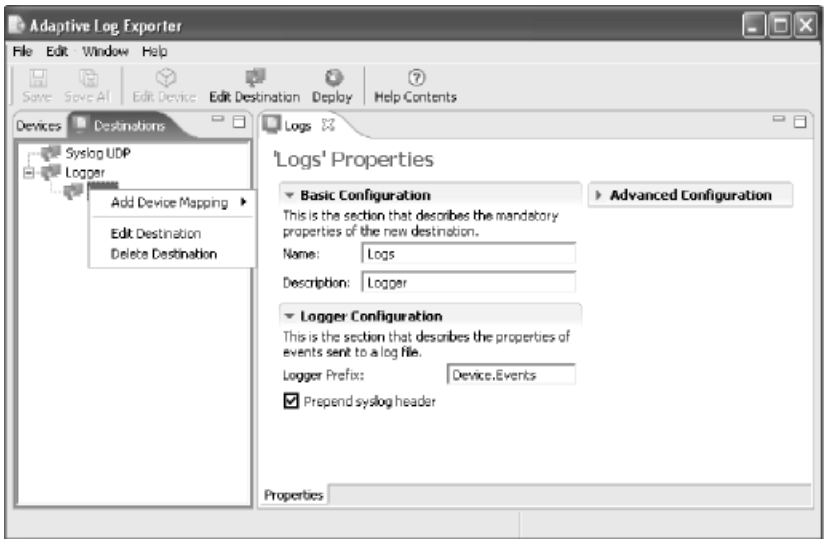
The Adaptive Log Exporter appears.

Step 2 Click the **Destination** tab.

Step 3 For the destination type that includes the destination that you map to a device, click + to expand the menu tree.

Step 4 For the destination you want to map to a device, use the right-mouse button (right-click) on the destination name and select **Add Device Mapping**.

The mapping is created. A new + sign appears next to the mapped destination.



Step 5 To view the mapping, click + to view the mapped device name.

Step 6 From the menu, select **File > Save**.

Step 7 Repeat for each destination you want to map to a device.

Step 8 From the menu, select **File > Save All**.

Step 9 From the menu, select **File > Deploy**.

Removing a Mapping

To delete a mapping between a device and a destination:

Step 1 From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

The Adaptive Log Exporter appears.

Step 2 Click the **Destination** tab.

Step 3 For the destination type that includes the mapping you want to remove, click + to expand the menu tree.

Step 4 For the destination that includes the mapping you want to remove, click + to expand the menu tree.

Step 5 For the mapping you want to remove, use the right-mouse button (right-click) on the device name and select **Delete Device Mapping**.

The mapping is removed.

Step 6 From the menu, select **File > Save**.

Step 7 Repeat for each mapping you want to remove.

Step 8 From the menu, select **File > Save All**.

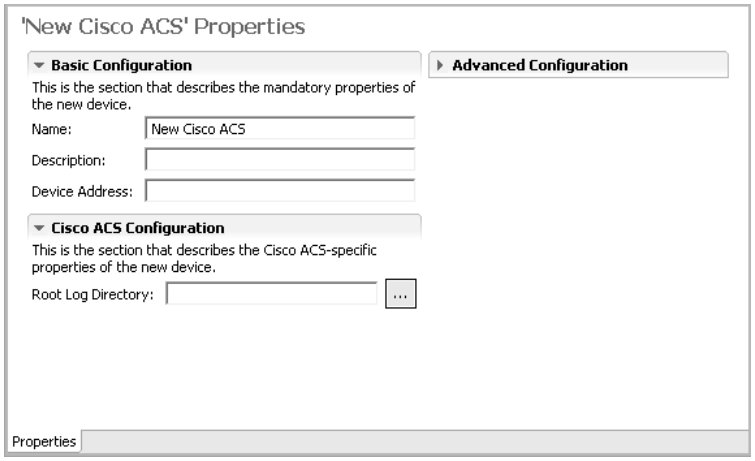
Step 9 From the menu, select **File > Deploy**.

6 CONFIGURING THE CISCO ACS DEVICE

This chapter provides information on configuring your Cisco ACS device.

Note: *Do not use the Cisco ACS device to monitor files that can only be accessed over the network (for example, a file share). Monitoring remote files is not supported.*

For information on adding or managing a device, see Chapter 4 Managing Devices.



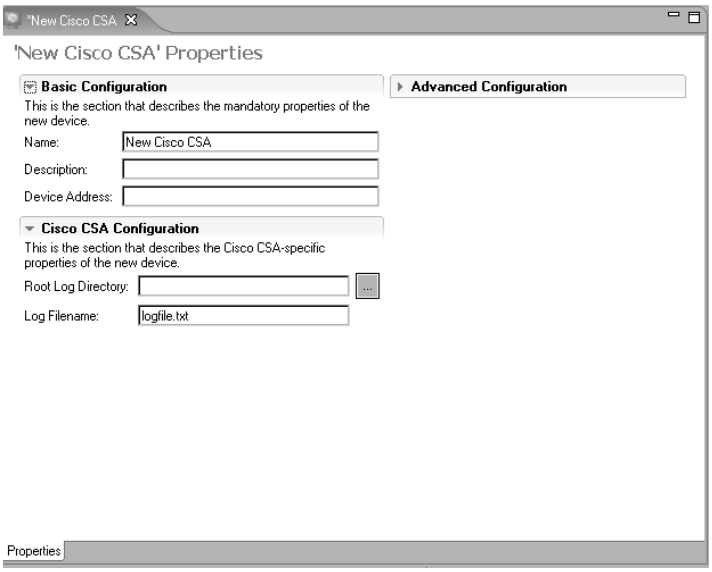
Configure the **Cisco ACS device** parameter to specify the **Root Log Directory**, which is the location Cisco ACS stores the logs files.

7 CONFIGURING THE CISCO CSA DEVICE

Cisco Security Agents (CSA) provides security to your deployment to defend against the spread of attacks across networks and systems. These CSA devices enforce a set of policies provided by the Management Center (MC) for CSA devices and selectively applied to system nodes by the network administrator.

Note: *Do not use the Cisco CSA device to monitor files that can only be accessed over the network (for example, a file share). Monitoring remote files is not supported.*

This chapter provides information on configuring your CSA device using the Adaptive Log Exporter. For information on adding or managing a device, see Chapter 4 Managing Devices.



Enter values for the following parameters:

- **Root Log Directory** — Specify the location of the CSA MC alert log files. By default, the CSA alert log files are located in the **`C:\alerts\`** directory
- **Log Filename** — Specify the name of the active alert log file. The CSA MC can generate a flat logging file to which events are written with a name of your choosing.

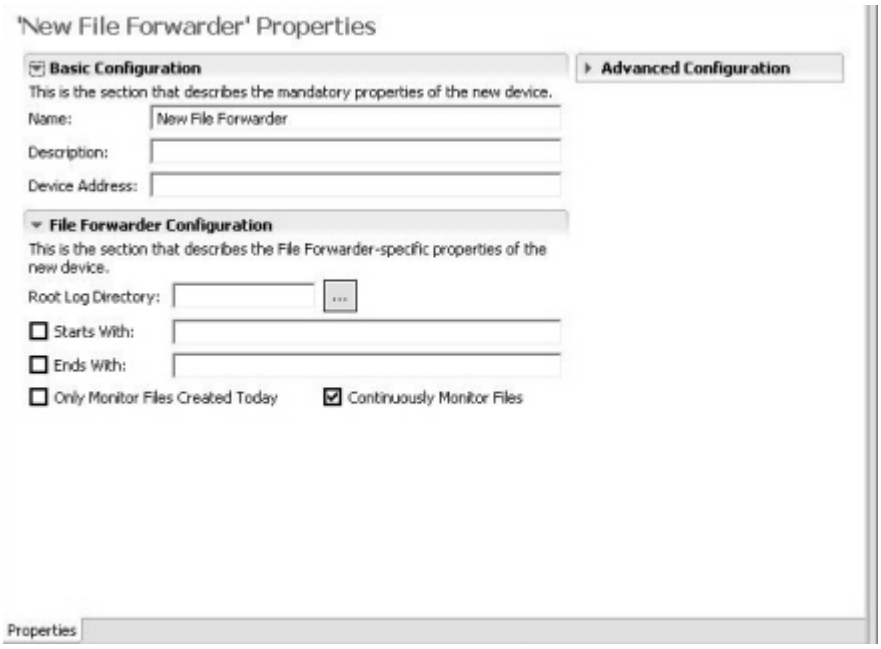


Note: *This file data is encoded in UTF-8 format. Entry fields are separated by a comma. Event entries are separated by a carriage return/line feed (ASCII Hex 0D 0A). Once a log file exceeds 1 MB, the file is closed and the file name is suffixed with a time stamp. A new file, using the same file name entered in the CSA MC Alerts Log file field, is then created. Events continue to be written to this new file until it reaches 1 MB.*

8 CONFIGURING THE FILE FORWARDER DEVICE

This chapter provides information on configuring your File Forwarder device.

For information on adding or managing a device, see Chapter 4 Managing Devices.



Enter values for the following parameters:

- **Root Log Directory** - Specify the location from which the File Forwarder device reads the logs files.
- **Starts With** - If you want the device to monitor files that start with a specific character combination, select the check box and enter the desired characters. The entered string can be up to 255 characters in length.
- **Ends With** - If you want the device to monitor files that ends with a specific character combination, select the check box and enter the desired characters. The entered string can be up to 255 characters in length.

  For example, to monitor all files ending in .log, specify **.log** as the value for the Ends With parameter.

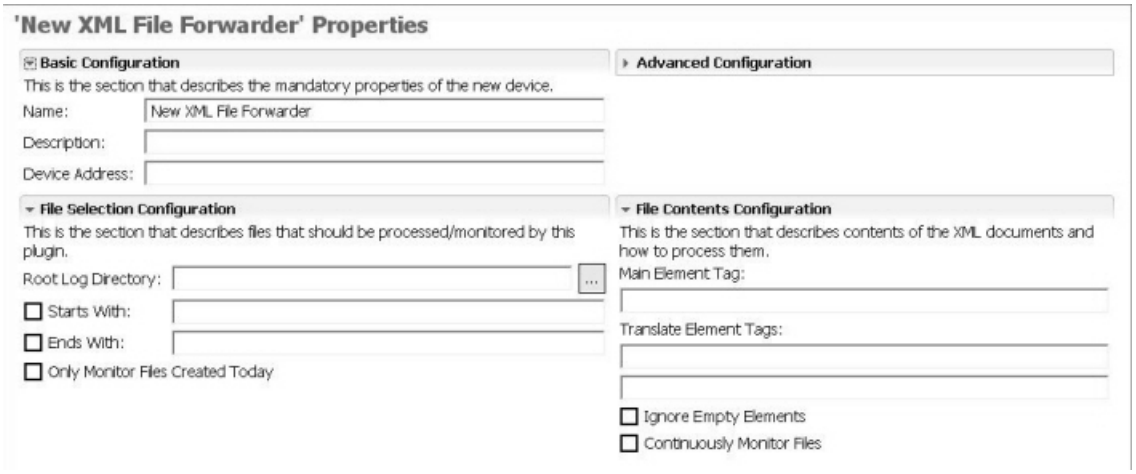
- **Only Monitor Files Created Today** - When a change to the root log directory occurs (for example, new files are created or deleted), all file monitors are reset. Select the check box if you only want to monitor files with a creation date matching the current date.
- **Continuously Monitor Files** - If the check box is selected, changes to the files are continually processed, as they are saved to disk. If the check box is clear, all new files are processed in their entirety upon creation and then will be closed and ignored.

9 CONFIGURING THE XML FILE FORWARDER DEVICE

This chapter provides information on configuring your XML File Forwarder device.

Note: *Do not use the XML File Forwarder device to monitor files that can only be accessed over the network (for example, a file share). Monitoring remote files is not supported.*

For information on adding or managing a device, see Chapter 4 Managing Devices.



Enter values the following parameters:

- **Root Log Directory** - Specify the location the XML File Forwarder device stores the logs files.
- **Starts With** - If you want the device to monitor files that start with a specific character combination, select the check box and enter the desired characters. The entered string can be up to 255 characters in length.
- **Ends With** - If you want the device to monitor files that ends with a specific character combination, select the check box and enter the desired characters. The entered string can be up to 255 characters in length.

  For example, to monitor all files ending in .log, specify **.log** as the value for the Ends With parameter.

- **Only Monitor Files Created Today** - When a change to the root log directory occurs (for example, new files are created or deleted), all file monitors are reset. Select the check box if you only want to monitor files with a creation date matching the current date.
- **Main Element Tab** - The XML element that is considered an event. This element and all of the associated child elements are processed.
- **Translate Element Tags** - Specify using the following format:

  `<dot-separated XML element path> = <replacement text>`

  All elements containing this path are replaced with the corresponding text. This can be used to shorten the payload length. For example:

  `LogEntry.MessageHeader = Hdr`

  This results in Hdr replacing occurrences of LogEntry.MessageHeader.

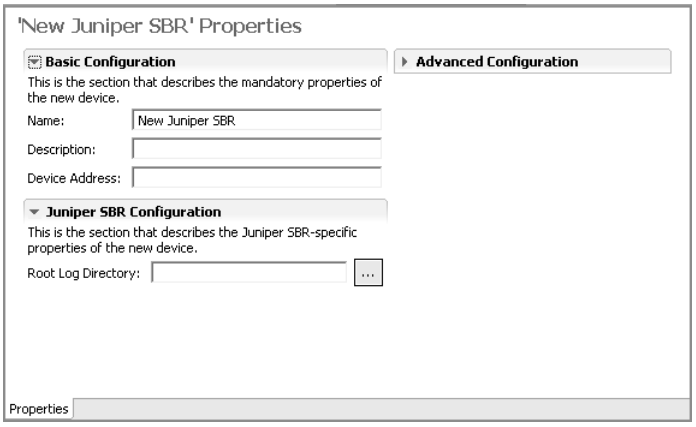
  All fields are matched using the longest algorithm first and then shorter algorithms are attempted after a match is found.
- **Ignore Empty Elements** - If the check box is selected, elements that have no associated value are not inserted into the payload. For example, elements that resemble **`x.y.z =`** with no data will not be inserted into the payload.
- **Continuously Monitor Files** - If the check box is selected, changes to the files are continually processed, as they are saved to disk. If the check box is clear, all new files are processed in their entirety upon creation and then will be closed and ignored.

10 CONFIGURING THE JUNIPER SBR DEVICE

This chapter provides information on configuring your Juniper SBR device.

Note: *Do not use the Juniper SBR device to monitor files that can only be accessed over the network (for example, a file share). Monitoring remote files is not supported.*

For information on adding or managing a device, see Chapter 4 Managing Devices.



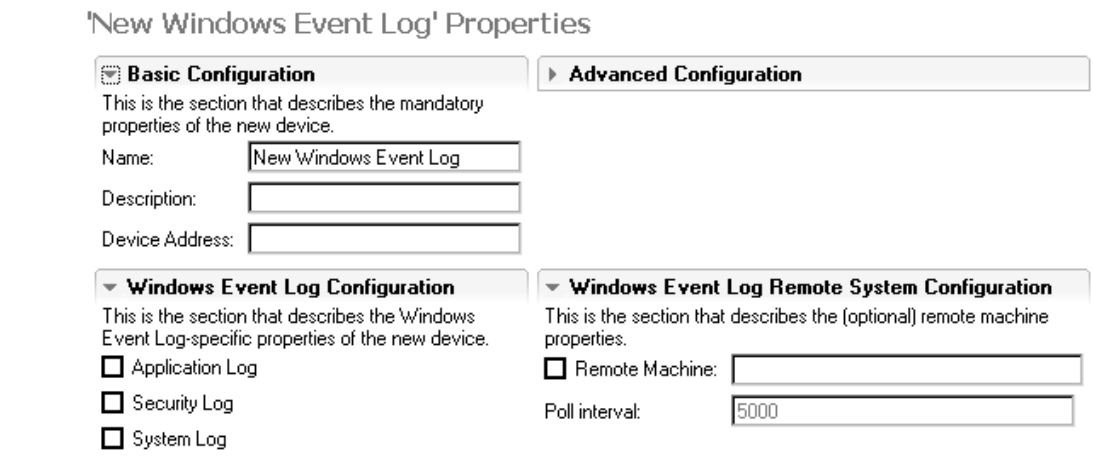
Configure the **Juniper SBR** parameter to specify the **Root Log Directory**, which is the location Juniper SBR stores the logs files.

11 CONFIGURING THE WINDOWS EVENT LOG DEVICE

In Microsoft Windows, an event is any significant occurrence in the system, a program that requires users to be notified, or an entry added to a log. The event log device records application, security, and system events in the STRM Events interface. Using the Events interface, you view hardware, software, and system component information. You can also monitor security events on a local or remote computer. Event logs enable you to identify and diagnose the source of current system problems or help you predict potential system problems.

This chapter provides information on configuring your Windows Event Log device using the Adaptive Log Exporter. For information on adding or managing a device, see Chapter 4 Managing Devices.

Note: *We recommend that you configure a maximum of 20 Windows Event Log Devices.*



Enter values for the following parameters:

- **Application Log** — Select the check box if you want the device to monitor the application log. The application log contains events logged by programs, for example, a database program may record a file error in the application log. The specific events recorded by the application log are determined by the software program.

- **Security Log** — Select the check box if you want the device to monitor the security log. The security log records events (for example, valid and invalid logon attempts) and events related to resource use (for example, creating, opening, or deleting files). You must be logged in with administrator privileges or as a member of the administrators group to enable, use, and specify which events you want to record in the security log.
- **System Log** — Select the check box if you want the device to monitor the system log. The system log contains events logged by Windows XP system components. For example, if a driver fails to load during startup, an event is recorded in the system log. Windows XP predetermines the events that are logged by system components.
- **Remote Machine**— Select the check box if you want the device to retrieve the logs from a remote machine. Enter the desired Universal Naming Convention (UNC) name. The entered string can be up to 255 characters in length. For example, \\tango123 or \\172.16.20.98.



Note: *When accessing remote logs, make sure that you configure the Adaptive Log Exporter service to run as a user with Administrative privileges on the remote system. For more information, see the Configure how a service is started technical note on www.microsoft.com.*

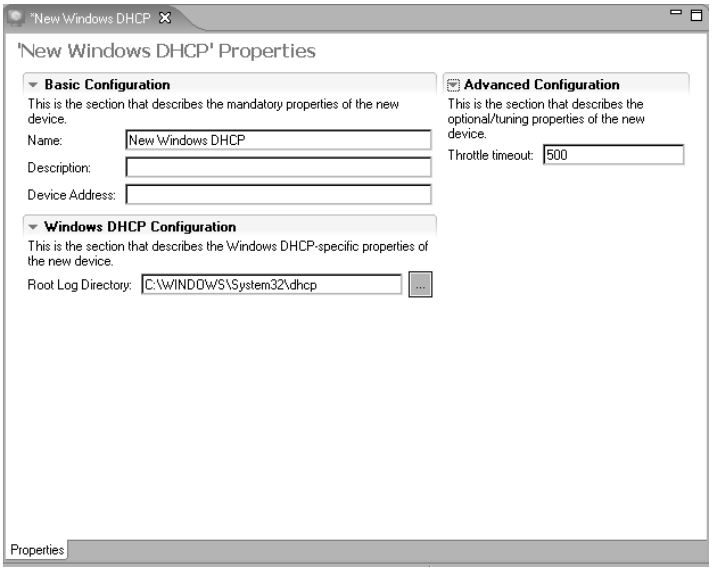
- **Poll Interval** — Specify the remote poll interval enter a value, in milliseconds. The default is 5000 milliseconds.

12 CONFIGURING THE MICROSOFT DHCP DEVICE

In the Microsoft Windows Server family, DHCP server log files use audit logging to permit log files to remain enabled without additional monitoring or administration. This allows you to manage log file growth or conserve disk resources.

Note: *Do not use the Microsoft DHCP device to monitor files that can only be accessed over the network (for example, a file share). Monitoring remote files is not supported.*

This chapter provides information on configuring your Microsoft DHCP device using the Adaptive Log Exporter. For information on adding or managing a device, see Chapter 4 Managing Devices.



Configure the **Root Log Directory** parameter, which is the location of the DHCP server log files. By default, the DHCP audit log files are located at %WINDIR%\system32\dhcp\DhcpSrvLog-xxx.log.

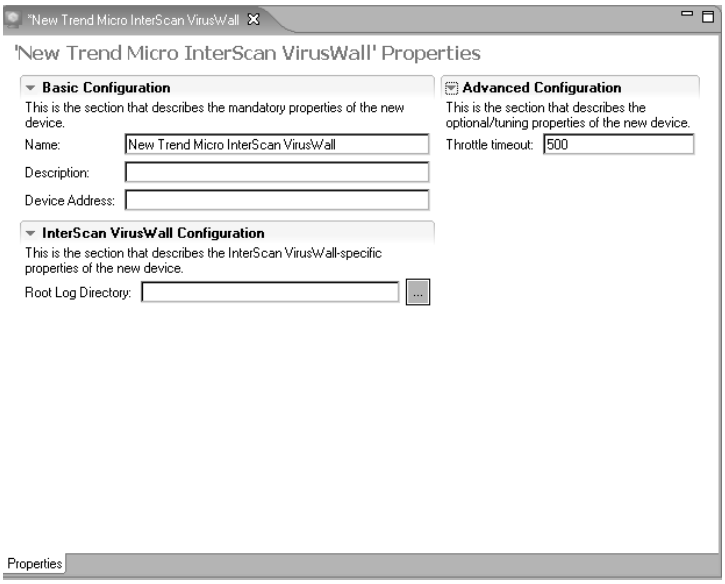
Once you configure your Microsoft DHCP device, make sure you restart the DHCP service to allow the Adaptive Log Exporter to communicate with your DHCP device.

13 CONFIGURING THE TREND MICRO INTERSCAN VIRUSWALL DEVICE

InterScan VirusWall (ISVW) 6 for Windows provides an all-in-one gateway, antivirus, anti-spam, and content management solution for your network. VirusWall's real-time scanning services for SMTP VirusWall, POP3, VirusWall, FTP VirusWall, and HTTP VirusWall monitors for security threats in e-mail, the Internet, and in file transfers to and from the local area network (LAN).

Note: *Do not use the Trend Micro InterScan VirsusWall device to monitor files that can only be accessed over the network (for example, a file share). Monitoring remote files is not supported.*

This chapter provides information on configuring your Trend Micro InterScan VirusWall device. For information on adding or managing a device, see Chapter 4 Managing Devices.



Configure the **Root Log Directory** parameter, which is the location of the InterScan VirusWall log files. By default, the VirusWall log files are located in the **`<installation folder>\Log`** directory. The **`<installation folder>`** is the folder in which you installed your InterScan VirusWall device.

14 Configuring the Microsoft Exchange Server Device

The Microsoft Exchange Server provides you with electronic mail, calendaring, contacts and tasks, and support for the mobile and web-based access to information, as well as supporting data storage. The Microsoft Exchange Server device allows you to forward Outlook Web Access (OWA) or SMTP logs to the Adaptive Log Exporter.

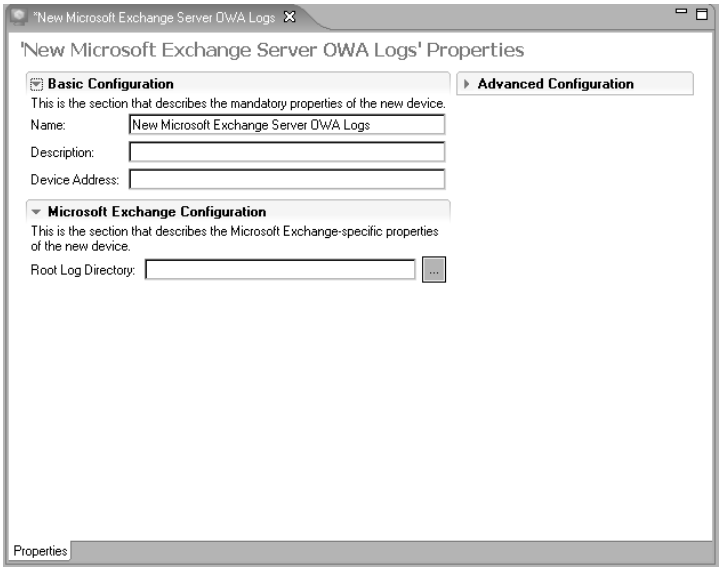
Note: *Do not use the Microsoft Exchange Server device to monitor files that can only be accessed over the network (for example, a file share). Monitoring remote files is not supported.*

This chapter provides information on forwarding OWA or SMTP logs from your Microsoft Exchange Server using the Adaptive Log Exporter including:

- Forwarding OWA Logs
- Forwarding SMTP Logs

Forwarding OWA Logs

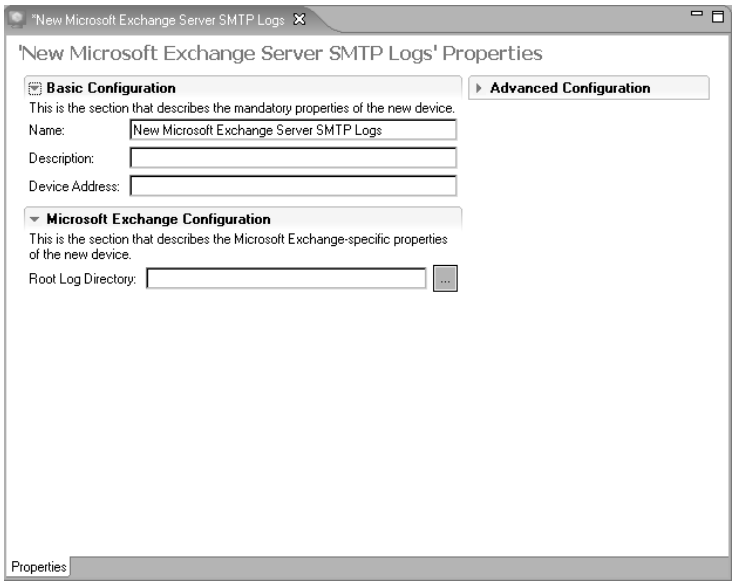
To forward OWA logs to the Adaptive Log Exporter, select the Microsoft Exchange Server OWA device. For information on adding or managing a device, see Chapter 4 Managing Devices.



Configure the **Root Log Directory** parameter, which is the location of the Microsoft Exchange Server OWA log files. By default, the Exchange log files are located in the **`%windir%\System32\LogFiles\W3SVC1\`** directory.

Forwarding SMTP Logs

To forward SMTP logs to the Adaptive Log Exporter, select the Microsoft Exchange Server SMTP device. For information on adding or managing a device, see Chapter 4 Managing Devices.



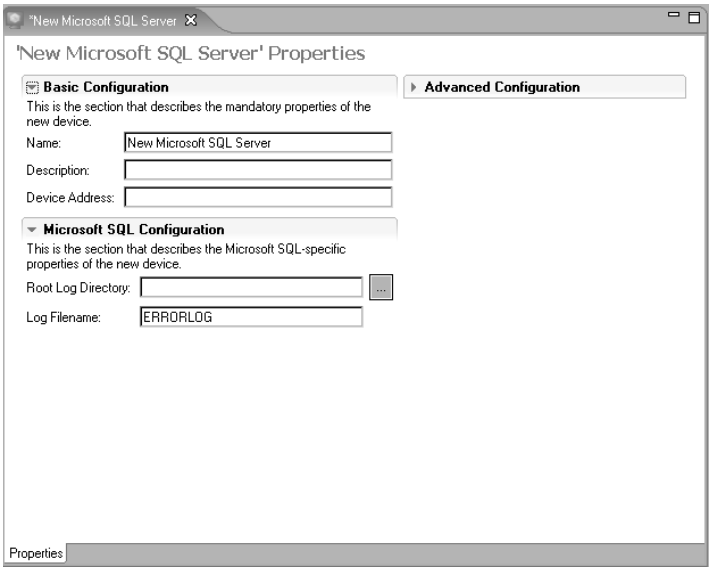
Configure the **Root Log Directory** parameter, which is the location of the Microsoft Exchange Server SMTP log files. By default, the Exchange log files are located in the **`%windir%\System32\LogFiles\SMTPSVC1\`** directory.

15 CONFIGURING THE MICROSOFT SQL SERVER DEVICE

Microsoft SQL Server is a comprehensive, integrated, end-to-end data solution that provides a platform for enterprise data and BI applications.

Note: *Do not use the Microsoft SQL Server device to monitor files that can only be accessed over the network (for example, a file share). Monitoring remote files is not supported.*

This chapter provides information on configuring your Microsoft SQL Server device using the Adaptive Log Exporter. For information on adding or managing a device, see Chapter 4 Managing Devices.



Enter values for the following parameters:

- **Root Log Directory** — Specify the location of the Microsoft SQL Server log files. By default, the SQL log files are located in the **`C:\Program Files\Microsoft SQL Server\MSSQL\LOG\`** directory.
- **Log Filename** — Specify the name of the active log file. By default, the name is ERRORLOG. If this field is empty, the filename defaults to ERRORLOG.

The error log is a standard text file that contains SQL Server information and error messages. The error log can provide meaningful information to assist you in troubleshooting issues or alerting you to potential or existing problems. The error log output includes the time and date the message was logged, the source of the message, and the description of the message. If an error occurs, the log contains the error message number and description. Typically, SQL Server retains backups of the previous six logs and provides each backup with an accrued number appended to the end of the name. For example, the most recent log backup is saved with the extension .1 and the second most recent with the extension .2.

16 CONFIGURING THE MICROSOFT IIS DEVICE

Microsoft Internet Information Services (IIS) includes a broad range of administrative features for managing web sites. You can monitor attempts to access your sites, virtual folders, or files and determine whether attempts were made to read or write to your files. IIS log file formats allow you to record events independently for any site, virtual folder, or file. For more information regarding your Microsoft IIS device, see your vendor documentation.



Note: *Do not use the Microsoft IIS device to monitor files that can only be accessed over the network (for example, a file share). Monitoring remote files is not supported.*

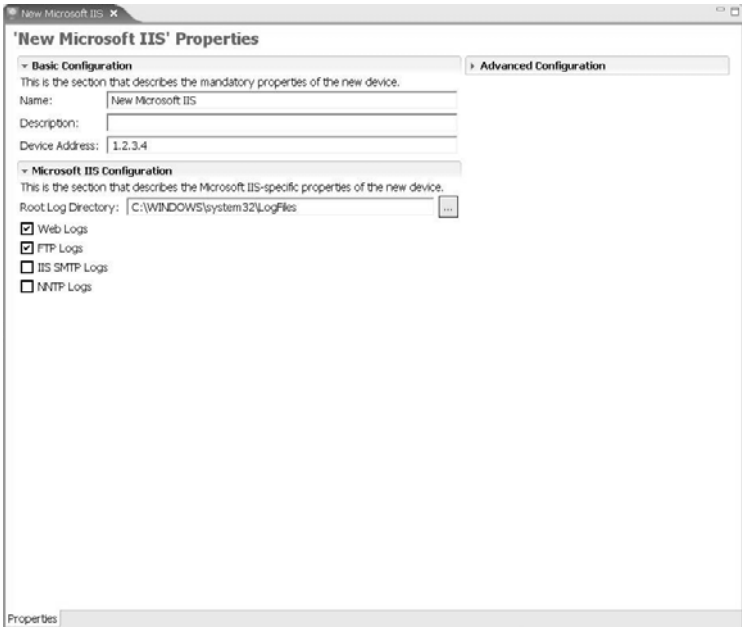


Note: *You can configure Microsoft IIS to host multiple web sites. The maximum number of Microsoft IIS web sites that a single Adaptive Log Exporter instance can monitor is 25.*

This chapter provides information on configuring your Microsoft IIS server using the Adaptive Log Exporter. For information on adding or managing a device, see Chapter 4 Managing Devices.



Note: *You must enable UTF-8 logging in the Microsoft IIS service for this device to function properly. For more information on enabling logging, see your Microsoft IIS documentation.*



Enter values for the following parameters:

- **Root Log Directory** - Specifies the location of the Microsoft IIS log files. By default, the IIS log files are located in the **`%windir%\System32\LogFiles\`** directory.
- Specify the types of logs you want to monitor:
  - **Web Logs** - Logs for the IIS Web service.
  - **FTP Logs** - Logs for the File Transfer Protocol (FTP) service.
  - **IIS SMTP Logs** - Logs for the IIS mail service.
  - **NNTP Logs** - Logs for the Network News Transfer Protocol (NNTP) service.

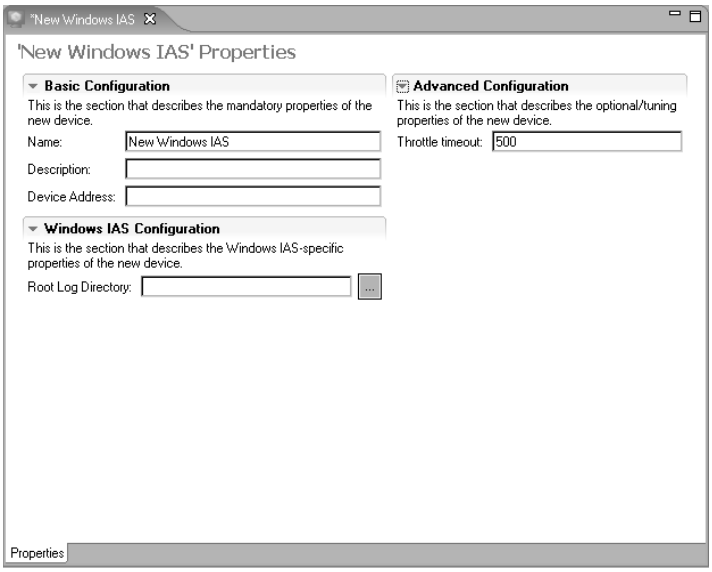
Note: *You can choose a format and enable logging for individual web sites and FTP sites. After you enable logging on a Web or FTP site, all traffic to the site (including virtual directories) is written to the corresponding file for each site.*

17 CONFIGURING THE MICROSOFT WINDOWS IAS DEVICE

The Microsoft Windows Internet Authentication Service (IAS) devices provides a Remote Authentication Dial-in User Service (RADIUS) server and proxy. As a RADIUS server, IAS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. As a RADIUS proxy, IAS forwards authentication and accounting messages to other RADIUS servers. The Microsoft Windows IAS device supports the database format.

Note: *Do not use the Microsoft Windows IAS device to monitor files that can only be accessed over the network (for example, a file share). Monitoring remote files is not supported.*

This chapter provides information on configuring your Windows IAS device using the Adaptive Log Exporter. For information on adding or managing a device, see Chapter 4 Managing Devices.



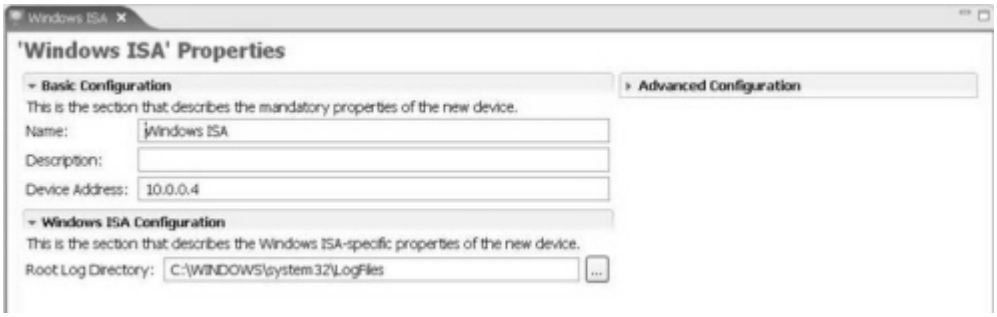
Configure the **Root Log Directory** parameter, which is the location of the IAS server log files. By default, the IAS log files are located in the **`%windir%\System32\LogFiles`** directory.

18 CONFIGURING THE MICROSOFT ISA DEVICE

The Microsoft Internet Security and Acceleration (ISA) Server provides you with network proxy and firewall services. The Microsoft ISA server device allows you to forward ISA logs to the Adaptive Log Exporter.

Note: *Do not use the Microsoft ISA Server device to monitor files that can only be accessed over the network (for example, a file share). Monitoring remote files is not supported.*

To forward ISA logs to the Adaptive Log Exporter, select the Microsoft ISA device. For information on adding or managing a device, see Chapter 4 Managing Devices.



Configure the **Root Log Directory** parameter, which is the location of the Microsoft ISA Server ISA log files. By default, the ISA log files are located in the **`%ProgramFiles%\MicrosoftISAServer\ISALogs\`** directory for ISA 2004 and in the **`%windir%\System32\LogFiles\`** for ISA 2006.

A Collecting Windows Event Logs

This appendix provides information about monitoring event logs from Windows-based servers and hosts. Typically, you can monitor your event logs with or without an agent. The Adaptive Log Exporter is an independent application that runs on a Windows host, commonly referred to as an agent. The Adaptive Log Exporter collects local and remote Windows logs supporting each method of monitoring event logs.

If you choose to use an agent, you must physically install software on the host to be monitored. The host collects and exports the log information to the desired destination. An agent distributes log collection and processing across multiple systems, which reduces the performance impact on each host. If a server or network outage occurs, logging activity is only affected on the server or area of the network affected by the outage. However, maintaining an agent-based deployment may require additional maintenance. For example, if configuration changes are required, you must replicate the configuration changes across all monitored hosts.

If you choose not to use an agent, the log information must be exported or collected from the Windows system without software being installed on the individual monitored hosts. However, you must communicate with remote Windows systems using NETBIOS, which is a relatively slow method of communication. Therefore, monitoring several Windows hosts remotely may cause a significant performance impact for the host server. Communicating remotely also requires that the appropriate domain credentials are supplied to the host server, which may be considered a security risk.

This appendix includes:

- Collecting Logs Without an Agent
- Collecting Logs With an Agent
- Configuring STRM To Accept Logs

Collecting Logs Without an Agent

To collect logs without an agent, you must install the Adaptive Log Exporter in your network. The Adaptive Log Exporter allows you to connect to remote Windows systems to return logs to STRM.

Note: *For more information on the Adaptive Log Exporter, see the Adaptive Log Exporter Users Guide.*

The Adaptive Log Exporter collects logs from individual hosts and forwards data to your STRM appliance using a UDP syslog connection. Collecting logs without an agent simplifies maintenance and does not require you to install software on individual Windows hosts.

When collecting logs without an agent, the Adaptive Log Exporter monitors the network and if a network outage occurs, any missed events are automatically collected and processed by STRM when network connectivity is restored. When the network connection is lost, records are archived on individual hosts.

Figure A-1 shows an example of a network collecting logs without using an agent.

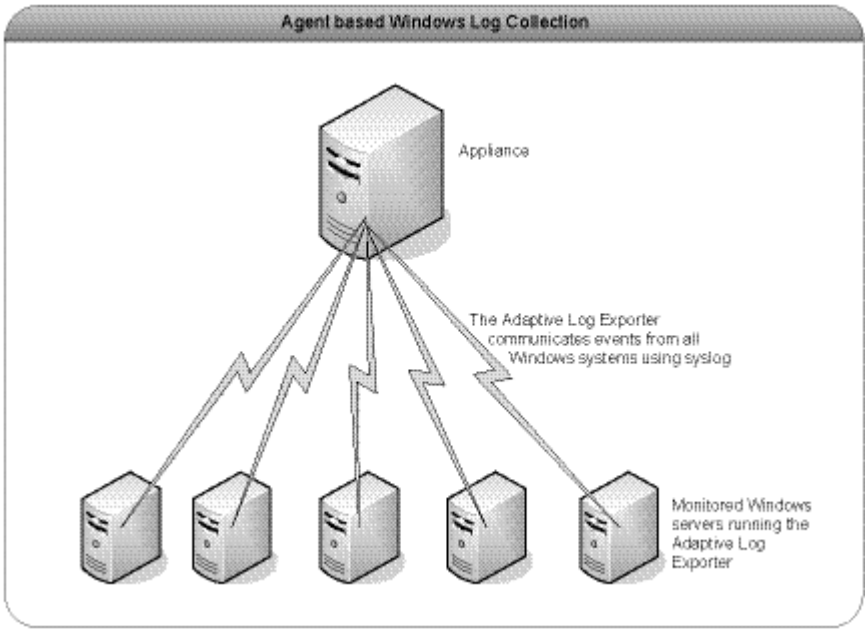


Figure A-1 Collecting Logs Without an Agent

Configuring the Adaptive Log Exporter

To configure the Adaptive Log Exporter to support a network without an agent:

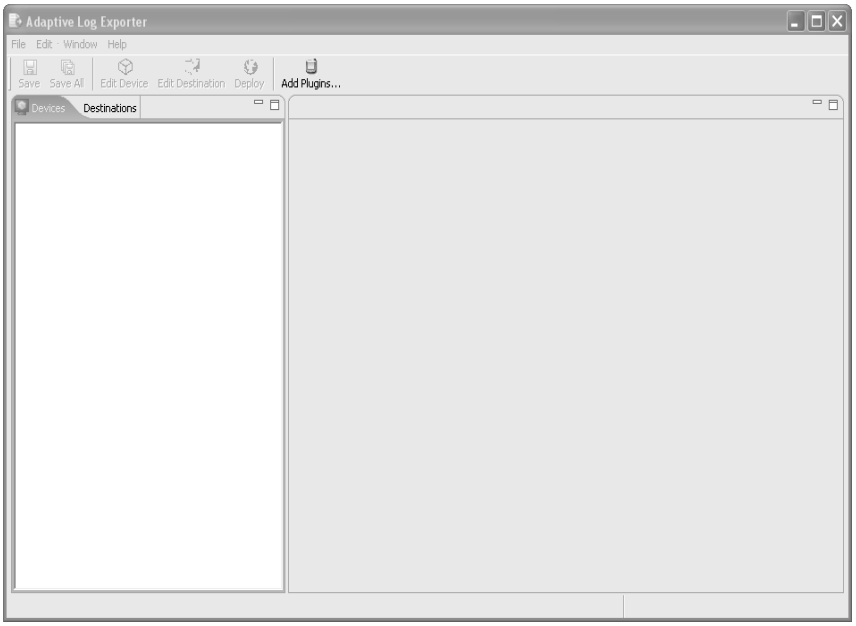
Step 1 Download and install the Adaptive Log Exporter on the system you want to host the Adaptive Log Exporter.

For detailed information on the Adaptive Log Exporter, see the *STRM Adaptive Log Exporter Users Guide*.

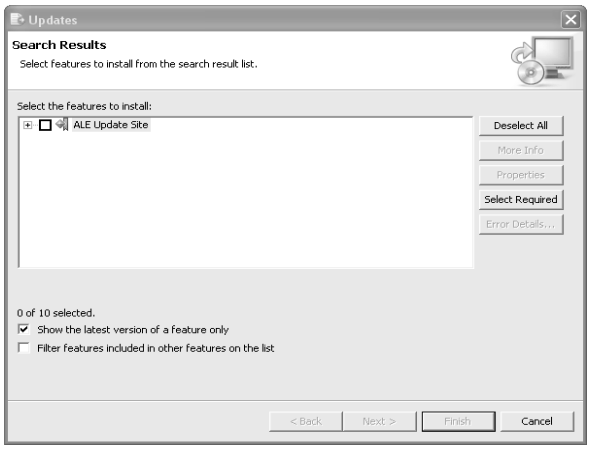
Step 2 Download and install the Windows Event Log plug-in:

a From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

The Adaptive Log Exporter appears.



b From the menu, select **Help > Software Updates > Add Extensions/Devices**.



c Click the + sign to expand the menu tree.

The available devices appear.

d Select the Windows Event Log plug-in.

e Click **Next**.

The Feature License window appears.

f Read the license associated with the selected device. To continue, you must select the **I accept the terms of the license agreement** option.

g Click **Next**.

The Installation Window appears.

Note: *You must install your devices to the default location. Therefore, do not change the Install Location for your devices.*

h Click **Finish**.

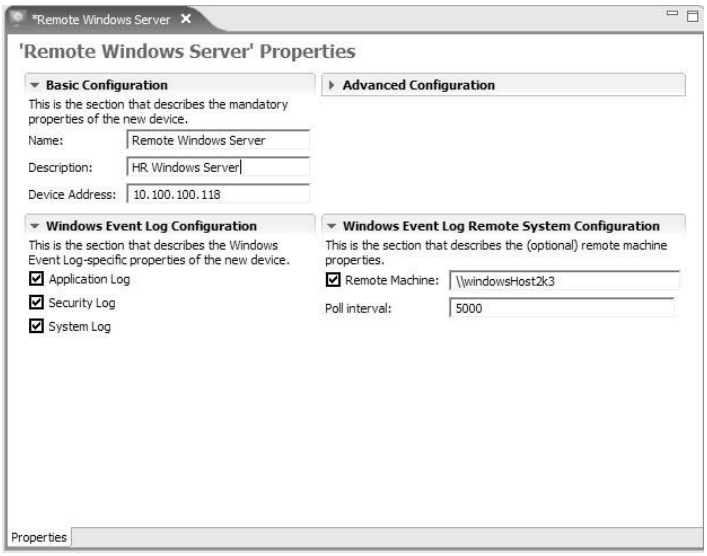
The Feature Verification window appears.

i Click **Install All** to install all chosen devices.

Step 3 In the Adaptive Log Exporter, click the **Devices** tab.

Step 4 Using your right mouse button (right-click) the Windows Event Log and select **Add Device.**

A new instance of the device is created and the Properties panel appears.



Step 5 In the Basic Configuration area, enter values for the parameters:

- **Name** — Specify the name you want to assign this device, composed only of alphanumeric characters and the underscore (_).
- **Description** — Specify a description for this device.
- **Device Address** — Specify the IP address or the hostname of the Windows system you want to monitor.

Step 6 In the Windows Event Log Configuration area, enter values for the parameters:

- **Application Log** — Select the check box if you want the device to monitor the application log.
- **Security Log** — Select the check box if you want the device to monitor the security log.
- **System Log** — Select the check box if you want the device to monitor the system log.

Step 7 In the Windows Event Log Remote System Configuration, enter values for the parameters:

- **Remote Machine**— Select the check box for the device to retrieve the logs from a remote machine. Enter the desired Universal Naming Convention (UNC) name. The entered string can be up to 255 characters in length. For example, \\tango123 or \\172.16.20.98.
- **Poll Interval** — Specify the remote poll interval enter a value, in milliseconds. The default is 5000 milliseconds.

Collecting Logs With an Agent

To collect logs with an agent, you must install the Adaptive Log Exporter on each monitored host in your network. The Adaptive Log Exporter then reports, using syslog, to your STRM system. The agent reads the individual Windows event logs and passes information to STRM using syslog.

Note: *For more information on the Adaptive Log Exporter, see the STRM Adaptive Log Exporter Users Guide.*

Figure A-2 shows an example of a network collecting logs using an agent.

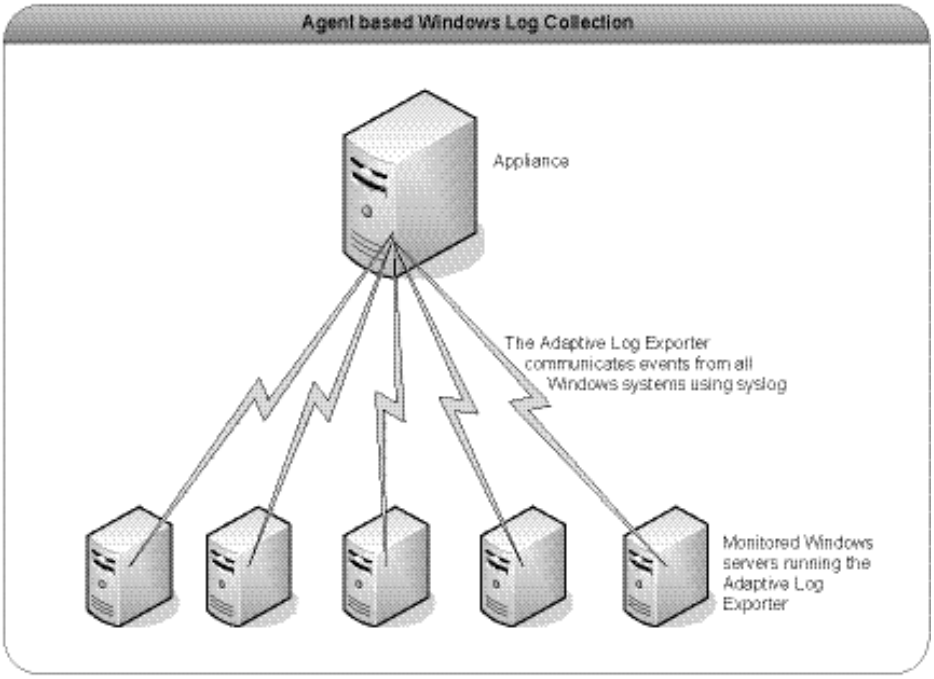


Figure A-2 Collecting Logs With an Agent

Configuring the Adaptive Log Exporter

To configure the Adaptive Log Exporter to support a network with an agent:

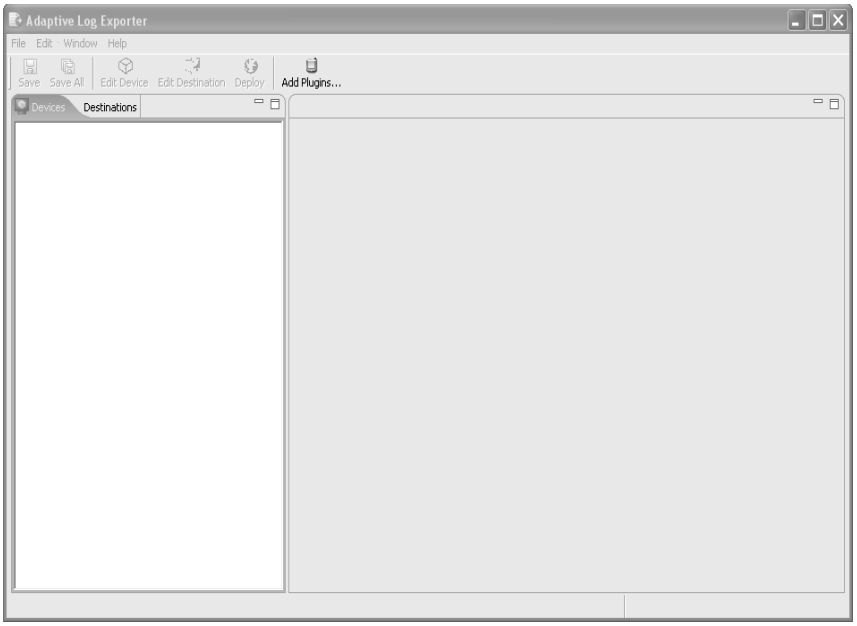
Step 1 Download and install the Adaptive Log Exporter on the system you want to host the Adaptive Log Exporter.

For more information on the Adaptive Log Exporter, see the *STRM Adaptive Log Exporter Users Guide*.

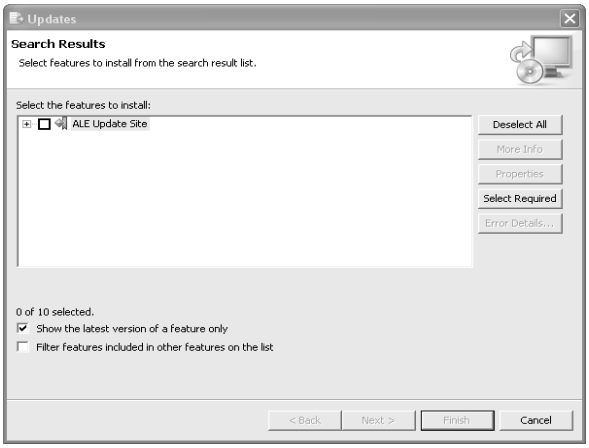
Step 2 Download and install the Windows Event Log plug-in:

a From the Start menu, select **Start > Programs > AdaptiveLogExporter > Configure Adapter Log Exporter**.

The Adaptive Log Exporter appears.



b From the menu, select **Help > Software Updates > Add Extensions/Devices**.



c Click the + sign to expand the menu tree.

The available devices appear.

d Select the Windows Event Log plug-in.

e Click **Next**.

The Feature License window appears.

f Read the license associated with the selected device. To continue, you must select the **I accept the terms of the license agreement** option.

g Click **Next**.

The Installation Window appears.

Note: *You must install your devices to the default location. Therefore, do not change the Install Location for your devices.*

h Click **Finish**.

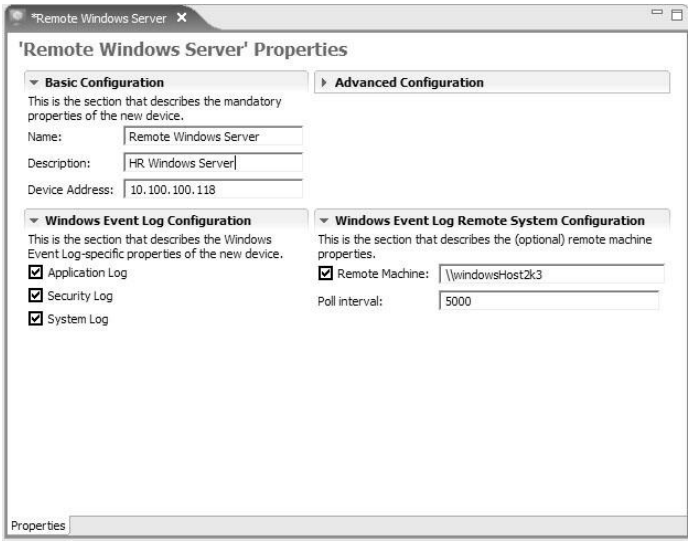
The Feature Verification window appears.

i Click **Install All** to install all chosen devices.

Step 3 In the Adaptive Log Exporter, click the **Devices** tab.

Step 4 Using your right mouse button (right-click) the Windows Event Log and select **Add Device**.

A new instance of the device is created and the Properties panel appears.



Step 5 In the Basic Configuration area, enter values for the parameters:

- **Name** — Specify the name you want to assign this device, composed only of alphanumeric characters and the underscore (_).
- **Description** — Specify a description for this device.
- **Device Address** — Specify the IP address or the hostname of the Windows system you want to monitor.

Step 6 In the Windows Event Log Configuration area, enter values for the parameters:

- **Application Log** — Select the check box if you want the device to monitor the application log.
- **Security Log** — Select the check box if you want the device to monitor the security log.
- **System Log** — Select the check box if you want the device to monitor the system log.

Step 7 In the Windows Event Log Remote System Configuration, clear the Remote Machine check box so the device does not retrieve the logs from a remote system.

Step 8 Repeat Step 4 to Step 7 for each remote host you want to monitor.

Configuring STRM To Accept Logs

Both methods of collecting logs (with or without an agent) results in information being transmitted to STRM using syslog. By default, STRM collects information forwarded using syslog through the device discovery function. STRM automatically recognizes and normalizes Windows event logs.

Once the system begins normalizing event data, STRM can analyze, report, and store the information. To verify that your Windows logs are being processed by STRM, use the Filter/Search function in the Events interface to filter on Windows Authorization devices. For more information on filtering using the Events interface, see the *STRM Users Guide*. The below window shows an example of data that results from a search.



B ADAPTIVE LOG EXPORTER QUICK START

This appendix provides a quick start for installing and setting up the Adaptive Log Exporter.



Note: *Before you install the Adaptive Log Exporter, see* Before You Begin*.*

To install and set up the Adaptive Log Exporter:

Step 1 Download the Adaptive Log Exporter from the following web site:

https://qmmunity.q1labs.com/.

Step 2 Select **Products > STRM 2008.1 > DSMs > Juniper Networks Adaptive Log Exporter**.

Step 3 Install the Adaptive Log Exporter.

For information about the full installation procedure, see Chapter 2 Installing the Adaptive Log Exporter.

Step 4 From the Start menu, select **Software > Configure Adapter Log Exporter**.

The Adaptive Log Exporter appears.

Step 5 Configure the location that the Adaptive Log Exporter uses for updates:

a From the menu, select **File > Preferences**.

The Preferences window appears.

b Click **Install/Update**.

The Install/Update parameters appear.

c Click **Update Site**.

d Enter the following as the Update Site URL:

http://downloads.q1labs.com/windowsagent

e Click **Apply**.

f Click **OK** to return to the main configuration screen.

Step 6 To install device types:

a Click the **Add Plugins** icon.

b Click the + sign to expand the menu tree.

The available devices appear.

c Select the check box for the Adaptive Log Exporter Devices option and click **Next**.

d Select the **I accept the terms of the license agreement** option and click **Next**.

e Click **Finish**.

f Click **Install All**.

g When prompted, click **Yes** to restart the service.

ALE restarts.



Note: *This restarts the process, not the server.*

Step 7 To add a device:

a Click the **Devices** tab.

b Using the right mouse button (right-click) on the Windows Event Log device, select **Add Device**.

c Configure the following parameters:

- **Name** - Specify the name of the server, followed by -Event, for example, AD01-Event.
- **Device Address** - Specify the IP address of the server on which the Adaptive Log Exporter has been installed, for example, 192.168.100.100.
- Under the Windows Event Log configuration section, select the check boxes for the following options: **Application Log**, **Security Log**, **System Log**.

d Click the **Save** icon.

Step 8 To add a destination:

a Click the **Destinations** tab.

b Using the right mouse button (right-click) on Syslog UDP destination, select **Add Destination**.

c Configure the following parameters:

- **Name** - Specify the name of the STRM device, for example, STRM.
- **Syslog Server Address** - Specify the IP address of STRM, for example, 192.168.100.20.

d Click the **Save** icon.

Step 9 Map the destination to the device:

a Click the **Destinations** tab.

b Using the right mouse button (right-click) on the destination that you created in Step 8 and select **Add Device Mapping**.

c Select the device that you created in Step 7

Step 10 Click the **Deploy** icon.