IBM Security QRadar
7.2.6 and later

Adaptive Log Exporter Users Guide

The Adaptive Log Exporter software will be designated "End of Engineering" on October 31, 2015 by IBM. The Adaptive Log Exporter software might still function as expected after the 'End of Engineering' date, however, IBM will no longer release code or vulnerability updates to resolve issues with the Adaptive Log Exporter. The Adaptive Log Exporter software will be designated "End of Support" on April 30, 2016 by IBM. Administrators who use the Adaptive Log Exporter to collect Windows events in their networks can transition Adaptive Log Exporter installations to WinCollect before the "End of Support" date expires. For more information, see Migrating from the Adaptive log Exporter (ALE) to WinCollect (http://www-01.ibm.com/support/docview.wss?uid=swg21678304).

Note
Before using this information and the product that it supports, read the information in Notices.

Product information

This document applies to IBM® QRadar® Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.

CONTENTS

ABOUT THIS GUIDE

The *Adaptive Log Exporter Guide for* IBM Security QRadar SIEM provides you with information for configuring device plug-ins and receiving events from Windows hosts within your network.

Intended Audience

This guide is intended for the system administrator responsible for setting up the Adaptive Log Exporter in your network. This guide assumes that you have QRadar SIEM administrative access and a knowledge of your corporate network and networking technologies.

Conventions

The following conventions are used throughout this guide:

- ▶ Indicates that the procedure contains a single instruction.

NOTE Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION *Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.*

WARNING *Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.*

Technical Documentation	For information on how to access more technical documentation, technical notes, and release notes, see the ***Accessing IBM Security QRadar Documentation Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)
Contacting Customer Support	For information on contacting customer support, see the ***Support and Download Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

1 OVERVIEW

The Adaptive Log Exporter is an independent application that runs on a Windows-based host, that is capable of collecting Windows-based or third party device logs and forwarding events to your QRadar SIEM Console or Event Collector. Each installation of the Adaptive Log Exporter uses an Adaptive Log Exporter service to forward events to QRadar SIEM.

NOTE The Adaptive Log Exporter supports a maximum of 20 devices per installation.

The Adaptive Log Exporter supports two installation configurations:

- **Local** - The Adaptive Log Exporter is installed locally on every host in your network. Each individual host supporting the Adaptive Log Exporter is responsible for collecting local event logs from the local host and forwarding the events to QRadar SIEM. Local installations require more effort to install and configure, but does not impact performance on the host system as much as collecting logs from remote Windows-based workstations.
- **Remote** - The Adaptive Log Exporter is installed on a single host and configured to poll remote Windows-based operating systems for their event logs. Remote event collection is only supported using the Windows Event Log device plug-in, but allows the collection of event logs from multiple Windows servers or workstations. Collecting logs from a Windows system requires using NETBIOS, which is a relatively slow method of communication. Therefore, remotely collecting logs from several Windows-based hosts can cause a significant performance impact for the server hosting the Adaptive Log Exporter.

NOTE The Window Event Log is the only Adaptive Log Exporter device plug-in that supports remote event collection using the **Remote Machine** check box.

The Adaptive Log Exporter supports remote polling of event logs from the following operating systems:

- Microsoft Windows 2000
- Microsoft Windows 2003 server
- Microsoft Windows 2008 server
- Microsoft Windows XP
- Microsoft Windows 7

NOTE

Remote event collection in a one-to-many configuration requires the Adaptive Log Exporter to be configured with domain administration credentials to access remote event logs. Supplying these credentials can be considered a security risk. For more information, see **Configuring Adaptive Log Exporter Service Credentials**.

Both methods of event collection result in information being transmitted to QRadar using syslog. By default, QRadar automatically discovers and normalizes Windows event logs.

After receiving events from the Adaptive Log Exporter, QRadar can analyze, report, and store the information. To verify that your Windows logs are being processed by QRadar, use the search function in the **Log Activity** tab to filter by the source or destination IP addresses of the devices configured in your Adaptive Log Exporter. For more information on filtering for events using the **Log Activity** tab, see the *QRadar Users Guide*.

Using the Adaptive Log Exporter

The Adaptive Log Exporter provides a number of menu, tool bar, and preference options.

This section provides information on the following topics:

- **Using the Menu**
- **Using the Toolbar**
- **Using the Preferences Window**

Using the Menu

The Adaptive Log Exporter includes the following menu options:

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 **Configuring Adaptive Log Exporter Updates**.
	Exit	Allows you to exit the application.
Edit	Edit Device	Allows you to edit the settings for a currently saved device.
	Edit Destination	Allows you to edit the mapping destination for a device. For more information, see **Managing Destinations**.
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 **Configuring Adaptive Log Exporter Updates**.
	About	Allows you to view the Adaptive Log Exporter version information.

Using the Toolbar

The toolbar provides the following buttons:

Table 1-2 Toolbar Options

Icon	Description
Save	Allows you to save the current device or destination tab. Tabs with unsaved changes are indicated with an asterisks (*) symbol.
Save All	Allows you to save all device or destination tabs that contain changes. Tabs with unsaved changes are indicated with an asterisks (*) symbol.
Edit Device	Allows you to edit the settings of the selected device. This toolbar button is only available when you select a device that has been previously saved on the **Devices** tab.
Edit Destination	Allows you to edit the destination for a device. This toolbar button is only available when you select a destination that has been previously saved on the **Destination** tab.

Table 1-2 Toolbar Options (continued)

Icon	Description
Deploy	Allows you to deploy all changes made during the current session. This toolbar button is available after you have saved a device configuration or destination.
Add Plugins	Allows you to manually check for updated device plug-ins using the **Install/Update** site you configured in the preferences for the Adaptive Log Exporter. If you receive an error that states the update site is invalid, you must configure the update site in the Adaptive Log Exporter preferences. For more information, see **Configuring the Update Site**.

Using the Preferences Window

The Preferences window provides the following options:

Table 1-1 Preference Options

Menu	Sub-Menu	Description
Help		We recommend that you use the default values for the Help options.
Install/Update		Select this option to configure your update options. For more information, see **Configuring Automatic Update Preferences**.
	Automatic Updates	Select this option to schedule device and application plug-in updates to your Adaptive Log Exporter. For more information, see **Scheduling Automatic Updates**.
	Update Site	Select this option to configure the directory path or website the Adaptive Log Exporter uses for updates to download updated plug-ins. For more information, see **Configuring the Update Site**.

NOTE If you change the default values of the Adaptive Log Exporter and you want to restore default values, select **File > Preferences**, and then click **Restore Defaults**.

2 INSTALLING THE ADAPTIVE LOG EXPORTER

The Adaptive Log Exporter supports two methods of installation:

- **Standard** - A standard Adaptive Log Exporter installation is a guided installation on the local host using an install wizard.
- **Command Line** - The command line installation (CLI) allows you to use advanced installation parameters for remotely installing the Adaptive Log Exporter or configuring Windows events.

Note: The Adaptive Log Exporter does not support packaging of a bulk installer, but does provide the command line for remote bulk installations, which can be scripted. If you require assistance on packaging methods, please contact IBM Professional Services.

This section includes the following topics:

Adaptive Log Exporter system requirements

Before you begin installing the Adaptive Log Exporter, you must ensure the Windows-based host of the Adaptive Log Exporter meets the following requirements:

- The Adaptive Log Exporter can be installed on the following 32-bit or 64-bit operating systems:
  - Windows 2000
  - Windows 2003 server
  - Windows 2008 server
  - Windows 2008R2 server
  - Windows XP
  - Windows 7
- 8GB of RAM (2GB reserved for the WinCollect agent)
- Intel Core 2 Duo processor 2.0 GHz or better

- 3 GB of available disk space for software and log files
- At minimum, 20% of the available processor resources
- The print spooler service must be enabled on each system that hosts an installation of the Adaptive Log Exporter software.

Installing the Adaptive Log Exporter

Before installing the Adaptive Log Exporter using the installation wizard, close all active applications.

Procedure

Step 1 Download the AdaptiveLogExporter_setup.exe file from the IBM Support website.

https://www.ibm.com/support

Step 2 Copy the Adaptive Log Exporter setup file to your Windows-based host system.

Step 3 Double-click the setup file to launch the installation wizard.

Step 4 Click **Next**.

The End User License Agreement (EULA) is displayed.

Step 5 Read the license agreement information in the window and select **I accept the agreement** to continue.

If you select **I do not accept the agreement**, you cannot continue with the installation.

Step 6 Click **Browse** or type the installation location for the Adaptive Log Exporter.

Step 7 From the list box, select **Full installation**. This option installs the following components:

- **ALE Windows Service** - Mandatory. This option installs the Adaptive Log Exporter service, which is required to forward events to QRadar SIEM.
- **ALE Configuration User Interface** - Select this check box to Install the Adaptive Log Exporter user interface. Clearing this check box installs the Adaptive Log Exporter without the user interface and requires text-based configuration files.

Note: Installing the Adaptive Log Exporter without the user interface is intended for advanced users only. For additional information, see **Installing and Configuring ALE Using the CLI**.

Step 8 Click **Next**.

Step 9 Type a name for the Adaptive Log Exporter **Start** menu folder.

If you do not want to include an Adaptive Log Exporter folder in your **Start** menu, select the **Don't create a Start Menu folder** check box.

Step 10 Click **Next**.

Step 11 Configure the available options:

- **Create a desktop icon** - Select this check box to create an icon on your desktop for the Adaptive Log Exporter. You can also select one of the following options:
  - For all users - Select this check box to install a desktop icon for all users.
  - For the current user only - Select this check box to install a desktop icon for the logged in user.
- **Create a Quick Launch icon** - Select the check box to create an icon on your Quick Launch toolbar.
- **Run service now** - Select the **Run Service Now** check box to launch the Q1WindowsAgent service after the installation is complete.

Step 12 Click **Next**.

Step 13 Click **Install**.

Step 14 Click **Finish**.

Note: If an error occurs when attempting to launch the Adaptive Log Exporter, you must run the program using the **Run as administrator** option or set the compatibility mode in Windows. For more information on troubleshooting your installation, see **Adaptive Log Exporter Troubleshooting**.

When the installation process completes, you must configure the location that the Adaptive Log Exporter uses for updates. These updates download the latest device plug-ins for the Adaptive Log Exporter. For more information, see **Configuring the Update Site**.

Installing and Configuring ALE Using the CLI

The command line interface (CLI) allows you to install, uninstall, and update devices for the Adaptive Log Exporter without the installation wizard. This document provides information on using the command line interface (CLI) and the available options. The command line interface allows you to update or deploy your Adaptive Log Exporter to multiple remote systems using third-party products that provide remote or batch installs, for example, MSI Packaging Tools, Message-Oriented Middleware (MOM), or System Center Configuration Manager (SCCM).

The procedures in this document assume an advanced knowledge of network administration.

This section includes the following topics:

- **Basic Adaptive Log Exporter CLI Installation**
- **Advanced Installation with Windows Event Log Monitoring**
- **Uninstalling the Adaptive Log Exporter**
- **Adaptive Log Exporter CLI Utility Examples**

Basic Adaptive Log Exporter CLI Installation

To install the Adaptive Log Exporter using a CLI:

Procedure

Step 1 Download the Adaptive Log Exporter setup file from the IBM support website:

https://www.ibm.com/support

After you download the Adaptive Log Exporter, you must decide on a distribution method to deploy the Adaptive Log Exporter to remote systems in your network.

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

Step 3 From your desktop, select **Start** > **Run**.

Step 4 Type the following command:

```
cmd
```

Step 5 Click **OK**.

Step 6 Navigate to the download directory of the Adaptive Log Exporter.

Step 7 In the CLI, type the following command:

```
AdaptiveLogExporter_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES
```

Note: For additional installation parameters, see Table 2-1.

The SP-, VERYSILENT, and SUPPRESSMSGBOXES parameters are required parameters for a silent installation without launching the installation wizard or when using optional installation parameters. Installation commands must be run from the directory containing the Adaptive Log Exporter setup file.

Step 8 Configure optional installation parameters.

Table 2-1 Optional installation parameters

Parameter	Description
`/DIR`	Type the fully qualified path name to specify a non-standard installation directory for the Adaptive Log Exporter. For example, `/DIR="D:\Windows Event Tools"` If you do not specify a directory for the installation, the Adaptive Log Exporter is installed in the Program Files or Program Files (x86) directory.

Table 2-1 Optional installation parameters (continued)

Parameter	Description
/COMPONENTS	Type the following command to specify individual components you want to install. The options include: • **main** - Allows you to install the Adaptive Log Exporter service without the configuration wizard. For example, **/COMPONENT=main** • **ui** - Allows you to install the configuration wizard with the Adaptive Log Exporter service. For example, **/COMPONENT=main,ui** If you do not include the component parameter, then the service and configuration wizard are installed.
/NOICONS	Type the following command if you do not want to include the Adaptive Log Exporter icon to display in your Start menu options. For example, **/NOICONS**
/GROUP	By default, the Start menu displays the application in a folder named Adaptive Log Exporter. The group parameter allows you to define a new group name or add the icon to an existing group. For example, **/Group="System"** **or** **/Group="Accessories\System Tools"** ***Note:*** *If you specify an existing group name, the Adaptive Log Exporter icon is added to the existing folder or sub folder.*

Advanced Installation with Windows Event Log Monitoring

The default installation of the Adaptive Log Exporter only includes two device plug-ins: Windows Event Log and the File Forwarder plug-in.

The advanced installation parameters for the Adaptive Log Exporter command line allow you to configure a Windows Event Log device plug-in during the installation. The advanced installation commands are typically used to install the Adaptive Log Exporter on the remote Windows host to monitor Windows events from the installation location.

Procedure

Step 1 Copy the AdaptiveLogExporter_setup.exe to the remote location.

Step 2 From the desktop of the remote machine, select **Start > Run**.

The Run window is displayed.

Step 3 Type the following command:

cmd

Step 4 Click **OK**.

The command line interface (CLI) is displayed.

Step 5 Navigate to the directory containing the AdaptiveLogExporter_setup.exe file.

Step 6 Type the following command to install the Adaptive Log Exporter using additional parameters, if required.

For example,

```
AdaptiveLogExporter_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES /COMPONENT=main
/MONITOR="Application","Security","System"
/MONITORDEST=10.100.100.100:514 /MONITORPROTO=TCP
/DEVICEADDRESS=%computername%
```

The example above installs the Adaptive Log Exporter service on the remote Windows host and configures the Windows Event Log. The Windows Event log collects application, security, and system logs from the local installation and forwards the events to the QRadar SIEM Console or Event Collector at 10.100.100.100 using TCP on port 514.

Table 2-2 Windows Event Log Monitoring Parameters

Parameter	Description
/MONITOR	Allows you to specify the list of event logs you want to monitor on the Windows operating system. The following Windows event logs can be monitored: • Application • Security • System • **Directory Service • **DNS Server • **File Replication The event log types must be separated using a comma-separated list. For example, **/MONITOR="Application","Security","System","Directory Service","DNS Server"** ***Note:** The ** indicates that these Windows Event Logs can be configured using the command line to collected events, but the check boxes for these event types are not displayed in the configuration until you update your Windows Event Log device plug-in.*

Table 2-2 Windows Event Log Monitoring Parameters (continued)

Parameter	Description
`/MONITORDEST`	Allows you to specify the syslog destination that you want to receive the events. The IP address you type should be the address of your QRadar SIEM Console or Event Collector. For example, **`/MONITORDEST=10.100.100.100:514`** If you do not specify a port number, the default of port 514 is used for forwarding syslog events.
`/MONITORPROTO`	Allows you to select the protocol to use when sending syslog events to QRadar SIEM. The protocol can be specified as TCP or UDP. For example, **`/MONITORPROTO=TCP`** or **`/MONITORPROTO=UDP`** If this parameter is not defined, the Adaptive Log Exporter service defaults to sending events using UDP.
`/DEVICEADDRESS`	Type the hostname or IP address for the device providing the Windows events to QRadar SIEM. For example, **`/DEVICEADDRESS=10.100.100.100`** or **`/DEVICEADDRESS=workstation102`** or **`/DEVICEADDRESS=%COMPUTERNAME%`** ***Note:*** *The device address field allows you to include system variables for bulk installations of the Adaptive Log Exporter. For example, %computername%.*

Adaptive Log Exporter CLI Utility Examples

This section provides additional examples of using the CLI utility including:

- **Batch File Command Line Install Script**
- **Full Adaptive Log Exporter Installation**
- **Installing the Adaptive Log Exporter Service Only**
- **Service Only Installation Monitoring the Windows Security Log**
- **Full Install Monitoring Windows Logs**

Batch File Command Line Install Script

The following batch file contains an example script you can use to install the Adaptive Log Exporter on a remote Windows host. You must download the associated installation files and create a Windows share. The script copies the

source files from a Windows share, installs the Adaptive Log Exporter and the Windows Event Plug-in, and configures the host to forward all Microsoft Windows events to QRadar SIEM.

```
copy \\SERVER\SHARE\AdaptiveLogExporter_setup.exe c:\
copy \\SERVER\SHARE\ALE_WindowsEventLogPlugin_setup.exe c:\

FOR /F "usebackq" %%i IN (`hostname`) DO SET MYHOST=%%i
AdaptiveLogExporter_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES /NOICONS /COMPONENTS=main,ui
/MONITOR="Application","Security","System","Directory
Service","DNS Server","File Replication Service"
/MONITORDEST=<QRadar SIEM IP>:514 /DEVICEADDRESS=%MYHOST%
ALE_WindowsEventLogPlugin_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES /PATCHONLY
del c:\ALE_WindowsEventLogPlugin_setup.exe
del c:\AdaptiveLogExporter_setup.exe
```

Where **<QRadar SIEM IP>** is the IP address or hostname of your QRadar SIEM Console or Event Collector.

Note: The Directory Service, DNS Server, and File Replication events are collected by the Adaptive Log Exporter; however, the configuration interface does not display the check boxes until after you update your device plug-ins.

Full Adaptive Log Exporter Installation

Using the command for the full install requires that you update your device plug-ins and configure devices. The above command installs the Adaptive Log Exporter only. To fully install the Adaptive Log Exporter, including the service and the wizard interface, type the following command:

```
AdaptiveLogExporter_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES /COMPONENTS=main,ui
```

Installing the Adaptive Log Exporter Service Only

The Adaptive Log Exporter can be installed using the command line with or without the wizard interface. Installing the service only allows you to install the service remotely to forward events, but still requires additional parameters to forward Windows events to QRadar SIEM. To install the Adaptive Log Exporter service only, type the following command:

```
AdaptiveLogExporter_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES /COMPONENTS=main
```

Note: If you install the service without additional Windows Event Log parameters, you must update your devices using the ALE_WindowsEventLogPlugin_setup.exe. For more information, see **Updating a Windows Event Log Configuration**.

Service Only Installation Monitoring the Windows Security Log

To install the Adaptive Log Exporter service without the configuration wizard and monitor Windows security logs for the local host, type the following command:

```
AdaptiveLogExporter_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES /COMPONENTS=main /MONITOR="Security"
/MONITORDEST=10.10.100.100 /DEVICEADDRESS=Device hostname or IP
address
```

Note: In the example above, QRadar SIEM is located at IP address 10.10.100.100.

Full Install Monitoring Windows Logs

To fully install the Adaptive Log Exporter, including the configuration wizard and preconfigure a Windows Security Logs, type the following command:

```
AdaptiveLogExporter_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES /COMPONENTS=main,ui /MONITOR="Security",
"Application", "System" /MONITORDEST=10.10.100.100
/DEVICEADDRESS=%COMPUTERNAME%
```

The command line installs the Adaptive Log Exporter, and then configures the Security, Application, and System logs.

Uninstalling the Adaptive Log Exporter

To uninstall the Adaptive Log Exporter using a CLI:

Step 1 Close all active applications on the Windows host.

Step 2 On your desktop, select **Start > Run**.

The Run window is displayed.

Step 3 Type the following:

```
cmd
```

Step 4 Click **OK**.

The command line interface (CLI) is displayed.

Step 5 Navigate to the download directory of the Adaptive Log Exporter.

Step 6 In the CLI, type the following:

```
unins000.exe /SILENT /VERYSILENT
```

Windows 2008 and Windows 7 Operating Systems can require user intervention to accept the User Account Control (UAC) prompt before the uninstall can complete. For more information about UAC settings, see your Microsoft Operating System documentation.

If the command fails to uninstall the Adaptive Log Exporter, you must verify the name of the uninstall file is correct. The uninstall can be named `unins001.exe`.

3 Configuring Adaptive Log Exporter Updates

After you have installed the Adaptive Log Exporter, you must complete the following configuration steps to update your device plug-ins:

1. Configure the update site to install device plug-ins for the Adaptive Log Exporter.

   If your host does not have Internet connectivity, see **Configuring Updates for Off-line Sites**.
2. Optional. Configure a schedule to look for updated device plug-ins.
3. Optional. Configure preferences for future plug-in updates.

Configuring the update site

The update site allows you to specify a download location for device plug-in files required by the Adaptive Log Exporter.

Device plug-ins are important because they contain updates for parsing events and can include new event types or event categories.

Proocedure

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

Step 2 On the main menu, select **File > Preferences**.

Step 3 Click the **+** icon to expand the Install/Update navigation tree.

Step 4 On the navigation menu, select **Update Site**.

Step 5 In the **Update Site URL** field, type the location of your update site file.

For example,

- To update from a Windows share, type the path to your server:
  `file://<SOMEWINDOWSSERVER>/ALE/UpdateSite`
- To update from a local file, type the path to the file:
  `file:///e:/UpdateSite`

Note: If you choose a Windows server or local file, you must download the ALEUpdateSite.zip file from the IBM Support website and extract the file to a Windows share or file repository. The update site file is located at the following address: *http://www.ibm.com/support/fixcentral/*. For more information, see **Configuring Updates for Off-line Sites**.

Step 6 Click **Apply**.

Step 7 Click **OK**.

Step 8 On the toolbar, click **Add Plugins**.

Step 9 Click the **+** to expand the device list.

Step 10 Choose one of the following options:

a To install all available device plug-ins, select the top level check box.

b To install specific device plug-ins, select a check box for each device plug-in to install.

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 11 To install all dependent plug-ins, click **Select Required**.

If you selected device plug-ins that requires additional software an error can display. Click **Error Details** for additional information.

Step 12 Click **Next**.

Step 13 Read the license associated with the selected device. To continue, you must select the **I accept the terms of the license agreement** option.

Step 14 Click **Next**.

Note: You must install your device plug-ins to the default location.

Step 15 Click **Finish**.

Step 16 Click **Install All** to install all chosen devices.

After the device plug-in installations complete, you are ready to configure your syslog destination. For more information, see **Managing Destinations**.

Configuring updates for off-line sites

The Adaptive Log Exporter might be configured on a host that does not have Internet connectivity.

Hosts without Internet connectivity is often the case when the Adaptive Log Exporter is used on hardened network assets. For these systems we recommend you download and configure a local site for updating the Adaptive Log Exporter device plug-ins.

Procedure

Step 1 From a system with Internet connectivity, download the ALEUpdateSize.zip file.

http://www.ibm.com/support/fixcentral/

Step 2 Copy the file to the Adaptive Log Exporter host or a local Windows share.

Step 3 Extract the file.

You must keep the folder and directory structure intact when you extract the ALEUpdateSize.zip file.

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

Step 5 From the main menu, select **File > Preferences**.

Step 6 Click the **+** icon to expand the Install/Update navigation tree.

Step 7 From the navigation menu, select **Update Site**.

Step 8 In the **Update Site URL** field, type the location of your update site file.

For example,

- To update from a Windows share, type the path to your server:

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

- To update from a local file, type the path to the file:

  `file:///e:/UpdateSite`

Step 9 Click **Apply**.

Step 10 Click **OK**.

Step 11 From the toolbar, click **Add Plugins**.

Step 12 Click the **+** to expand the device list.

Step 13 Choose one of the following options:

a To install all available device plug-ins, select the top level check box.

b To install specific device plug-ins, select a check box for each device plug-in to install.

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 14 To install all dependent plug-ins, click **Select Required**.

If you selected device plug-ins that requires additional software an error can display. Click **Error Details** for additional information.

Step 15 Click **Next**.

The Feature License window is displayed.

Step 16 Read the license associated with the selected device. To continue, you must select the **I accept the terms of the license agreement** option.

Step 17 Click **Next**.

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

Step 18 Click **Finish**.

Step 19 Click **Install All** to install all chosen devices.

After the device plug-in installations complete, you are ready to configure your syslog destination. For more information, see **Managing Destinations**.

Scheduling Automatic Updates

You can configure the Adaptive Log Exporter to automatically search for device plug-in updates. Device plug-in updates are important because they often contain event parsing updates and can include new event types or event categories.

Procedure

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

Step 2 On the toolbar, select **File > Preferences**.

Step 3 In the navigation manu, click the **+** sign next to Install/Update.

Step 4 Click **Automatic Updates**.

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

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 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 notifications when device updates are available.
- **Download new updates automatically and notify me when ready to install them** - Enables the system to download updates automatically and notifies you when the updates are ready to install.

Step 8 Click **Apply**.

Step 9 Click **OK**.

The automatic update schedule is complete.

Configuring automatic update preferences

After you have updated your device plug-ins, you can define the content installed in future device plug-in updates.

Procedure

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

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

Step 3 Click **Install/Update**.

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

Step 5 Select the **Check digital signatures of downloaded archives** check box.

By default, this check box is selected to prevent unauthorized or unsigned signatures from being installed.

Step 6 Select one of the following update options:

- **equivalent** - Equivalent updates include device plug-ins that are at the same revision level as your Adaptive Log Exporter application.
- **compatible** - Compatible updates include any device plug-ins that work with your Adaptive Log Exporter regardless of the software revision of the device plug-in.

Step 7 To define 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 might need to schedule event uploads to minimize the potential high load on the network. For assistance creating a custom update policy, contact IBM Corp. Customer Support.

Step 8 To define specific proxy settings for your updates:

a Select the Enable **HTTP Proxy connection** check box.

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

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

Step 9 Click **Apply**.

Step 10 Click **OK**.

4 MANAGING DESTINATIONS

Destinations in the Adaptive Log Exporter allow you to create a syslog forwarding destination for events and map specific devices to the destination address. This allows you to create unique destinations for each of the device plug-ins in your network, but in most cases, you only need to map your devices directly to your QRadar SIEM Console or Event Collector. The Adaptive Log Exporter allows you to create three types of destinations:

- **Syslog TCP** - Allows you to forward syslog events using the TCP protocol on the port of your choosing.
- **Syslog UDP** - Allows you to forward syslog events using the UDP protocol on the port of your choosing.
- **Logger** - Allows you to log events to a local file on the Adaptive Log Exporter host.

Configuring destinations

The destination provides the Adaptive Log Exporter with an event forwarding destination for event logs. You must configure the destination before you configure individual device plug-ins for the Adaptive Log Exporter. These destinations are then mapped to the device plug-in, which allows each device to forward events to the appropriate destination.

This section includes the following topics:

Adding a syslog TCP destination

The following instructions include the steps required to create a destination address or log file of events for the Adaptive Log Exporter. You can create an individual destination or multiple destinations and save them all simultaneously from the toolbar.

As you open tabs for devices or destinations, unsaved changes display the * character next to their name. If you select **Save All** from the toolbar, this saves all open tabs with changes. Issues that prevent the tab from saving generate an error message and the * character is still displayed on the tab.

Procedure

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

Step 2 Click the **Destinations** tab.

The Destinations tab is displayed showing the three destination types that can be created.

Step 3 Right-click on a destination type and select **Add Destination**.

Step 4 Configure the following values:

Table 4-1 Syslog TCP parameters

Parameter	Description
Name	Type the name you want to assign this destination. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Syslog Server Address	Type the IP address or hostname of the syslog destination. The information specified in this field is typically the IP address or hostname of your QRadar SIEM Console or Event Collector.
Syslog Server Port	Type the port number used for receiving events by the syslog destination. By default, QRadar SIEM Consoles and Event Collectors listen on port 514 for TCP and UDP syslog.
Append Line Terminator	Select this check box to include a line termination character at the end of every TCP syslog event message.
Number of Threads	Type the number of concurrent processing threads you want to run in this destination. The default is 1.

Step 5 Click **Save**.

Step 6 Click **Deploy**.

The configuration is complete for your TCP protocol destination.

Adding a syslog UDP destination

The following instructions include the steps required to create a syslog destination for UDP events. You can create an individual destination or create multiple destinations, and then save them simultaneously from the toolbar.

As you open tabs for devices or destinations, unsaved changes display the * character next to their name. If you select **Save All** from the toolbar, this saves all open tabs with changes. Issues that prevent the tab from saving generate an error message and the * character is still displayed on the tab.

CAUTION: *We recommend that you configure a TCP syslog destination if the event payload for your device exceeds 1024 bytes.*

Procedure

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

Step 2 Click the **Destinations** tab.

The Destinations tab is displayed showing the three destination types that can be created.

Step 3 Right-click on **Syslog UDP** and select **Add Destination**.

Step 4 Configure the following values:

Table 4-1 Syslog UDP parameters

Parameter	Description
Name	Type the name you want to assign this destination. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Syslog Server Address	Type the IP address or hostname of the syslog destination. The information specified in this field is typically the IP address or hostname of your QRadar SIEM Console or Event Collector.
Syslog Server Port	Type the port number used for receiving events by the syslog destination. By default, QRadar SIEM Consoles and Event Collectors listen on port 514 for TCP and UDP syslog.
Number of Threads	Type the number of concurrent processing threads you want to run in this destination. The default is 1.

Step 5 Click **Save**.

Step 6 Click **Deploy**.

The configuration is complete for your UDP protocol destination.

Adding a logger destination

The following instructions include the steps required to create a logger destination for the Adaptive Log Exporter.

Note: As you open tabs for devices or destinations, unsaved changes display the * character next to their name. If you select **Save All** from the toolbar, this saves all open tabs with changes. Issues that prevent the tab from saving generate an error message and the * character is still displayed on the tab.

Procedure

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

Step 2 Click the **Destinations** tab.

The Destinations tab is displayed showing the three destination types that can be created.

Step 3 Right-click on **Logger** and select **Add Destination**.

Step 4 Configure the following values:

Table 4-1 Logger parameters

Parameter	Description
Name	Type the name you want to assign this destination. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Logger Prefix	Type the heading you want to assign to the logs. The Logger Prefix must start with **Device.Events** and may contain letters, numbers and periods.
Prepend syslog header	Select this check box if you want the syslog header to be attached to the message in the logs.
Number of Threads	Type the number of concurrent processing threads you want to run in this destination. The default is 1.

Step 5 Click **Save**.

Step 6 Click **Deploy**.

The configuration is complete for your logger destination.

Editing a destination

To edit a destination:

Procedure

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

Step 2 Click the **Destinations** tab.

Step 3 Click the **+** sign to expand the menu tree for your destination.

Step 4 Select your destination and click **Edit Destination**.

Step 5 Update your destination parameters.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

The new event destination changes are complete. The device plug-ins mapped to the edited destination should start arriving with the new parameters after the deploy process completes.

Deleting a destination

To delete a destination:

Procedure

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

Step 2 Click the **Destination** tab.

Step 3 Click **+** to expand the menu tree for your destination.

Step 4 Right-click on the destination name and select **Delete Destination**.

Step 5 Click **OK**.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

5 CONFIGURING CISCO ACS

The Adaptive Log Exporter monitors all comma-separated value log files from the root log directory you define when configuring the device plug-in.

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1 Configure the Adaptive Log Exporter update site.

2 Configure a destination for your Cisco ACS events.

If these steps are complete, you are ready to configure your Cisco ACS device plug-in and map your device to a destination.

Configuring Cisco ACS

The Cisco ACS device plug-in allows you to configure the root log directory for your comma-separated log files, configure polling options, and create a name and IP address to identify your device. After you configure your device, you can map your Cisco ACS to a syslog destination.

To configure a Cisco ACS:

1 Add and configure a Cisco ACS device plug-in the Adaptive Log Exporter. For more information, see **Configuring the Cisco ACS Device Plug-in**.

2 Map the Cisco ACS device plug-in to a destination. For more information, see **Creating a Device Mapping**.

Configuring the Cisco ACS device plug-in

The Adaptive Log Exporter monitors all comma-separated value log files from the root log directory you define when configuring the device plug-in.

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Right click on **Cisco ACS** and select **Add Device**.

The device properties for adding new Cisco ACS device are displayed.

Step 4 Configure the following parameters:

Table 5-1 Cisco ACS plug-in parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your Cisco ACS device.
Root Log Directory	Click **Browse** or type the location of the Cisco ACS log files. Cisco ACS monitors all comma-seperated value (csv) files in the Root Log Directory. By default, Cisco ACS log files are located in **`<ACS Install Directory>\<Service Name>\Logs`**. Where: **`<ACS Install Directory>`** is the install directory of Cisco ACS. **`<Service Name>`** is the directory that identifies the Cisco ACS service. ***Note:*** *Do not use the Cisco ACS device plug-in to monitor files that can only be accessed over the network, such as a file share.*
Throttle timeout	Type the delay between polling events, in milliseconds, for the Cisco ACS device. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The higher the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 Click **Save**.

You are now ready to map your Cisco ACS device to a syslog destination.

Creating a device mapping

After you have configured your device, you must map your device to a destination.

Procedure

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your Cisco ACS device.

A mapping is created for your Cisco ACS device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your Cisco ACS device.

Step 8 Repeat this process to create and map additional Cisco ACS devices.

The Cisco ACS configuration is complete.

6 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.

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1. Configure the Adaptive Log Exporter update site.
2. Configure a destination for your Cisco CSA events.

If these steps are complete, you are ready to configure your Cisco CSA device plug-in and map your device to a destination.

Configuring Cisco CSA

The Cisco CSA device plug-in allows you to configure the root log directory for your active alert file, configure polling options, and create a name and IP address to identify your device. After you configure your device, you can map your Cisco CSA to a syslog destination.

To configure Cisco CSA:

1. Add and configure a Cisco CSA device plug-in. For more information, see **Configuring the Cisco CSA Device Plug-in**.
2. Map the Cisco CSA device plug-in to a destination. For more information, see **Creating a Device Mapping**.

Configuring the Cisco CSA Device Plug-in

To configure your Cisco CSA in the Adaptive Log Exporter:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **Cisco CSA** and select **Add Device**.

The device properties for adding a new Cisco CSA device are displayed.

Step 4 Configure the following parameters:

Table 6-1 Cisco CSA Plug-in Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your Cisco CSA device.
Root Log Directory	Click **Browse** or type the location of the CSA MC alert log files. By default, the CSA alert log files are located in the following directory: `C:\alerts\` ***Note:*** *Do not use the Cisco CSA device plug-in to monitor files that can only be accessed over the network, such as a file share.*
Log Filename	Type the name of the active alert log file. The Adaptive Log Exporter monitors this log file for events. The default value for the log file is logfile.txt. Events are written to the active alert log file as a UTF-8 encoded text file in the Root Log Directory. ***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). After a log file exceeds 1 MB in size, 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.*
Throttle timeout	Type the delay between polling events, in milliseconds, for the Cisco CSA device. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The higher the value specified in the throttle timeout indicates that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout indicates that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 Click **Save**.

Step 6 Repeat this process to create and configure additional Cisco CSA device plug-ins.

You are now ready to map your Cisco CSA device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

Procedure

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your Cisco CSA device.

A mapping is created for your Cisco CSA device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your Cisco CSA device.

Step 8 Repeat this process to map additional Cisco CSA devices.

The Cisco CSA configuration is complete.

7 CONFIGURING A FILE FORWARDER DEVICE

The File Forwarder plug-in allows you to take an event log from an unsupported device or log type and forward the events to QRadar SIEM. The log files read by the File Forwarder device plug-in must be text based, single-line events. Multi-line events are not supported. After you configure the File Forwarded plug-in to forward the events to QRadar SIEM, you can create a Universal DSM to parse and categorize events.

We recommend you configure the File Forwarder device plug-in to use unique values of the **Starts With** and **Ends With** fields, if:

- Multiple devices are writing log files to the same root log directory.
- Your root log directory contains a mix of log files from devices that use the **Continuously Monitor Files** check box differently.

CAUTION

If a log file is copied to the Root Log Directory and overwrites an existing file, the events in the new file might not be properly forwarded to QRadar SIEM. The File Forwarder plug-in is intended to monitor existing files being appended or newly created event log files.

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1. Configure the Adaptive Log Exporter update site. For more information, see **Configuring the Update Site**.
2. Configure a destination for your File Forwarder events. For more information, see **Configuring Destinations**.

If these steps are complete, you are ready to configure your Cisco CSA device plug-in and map your device to a destination.

Configuring a File Forwarder

The File Forwarder device plug-in allows you to configure the root log directory for your file, select the starting and ending file identifiers, and create a name and IP address to identify your device. After you configure your device, you can map your File Forwarder to a syslog destination.

To configure a File Forwarder:

1 Add and configure a File Forwarder device plug-in for the Adaptive Log Exporter. For more information, see **Configuring the File Forwarder Device Plug-in**.

2 Map the File Forwarder device plug-in to a destination. For more information, see **Creating a Device Mapping**.

Configuring the File Forwarder Device Plug-in

To configure a file forwarder in the Adaptive Log Exporter:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **File Forwarder** and select **Add Device**.

The device properties for a adding new File Forwarder device are displayed.

Step 4 Configure the following parameters:

Table 7-1 File Forwarder Plug-in Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your File Forwarder device.
Root Log Directory	Click **Browse** or type the location of the log files to forward to QRadar SIEM. ***Note:*** *Do not use the File Forwarder device plug-in to monitor files that can only be accessed over the network, such as a file share.*

Table 7-1 File Forwarder Plug-in Parameters (continued)

Parameter	Description
Starts with	Select this check box and type a pattern to define a specific character combination matching the first letters or numbers \ in the name of your log file. This field allows you to select a specific log file from a directory that can contain several other log file types. For example, if you have a directory containing log files labeled IPv4.log and IPv6.log, this field allows you to select all files starting with IPv4. To select only IPv4 files for forwarding, type **IPv4** in the **Starts With** field. This string can be up to 255 characters in length and does not support wildcard (*****) characters.
Ends with	Select this check box and type a pattern to define a specific character combination matching the end of your log file. This field allows you to select a specific log file from a directory that can contain several other log file types. For example, to monitor all files ending in .log, type **.log** as the value in the **Ends With** field. This string can be up to 255 characters in length and does not support wildcard (*****) characters.
Only Monitor Files Created Today	Select this check box if you only want to monitor files with a creation date matching the current date. The Adaptive Log Exporter evaluates the root log directory for files created today when a change to the root log directory occurs. For example, new files are created or deleted.
Continuously Monitor Files	Select or clear the check box. • If the check box is selected, log files in the root log directory are continually monitored for changes in file size. When a new log file is written to the root log directory, the log file is processed when an increase in the file size is detected. After the file size change is detected, all lines of the log file are processed. The processed events are forwarded to QRadar SIEM. Existing log files in the root log directory are monitored and processed every time an increase in the file size is detected. New lines that have been added to the file since the last time the file was processed are forwarded to QRadar SIEM. • If the check box is clear, new log files created in the root log directory are read once and processed. Further changes to the log file are ignored.

Table 7-1 File Forwarder Plug-in Parameters (continued)

Parameter	Description
Throttle timeout	Type the delay between polling events, in milliseconds, for the File Forwarder plug-in. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The higher the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 Click **Save**.

Step 6 Repeat this process to create and configure additional File Forwarder device plug-ins.

You are now ready to map your File Forwarder device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your File Forwarder device.

A mapping is created for your File Forwarder to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your File Forwarder device.

Step 8 Repeat this process to map additional File Forwarder devices.

The File Forwarder configuration is complete for the Adaptive Log Export. However, events from your File Forwarder device plug-in are categorize as generic events by QRadar SIEM. You can create a Universal DSM to parse and categorized these events.

8 Configuring the XML File Forwarder Device

The XML File Forwarder plug-in allows the Adaptive Log Exporter to monitor XML-based log files and forward specific data from the event logs to QRadar SIEM. XML files are read by identifying element tags within the XML file that contain the event payload. The Adaptive Log Explorer monitors changes to the root log directory for XML files with names matching the specified starts with or ends with text pattern.

We recommend you configure the XML File Forwarder device plug-in to use unique values of the **Starts With** and **Ends With** fields, if:

- Multiple devices are writing log files to the same root log directory.
- Your root log directory contains a mix of log files from devices that use the **Continuously Monitor Files** check box differently.

CAUTION

If a log file is copied to the Root Log Directory and overwrites an existing file, the events in the new file might not be properly forwarded to QRadar SIEM*. The XML File Forwarder plug-in is intended to monitor existing files being appended or newly created XML event log files.*

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1. Configure the Adaptive Log Exporter update site. For more information, see **Configuring the Update Site**.
2. Configure a destination for your File Forwarder events. For more information, see **Configuring Destinations**.

If these steps are complete, you are ready to configure your XML File Forwarder device plug-in and map your device to a destination.

Configuring an XML File Forwarder

The XML File Forwarder device plug-in allows you to monitor an XML file for specific XML element tags containing your event payload. You can configure the root log directory for your file, select the starting and ending XML file identifiers,

and define the element tags that contain your events. After you configure your device, you can map your XML File Forwarder to a syslog destination.

To configure an XML File Forwarder device, you must:

1 Add and configure your XML File Forwarder device plug-in. For more information, see **Configuring the XML File Forwarder Device Plug-in**.

2 Map the XML File Forwarder device to a destination. For more information, see **Creating a Device Mapping**.

Configuring the XML File Forwarder Device Plug-in

To configure an XML file forwarder in the Adaptive Log Exporter:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **XML File Forwarder** and select **Add Device**.

The device properties for adding a new File Forwarder device are displayed.

Step 4 Configure the following parameters:

Table 4-1 XML File Forwarder Plug-in Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your XML File Forwarder device.
Root Log Directory	Click **Browse** or type the location of your XML log files. ***Note:*** *Do not use the XML File Forwarder device plug-in to monitor files that can only be accessed over the network, such as a file share.*
Starts with	Select this check box and type a pattern to define a specific character combination matching the first letters or numbers \ in the name of your log file. This field allows you to select a specific log file from a directory that can contain several other log file types. For example, if you have a directory containing log files labeled IPv4.log and IPv6.log, this field allows you to select all files starting with IPv4. To select only IPv4 files for forwarding, type **IPv4** in the **Starts With** field. This string can be up to 255 characters in length and does not support wildcard (*) characters.

Table 4-1 XML File Forwarder Plug-in Parameters (continued)

Parameter	Description
Ends with	Select this check box and type a pattern to define a specific character combination matching the end of your log file. This field allows you to select a specific log file from a directory that can contain several other log file types. For example, to monitor all files ending in .log, type **.log** as the value in the **Ends With** field. This string can be up to 255 characters in length and does not support wildcard (*) characters.
Only Monitor Files Created Today	Select this check box if you only want to monitor files with a creation date matching the current date. The Adaptive Log Exporter evaluates the root log directory for files created today when a change to the root log directory occurs. For example, new files are created or deleted.
Main Element Tag	Type the XML element that is considered an event. This element and all of the associated child elements are processed.
Translate Element Tag	Type the translators required to correctly parse the XML element. This field allows you to substitute an element with another text value that is easier to parse. For example, **<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	Select this check box to ignore elements that contain empty values. Elements that does not have an associated value are not inserted into the payload. For example, elements that resemble x.y.z = with no data are not inserted into the payload.

Table 4-1 XML File Forwarder Plug-in Parameters (continued)

Parameter	Description
Continuously Monitor Files	Select or clear the check box. • If the check box is selected, log files in the root log directory are continually monitored for changes in file size. When new log files are written to the root log directory, the XML files are processed when an increase in the file size is detected. After the file size change is detected, all lines of the XML file are processed. The processed events are forwarded to QRadar SIEM. Existing log files in the root log directory are monitored and processed every time an increase in the file size is detected. New lines that have been added to the file since the last time the file was processed are forwarded to QRadar SIEM. • If the check box is clear, new log files created in the root log directory are read once and processed. Further changes to the log file are ignored.
Throttle timeout	Type the delay between polling events, in milliseconds, for the XML File Forwarder plug-in. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The higher the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 On the Adaptive Log Exporter toolbar, click **Save**.

You are now ready to map your File Forwarder device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your XML File Forwarder device.

A mapping is created for your XML File Forwarder to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your File Forwarder device.

Step 8 Repeat this process to map additional XML File Forwarder devices.

The File Forwarder configuration is complete for the Adaptive Log Export. However, events from your XML File Forwarder device plug-in are categorize as generic events by QRadar SIEM. You can create a Universal DSM to parse and categorized these events.

9 CONFIGURING JUNIPER STEEL-BELTED RADIUS (SBR)

The Juniper Steel-Belted Radius (SBR) plug-in for the Adaptive Log Exporter allows you to collect logs for the Juniper Steel-Belted Radius appliance and forward the events to QRadar SIEM. The Adaptive Log Exporter must be installed on the same host as Juniper SBR. The Adaptive Log Exporter must be updated to include the latest Juniper SBR device plug-in.

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1. Configure the Adaptive Log Exporter update site. For more information, see **Configuring the Update Site**.
2. Configure a destination for your Juniper SBR events. For more information, see **Configuring Destinations**.

If these steps are complete, you are ready to configure your Juniper SBR device plug-in and map your device to a destination.

Configuring Juniper Steel-Belted Radius

The Juniper SBR device plug-in allows you to configure the root log directory for your comma-separated event log file, configure polling options, and create a name and IP address to identify your device. After you configure your device, you can map your Juniper SBR to a syslog destination.

To configure a Juniper Steel-Belted Radius:

1. Add and configure Juniper SBR device plug-in. For more information, see **Configuring the Juniper SBR Device Plug-in**.
2. Map the device plug-in to a destination. For more information, see **Creating a Device Mapping**.

Configuring the Juniper SBR Device Plug-in

To configure a Juniper Steel-Belted Radius device:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **Juniper SBR** and select **Add Device**.

The device properties for adding a new Juniper SBR device are displayed.

Step 4 Configure the following parameters:

Table 5-1 Juniper SBR Plug-in Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your Juniper SBR device.
Root Log Directory	Click **Browse** or type the location of the Juniper SBR log files. The Adaptive Log Exporter monitors the root log directory for any comma-separated value (.csv) files with a file name containing a date stamp matching the current day. Report log files should be located in the following Steel-Belted Radius directory: **`<radiusdir>\authReports`** ***Note:*** *The Juniper SBR device must have the authReport.ini initialization file configured to generate the following log files in the root log directory:* • **Authentication acceptance report** - The file in the root log directory must match accepts_yyyymmdd.csv. • **Authentication rejection report** - The file in the root log directory must match rejects_yyyymmdd.csv. • **Unknown authentication client report** - The file in the root log directory must match unknownClient_yyyymmdd.csv. • **Invalid shared secret report** - The file in the root log directory must match badSharedSecret_yyyymmdd.csv. ***Note:*** *Do not use the Juniper SBR device plug-in to monitor files that can only be accessed over the network, such as a file share.*
Throttle timeout	Type the delay between polling events, in milliseconds, for the device. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The higher the value specified in the throttle timeout indicates that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout indicates that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 Click **Save**.

Step 6 Repeat this process to create and configure additional Juniper SBR device plug-ins.

You are now ready to map your Juniper Steel-Belted Radius device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your Juniper SBR device.

A mapping is created for your Juniper SBR device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your Juniper SBR device.

Step 8 Repeat this process to map additional Juniper SBR devices.

The Juniper SBR configuration is complete.

10 Configuring the NetApp Data ONTAP Device

The NetApp Data ONTAP device plug-in allows you to audit your NetApp storage device by monitoring audit events from the Data ONTAP operating system. The NetApp Data ONTAP device plug-in monitors event log files in the Remote Log Directory and copies the event log files to a local directory for processing. The processed events are then forwarded to QRadar SIEM as syslog events.

You must configure the Adaptive Log Exporter service with NetApp Data ONTAP administrative user credentials. The user account must have read privileges to the Remote Log Directory and Local Temporary Directory. For more information, see **Configuring Adaptive Log Exporter Service Credentials**.

CAUTION

The NetApp Data ONTAP plug-in only supports the Common Internet File System (CIFS) protocol.

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1. Configure the Adaptive Log Exporter update site. For more information, see **Configuring the Update Site**.
2. Configure a destination for your NetApp Data ONTAP events. For more information, see **Configuring Destinations**.

If these steps are complete, you are ready to configure your NetApp device plug-in and map your device to a destination.

Configuring NetApp Data ONTAP

The NetApp device plug-in allows you to configure the root log directory for your event (.evt) files, configure polling options, and create a name and IP address to identify your device. After you configure your device, you can map your NetApp Data ONTAP to a syslog destination.

To configure a NetApp Data ONTAP device, you must:

1 Add and configure NetApp Data ONTAP device plug-in. For more information, see **Configuring the NetApp Data ONTAP Device Plug-in**.

2 Map the device plug-in to a destination. For more information, see **Creating a Device Mapping**.

Configuring the NetApp Data ONTAP Device Plug-in

To configure your NetApp device in the Adaptive Log Exporter:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **NetApp** and select **Add Device**.

The device properties for adding a new NetApp device is displayed.

Step 4 Configure the following parameters:

Table 6-1 NetApp Data ONTAP Plug-in Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your NetApp Data ONTAP device.
Root Log Directory	Click **Browse** or type the directory location for your NetApp Data ONTAP log files. The following directory location is the default directory for storing NetApp Data ONTAP event files: `/etc/log` QRadar SIEM monitors the directory for Event (.evt) files. Event files in the Remote Log Directory are processed if the time and date stamp of the event file is newer than the last scan time of the plug-in. If you are using Windows 2008 Server, Windows Vista, or Windows 7, the Adaptive Log Exporter converts .evt files in the Remote Log Directory to the .evtx format using the wevtutil.exe utility, which is included with your operating system. For more information on using wevutil.exe, see your Microsoft Operating System documentation. ***Note:*** *Do not use the NetApp device plug-in to monitor files that can only be accessed over the network, such as a file share.*

Table 6-1 NetApp Data ONTAP Plug-in Parameters (continued)

Parameter	Description
Local Temporary Directory	Type the directory location where the NetApp plug-in copies event files. After an event file is copied from the specified location, the event file is processed and deleted from the temporary directory.
Remote Directory Poll Interval (seconds)	Type the delay between polling events, in seconds, for the NetApp device. The minimum polling interval is 60 seconds. The larger the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.
Enable EPS Throttle	Select this check box to enable EPS throttling and type the maximum number of events the NetApp plug-in allowed to forward to QRadar SIEM every second. By default, EPS throttle is disabled. ***Note:*** *EPS Throttling does not delay the processing of the events, but does queue NetApp events in memory for delivery to QRadar SIEM. If you enable EPS throttling, we recommend that you carefully tune your configuration. If events are generated at a greater rate than the events are forwarded, events may be dropped.*

Step 5 Click **Save**.

Step 6 Repeat this process to create and configure additional NetApp device plug-ins.

You are now ready to map your NetApp Data ONTAP device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your NetApp Data ONTAP device.

A mapping is created for your NetApp Data ONTAP device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your NetApp Data ONTAP device.

Step 8 Repeat this process to map additional NetApp Data ONTAP devices.

The NetApp Data ONTAP configuration is complete.

11 CONFIGURING THE WINDOWS EVENT LOG DEVICE

In Microsoft Windows an event is a significant occurrence in the system. Events can be generated by programs, applications, security events, or system notifications. Event logs enable you to identify and diagnose the source of system problems or help you predict potential asset problems. The Windows Event Log is unique from the other device plug-ins because it allows remote polling of other Windows hosts for their event logs. We recommend that you configure a maximum of 20 Windows Event Log Devices.

CAUTION

Windows Event Log files can contain payloads larger than 1024 bytes, which is the maximum payload size for the UDP protocol. We recommend that you configure a TCP syslog destination for Windows Event Log device plug-ins reporting events for Windows 2008 Server.

The Microsoft Windows Event Log can record the following event logs:

- Application Logs
- Security Logs
- System Logs
- Directory service logs
- DNS Server Logs
- File Replication Service Logs

NOTE

The Adaptive Log Exporter might not display check boxes for Directory Service Logs, DNS Server Logs, or File Replication Service Logs if you have not updated your device plug-ins. For more information, see **Configuring the Update Site**.

When accessing Windows Event Logs on a remote machine using the **Remote Machine** field, you must specify a user account with administrative privileges for the Adaptive Log Exporter service. Domain administrative privileges might be required if you are remotely accessing logs located on domain controllers. The Adaptive Log Exporter service uses these credentials to retrieve log files from remote sources. For more information, see **Configuring Adaptive Log Exporter Service Credentials**.

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1 Configure the Adaptive Log Exporter update site. For more information, see **Configuring the Update Site**.

2 Configure a destination for your Windows Event Log events. For more information, see **Configuring Destinations**.

If these steps are complete, you are ready to configure your Windows Event Log device plug-in and map your device to a destination.

Configuring Windows Event Log

The Windows Event Log device plug-in allows you to configure the events logs to collect using check boxes. Selecting a check box allows the Windows Event Log device plug-in to request the information for the local or remote Windows host using an application programming interface (API). You can configure polling options, collect events from remote Windows hosts, and create a name and IP address to identify your device. After you configure your device, you can map your Windows Event Log device to a syslog destination.

To configure a Windows Event Log device:

1 Add and configure a Windows Event Log device plug-in. For more information, see **Configuring the Windows Event Log Device Plug-in**.

2 Map the device to a destination. For more information, see **Creating a Device Mapping**.

Configuring the Windows Event Log Device Plug-in

To configure your Microsoft Event Log device in the Adaptive Log Exporter:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **Windows Event Log** and select **Add Device**.

The device properties for adding a new Windows Event Log device are displayed.

Step 4 Configure the following parameters:

Table 7-1 Windows Event Log Plug-in Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.

Table 7-1 Windows Event Log Plug-in Parameters (continued)

Parameter	Description
Device Address	Type the IP address or hostname for your local or remote Windows host. ***Note:*** *You only need to specify a remote IP address or hostname when using the* ***Remote Machine*** *check box.*
Windows Event Log Configuration	
Application Log	Select this 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 this check box if you want the device to monitor the security log. The security log records security-based events, such as, valid and invalid logon attempts, creating files, opening files, or deleting files from the network. You must have administrator privileges or be a member of the administrators group to enable, use, and specify which events you want to record in the security log.
System Log	Select this 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. The operating system contains a predetermined list of events that are logged by system components.
Directory Service Log	Select this check box if you want the device to monitor the directory service log file. The directory service log contains events logged by the Active Directory domain controller.
DNS Server Log	Select this check box if you want the device to monitor the Domain Name Service (DNS) server log file. The DNS server log file contain events related to the resolution of DNS names to IP addresses.
File Replication Log	Select this check box if you want the device to monitor the file replication service log file. The file replication log tracks replication between domain controllers.

Table 7-1 Windows Event Log Plug-in Parameters (continued)

Parameter	Description
Remote Machine	Select this check box and type the path to the remote machine to allow the Adaptive Log Exporter to retrieve Windows Event Logs from a remote machine. The path must be specified using a Universal Naming Convention (UNC) name. For example, **`\\host123`** or **`\\172.16.20.98`**. The **Remote Machine** field can include up to 255 characters. ***Note:*** *The Adaptive Log Exporter Service must be configured with the correct permission level to read WIndows Event Logs from a remote Windows host. You must provide Domain Administrator credentials to the Adaptive Log Exporter service. For more information, see* **Configuring Adaptive Log Exporter Service Credentials**.
Polling Interval	Type the delay between polling for events, in milliseconds, from a remote machine containing Windows Event Logs. The default polling interval is 5000 milliseconds. The higher the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated Windows Event Logs on the remote machine less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks the remote machine for updated Windows Event Logs more often.
Advanced Configuration	
Throttle timeout	Type the delay between polling events, in milliseconds, for the Windows Event Log device. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The higher the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 Click **Save**.

Step 6 Repeat this process to create and configure additional Windows Event Log device plug-ins.

You are now ready to map your Windows Event Log device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your Windows Event Log device.

A mapping is created for your Windows Event Log device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your Windows Event Log device.

Step 8 Repeat this process to map additional Windows Event Log devices.

The Windows Event Log configuration is complete.

12 Configuring the Microsoft DHCP Device

In the Microsoft Windows Server suite, 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.

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1. Configure the Adaptive Log Exporter update site. For more information, see **Configuring the Update Site**.
2. Configure a destination for your Windows DHCP Server events. For more information, see **Configuring Destinations**.

If these steps are complete, you are ready to configure your Windows DHCP device plug-in and map your device to a destination.

Configuring a Microsoft DHCP Device

The Windows DHCP device plug-in allows you to configure the root log directory for your DHCP log files, configure polling options, and create a name and IP address to identify your device. After you configure your device, you can map your Windows DHCP device to a syslog destination.

To configure a Microsoft DHCP device, you must:

1. Add and configure a Microsoft DHCP device plug-in for the Adaptive Log Exporter. See **Configuring a Microsoft DHCP Device**.
2. Map the device to a destination. For more information, see **Creating a Device Mapping**.

Configuring the Windows DHCP Device Plug-in

To configure your Microsoft DHCP device in the Adaptive Log Exporter:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **Windows DHCP** and select **Add Device**.

The device properties for adding a new Windows DHCP device are displayed.

Step 4 Configure the following parameters:

Table 8-1 Windows DHCP Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your DHCP Server.
Root Log Directory	Click **Browse** or type the directory location for your Windows DHCP log files. The Windows DHCP plug-in monitors the Root Log Directory for **DhcpSrvLog** and **DhcpV6SrvLog** log files to be modified. The day of the week specified in the file name determines the current log file. Windows DHCP audit log files are stored in the following directory: **`<windir>\system32\dhcp\DhcpSrvLog-xxx.log`** Where **`<windir>`** is the drive letter and directory path of Windows, such as c:\Windows. ***Note:*** *Do not use the Microsoft DHCP device plug-in to monitor files that can only be accessed over the network, such as a file share.*
Throttle timeout	Type the delay between polling events, in milliseconds, for the Windows DHCP device. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The higher the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 Restart the DHCP service on your Microsoft DHCP Server.

You must restart the DHCP service before the Adaptive Log Exporter can read DHCP server logs.

Step 6 Click **Save**.

Step 7 Repeat this process to create and configure additional Windows DHCP device plug-ins.

You are now ready to map your Microsoft DHCP device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your Windows DHCP device.

A mapping is created for your Windows DHCP device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your Windows DHCP device.

Step 8 Repeat this process to map additional Windows DHCP devices.

The Windows DHCP configuration is complete.

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).

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1. Configure the Adaptive Log Exporter update site. For more information, see **Configuring the Update Site**.
2. Configure a destination for your Trend Micro InterScan VirusWall events. For more information, see **Configuring Destinations**.

If these steps are complete, you are ready to configure your Trend Micro InterScan VirusWall device plug-in and map your device to a destination.

Configuring an Trend Micro Device

The Trend Micro InterScan VirusWall device plug-in allows you to configure the root log directory for system and virus log files, configure polling options, and create a name and IP address to identify your device. After you configure your device, you can map your Trend Micro InterScan VirusWall device to a syslog destination.

To configure a Trend Micro InterScan VirusWall device, you must:

1. Add and configure Trend Micro InterScan VirusWall device plug-in. For more information, see **Configuring the Trend Micro InterScan VirusWall Device Plug-in**.
2. Map the device to a destination. For more information, see **Creating a Device Mapping**.

Configuring the Trend Micro InterScan VirusWall Device Plug-in

To configure your Trend Micro InterScan VirusWall device plug-in:

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

Step 2 Click the **Devices** tab.

Step 3 Select **Trend Micro InterScan VirusWall**, right-click and select **Add Device**.

The device properties for adding new Trend Micro device is displayed.

Step 4 Configure the following parameters:

Table 9-1 Trend Micro InterScan VirusWall Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your Trend Microsoft InterScan VirusWall device.
Root Log Directory	Click **Browse** or type the location of your Trend Micro InterScan VirusWall log files. The Adaptive Log Exporter monitors the log files for changes having a creation date matching the current day of the week. By default, the VirusWall log files are located in the following directory: **<installation folder>\Log directory** **or** **Program Files\InterScan\logs** The **<installation folder>** is the folder in which you installed your InterScan VirusWall device. ***Note:*** *Do not use the Trend Micro InterScan VirusWall device plug-in to monitor files that can only be accessed over the network, such as a file share.*
Throttle timeout	Type a value to indicate the delay between polling for new events, in milliseconds, for the Trend Micro device. The default throttle timeout is 500 milliseconds. The minimum throttle timeout is 10 milliseconds. The higher the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 Click **Save**.

Step 6 Repeat this process to create and configure additional Trend Micro InterScan VirusWall device plug-ins.

You are now ready to map your device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your Trend Micro InterScan VirusWall device.

A mapping is created for your Trend Micro InterScan VirusWall device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your Trend Micro InterScan VirusWall device.

Step 8 Repeat this process to map additional Trend Micro InterScan VirusWall devices.

The Trend Micro InterScan VirusWall configuration is complete.

14 CONFIGURING THE MICROSOFT EXCHANGE SERVER DEVICE

The Microsoft Exchange Server device allows you to forward Outlook Web Access (OWA) or SMTP logs to the Adaptive Log Exporter. The Microsoft Exchange Server device plug-in can read OWA and SMTP event logs to collect the following Outlook events:

- E-mail events
- Calendar events
- Contact events
- Tasks events
- Mobile and web-based access event
- Data storage events

The Adaptive Log Exporter supports the following software versions:

Table 10-1 Microsoft Exchange Format and Method of Configuration

Version	Mail Protocol	Method of Configuration
Microsoft Exchange 2003	Outlook Web Access (OWA)	Adaptive Log Exporter
Microsoft Exchange 2003	SMTP	Adaptive Log Exporter
Microsoft Exchange 2007	OWA	Adaptive Log Exporter Microsoft Exchange Protocol
	SMTP	Microsoft Exchange Protocol
Microsoft Exchange 2010	OWA	Microsoft Exchange Protocol
	SMTP	Microsoft Exchange Protocol

NOTE For more information on the Microsoft Exchange Protocol, see the *Configuring DSMs Guide*.

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1 Configure the Adaptive Log Exporter update site. For more information, see **Configuring the Update Site**.

2 Configure a destination for your Windows Exchange Server events. For more information, see **Configuring Destinations**.

If these steps are complete, you are ready to configure your Windows Exchange Server to create and forward event logs.

This section includes the following topics:

- **Configuring Microsoft Exchange OWA**
- **Forwarding Microsoft Exchange SMTP Logs**

Configuring Microsoft Exchange OWA

The Adaptive Log Exporter reads Outlook Web Access (OWA) logs from the location specified in the Microsoft Internet Information Service (IIS) for your Exchange Server 2003 or Exchange Server 2007. Before you can configure the Adaptive Log Exporter, you must enable logging using Microsoft Internet Information Services (IIS).

NOTE The Adaptive Log Exporter supports OWA logs from Microsoft Exchange 2003 and Microsoft Exchange 2007. For more information on supported versions, see **Table 10-1**.

This section includes the following topics:

- **Enabling Exchange OWA Logs using IIS 6.x**
- **Enabling Exchange OWA Logs using IIS 7.x**
- **Configuring the Microsoft Exchange Server OWA Plug-in**
- **Creating a Device Mapping**

Enabling Exchange OWA Logs using IIS 6.x

Event logs for Microsoft Exchange are logged by Microsoft Internet Information Services (IIS). You must configure and enable event logging in Microsoft IIS before you can configure the Microsoft Exchange device plug-in.

To enable logging using Internet Information Services (IIS):

Step 1 In the IIS 6.0 Manager menu tree, expand **Local Computer**.

Step 2 Expand **websites**.

Step 3 Right-click **Default website** and select **Properties**.

Step 4 On the **website** tab, select the **Enable logging** check box.

Step 5 From the **Active Log Format** list box, select one of the following log formats:

- **NCSA** (Go to**Step 9**)

- **IIS** (Go to**Step 9**)
- **W3C** (Go to**Step 6**)

Step 6 Click **Properties**.

The W3C Properties window is displayed.

Step 7 Click the **Advanced** tab.

Step 8 From the list of properties, select all properties that you want to apply to the Microsoft Exchange Server DSM. You must select the following check boxes:

- **Method (cs-method)**
- **Protocol Version (cs-version)**

Step 9 Click **OK**.

You are now ready to configure the Adaptive Log Exporter plug-in for Microsoft Exchange Server OWA Logs. For more information, see **Configuring the Microsoft Exchange Server OWA Plug-in**.

Enabling Exchange OWA Logs using IIS 7.x

The following steps allow you to configure Microsoft IIS to create logs for your Microsoft Exchange Server. After you complete these steps, you can configure the Adaptive Log Exporter plug-in for Microsoft Exchange.

To enable logging using Internet Information Services (IIS):

Step 1 In the IIS 7.0 Manager menu tree, expand **Local Computer**.

Step 2 On the IIS pane, click **Logging**.

The Logging window is displayed.

Step 3 From the **Format** list box, select one of the following options:

- **NCSA** (Go to**Step 6**)
- **IIS** (Go to**Step 6**)
- **W3C** (Go to**Step 4**)

Step 4 Click **Select Fields**.

The W3C Logging Fields window is displayed.

Step 5 From the list of properties, select all properties that you want to apply to the Microsoft Exchange Server DSM. You must select the following check boxes:

a **Method (cs-method)**

b **Protocol Version (cs-version)**

Step 6 On the Actions pane, click **Apply**.

You are now ready to configure the Adaptive Log Exporter plug-in for Microsoft Exchange Server OWA Logs. For more information, see **Configuring the Microsoft Exchange Server OWA Plug-in**.

Configuring the Microsoft Exchange Server OWA Plug-in

To configure your Microsoft Exchange Server OWA device in the Adaptive Log Exporter:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **Microsoft Exchange Server OWA Logs** and select **Add Device**.

The device properties for adding a new Microsoft Exchange Server are displayed.

Step 4 Configure the following parameters:

Table 10-2 Microsoft Exchange Server OWA Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your Microsoft Exchange Server.
Root Log Directory	Click **Browse** or type the directory location for your Microsoft Exchange log files. The Microsoft Exchange Server OWA Log plug-in monitors recently created files in the root log directory that match the following format: • Files starting with **`(u_)ex`**, **`(u_)nc`**, or **`(u_)in`** • Files ending with **`.log`** The following directory location is the default directory for storing Windows IIS audit log files: **`<windir>\System32\Log Files\W3SVC1`** Where **`<windir>`** is the drive letter and directory path of Windows, such as c:\Windows. ***Note:*** *Do not use the Microsoft Exchange Server OWA Log device plug-in to monitor files that can only be accessed over the network, such as a file share.*
Throttle timeout	Type the delay between polling events, in milliseconds, for the Windows Event Log device. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The higher the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 Click **Save**.

Step 6 Repeat this process to create and configure additional Microsoft Exchange Service device plug-ins.

You are now ready to map your Microsoft Exchange Service OWA Log device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your Microsoft Exchange OWA device.

A mapping is created for your Microsoft Exchange OWA device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your Microsoft Exchange OWA device.

Step 8 Repeat this process to map additional Microsoft Exchange OWA devices.

The Microsoft Exchange OWA device configuration is complete.

Forwarding Microsoft Exchange SMTP Logs

The Adaptive Log Exporter reads SMTP logs from the location specified in the Microsoft Internet Information Service (IIS) for your Exchange Server 2003. Before you can configure the Adaptive Log Exporter, you must enable logging using Microsoft Internet Information Services (IIS).

NOTE The Adaptive Log Exporter supports SMTP logs only from Microsoft Exchange 2003 Servers. For more information on supported versions, see **Table 10-1**.

This section includes the following topics:

- **Enabling Microsoft Exchange 2003 SMTP Logs**
- **Configuring the Microsoft Exchange Server SMTP Plug-in**
- **Creating a Device Mapping**

Enabling Microsoft Exchange 2003 SMTP Logs

To enable logs using Internet Information Services (IIS) for Microsoft Exchange:

Step 1 In the Exchange System Manager menu tree, expand **Servers > Protocols > SMTP**.

Step 2 Right-click **Default SMTP Virtual Server** and select **Properties**.

The Default SMTP Virtual Server Properties window is displayed.

Step 3 On the **General** tab, select the **Enable logging** check box.

Step 4 From the **Active Log Format** list box, select one of the following options:

- **NCSA** (Go to**Step 8**)
- **IIS** (Go to**Step 8**)
- **W3C** (Go to**Step 5**)

Step 5 Click **Properties**.

The W3C Properties window is displayed.

Step 6 Click the **Advanced** tab.

Step 7 From the list of properties, select all properties that you want to apply to the Microsoft Exchange Server SMTP log. You must select the following check boxes:

- **Method (cs-method)**
- **Protocol Version (cs-version)**

Step 8 Click **OK**.

You are now ready to configure the Adaptive Log Exporter plug-in for Microsoft Exchange Server SMTP Logs. For more information, see **Configuring the Microsoft Exchange Server SMTP Plug-in**.

Configuring the Microsoft Exchange Server SMTP Plug-in

Before you can add a Windows Event Log device, you must create a destination for the syslog events. For more information on creating a destination, see **Configuring Destinations**.

To configure your Microsoft Event Log device in the Adaptive Log Exporter:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **Microsoft Exchange Server SMTP Logs** and select **Add Device**.

The device properties for adding new a Microsoft Exchange Server with SMTP Logs is displayed.

Step 4 Configure the following parameters:

Table 10-3 Microsoft Exchange Server SMTP Logs Plug-in Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your Microsoft Exchange Server.
Root Log Directory	Click **Browse** or type the directory location for your Microsoft Exchange log files. The Microsoft Exchange Server SMTP Log plug-in monitors recently created files in the root log directory that match the following format: • Files starting with **`(u_)ex`**, **`(u_)nc,`** or **`(u_)in`** • Files ending with **`.log`** The following directory location is the default directory for storing Windows IIS audit log files: **`<windir>\System32\Log Files\SMTPSVC1\`** Where **`<windir>`** is the drive letter and directory path of Windows, such as c:\Windows. ***Note:*** *Do not use the Microsoft Exchange Server SMTP Log device plug-in to monitor files that can only be accessed over the network, such as a file share.*
Throttle timeout	Type the delay between polling events, in milliseconds, for the Windows Event Log device. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The higher the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 On the Adaptive Log Exporter toolbar, click **Save**.

You are now ready to map your Microsoft Exchange Service SMTP Log device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your Microsoft Exchange OWA device.

A mapping is created for your Microsoft Exchange OWA device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your Microsoft Exchange OWA device.

Step 8 Repeat this process to map additional Microsoft Exchange OWA devices.

The Microsoft Exchange OWA device configuration is complete.

15 CONFIGURING THE MICROSOFT SQL SERVER DEVICE

Microsoft SQL Server plug-in reads and forwards Microsoft SQL events from the error log file. 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. This plug-in supports Microsoft SQL Server 2000, 2005, and 2008.

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, ERRORLOG.1 being the most recent backup of the error log and ERRORLOG.2 being the second most recent.

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1. Configure the Adaptive Log Exporter update site. For more information, see **Configuring the Update Site**.
2. Configure a destination for your Microsoft SQL Server events. For more information, see **Configuring Destinations**.

If these steps are complete, you are ready to configure your Microsoft SQL Server device plug-in and map your device to a destination.

Configuring a Microsoft SQL Server Device

The Microsoft SQL Server device plug-in allows you to configure the root log directory for your ERRORLOG files, configure polling options, and create a name and IP address to identify your device. After you configure your device, you can map your Microsoft SQL Server to a syslog destination.

To configure a Microsoft SQL Server device, you must:

1 Add and configure a Microsoft SQL Server device plug-in. For more information, see **Configuring the Microsoft SQL Device Plug-in**.

2 Map the device to a destination. For more information, see **Creating a Device Mapping**.

Configuring the Microsoft SQL Device Plug-in

To configure your Microsoft SQL Server device plug-in:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **Microsoft SQL** and select **Add Device**.

The device properties for adding a new Microsoft SQL Server are displayed.

Step 4 Configure the following parameters:

Table 11-1 Microsoft SQL Server Plug-in Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your DHCP Server.
Root Log Directory	Click **Browse** or type the directory location for your Microsoft SQL Server log files. The following directory location is the default directory for storing Microsoft SQL Server log files: **`C:\Program Files\Microsoft SQL Server\MSSQL\LOG\`** Where **`<windir>`** is the drive letter and directory path of Windows, such as c:\Windows. ***Note:*** *Do not use the Microsoft SQL Server device plug-in to monitor files that can only be accessed over the network, such as a file share.*
Log Filename	Type the name of the log file to be monitored by QRadar SIEM. By default, the log file name is ERRORLOG. If this field is left blank, then the filename defaults to ERRORLOG.

Table 11-1 Microsoft SQL Server Plug-in Parameters (continued)

Parameter	Description
Throttle timeout	Type the delay between polling events, in milliseconds, for the Windows Event Log device. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The higher the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 Click **Save**.

Step 6 Repeat this process to create and configure additional Microsoft SQL Server device plug-ins.

You are now ready to map your Microsoft SQL Server device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your Microsoft SQL Server device.

A mapping is created for your Microsoft SQL Server device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your Microsoft SQL Server device.

Step 8 Repeat this process to map additional Microsoft SQL Server devices.

The Microsoft SQL Server configuration is complete.

16 Configuring the Microsoft IIS Device

Microsoft Internet Information Services (IIS) includes a broad range of administrative features for managing websites. You can monitor attempts to access your websites, 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 from your entire website directory or record events for an individual website, virtual folder, or file. For more information regarding your Microsoft IIS device, see your vendor documentation.

The Microsoft IIS device plug-in can read and forward events for the following logs:

- Website Logs (W3C)
- File Transfer Protocol (FTP) Logs
- Simple Mail Transfer Protocol (SMTP) Logs
- Network News Transfer Protocol (NNTP) Logs

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.

CAUTION *The Adaptive Log Exporter can monitor up to 25 Microsoft IIS websites.*

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1. Configure the Adaptive Log Exporter update site. For more information, see **Configuring the Update Site**.
2. Configure a destination for your Microsoft IIS Server events. For more information, see **Configuring Destinations**.

If these steps are complete, you are ready to configure your Microsoft IIS device plug-in and map your device to a destination.

Configuring a Microsoft IIS Server Device

The Microsoft IIS Server device plug-in allows you to configure the root log directory for your log files to monitor up to 25 websites. The Microsoft IIS Server device plug-in monitors the root log directory and any folders under the root log directory that contain log files for IIS. After you configure your device, you can map your Microsoft IIS Server device to a syslog destination.

NOTE If you are using the Adaptive Log Exporter to monitor several individual websites instead of the top-level website directory, we recommend you create several Microsoft IIS device plug-ins to monitor these individual websites.

If you use customized directories for your log files, the sub-folders under your root log directory must contain the name of the logs stored in the folder. **Figure 12-1** displays a custom directory structure and the file names required for reading FTP logs, Usenet logs (NNTP), e-mail logs (SMTP), and website logs (W3C).

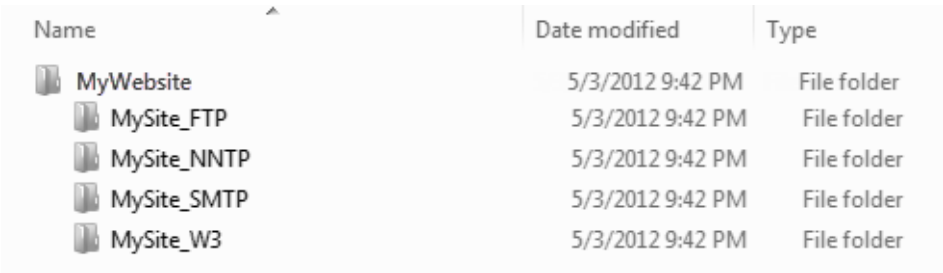

Figure 12-1 Customized Directories Structure for Microsoft IIS Websites

To configure a Microsoft IIS device:

1. Add and configure a Microsoft IIS device plug-in. For more information, see **Configuring the Microsoft IIS Server Device Plug-in**.
2. Map the device to a destination. For more information, see **Creating a Device Mapping**.

Configuring the Microsoft IIS Server Device Plug-in

To configure a Microsoft IIS device plug-in:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **Microsoft IIS** and select **Add Device**.

The device properties for adding a new Microsoft IIS device are displayed.

Step 4 Configure the following parameters:

Table 12-1 Microsoft IIS Parameters

Parameter	Description
Name	Type the name you want to assign this device. This name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your Microsoft IIS Server. ***Note:*** *If you configure the Adaptive Log Exporter to monitor several individual websites, you must type the IP address or hostname for the website.*
Root Log Directory	Click **Browse** or type the directory location for your Microsoft IIS log files. The Microsoft IIS plug-in monitors recently created files and sub-folders under the root log directory that match the following format: • Files starting with **`(u_)ex`**, **`(u_)nc`**, or **`(u_)in`** • Files ending with **`.log`** Windows IIS log files are stored in the following default directory: **`<windir>\System32\LogFiles\`** Where **`<windir>`** is the drive letter and directory path of Windows, such as c:\Windows. ***Note:*** *Do not use the Microsoft IIS Server device plug-in to monitor files that can only be accessed over the network, such as a file share.*
Web Logs	Select this check box to monitor the event log files for IIS website events. By default, the **Web Logs** check box is selected.
FTP Logs	Select this check box to monitor the event log files for IIS FTP site events. By default, the **FTP Logs** check box is selected.
IIS SMTP Logs	Select this check box to monitor the event log files for Simple Mail Transfer Protocol (SMTP) events.
NNTP Logs	Select this check box to monitor the event log files for Network News Transfer Protocol (NNTP) events.

Table 12-1 Microsoft IIS Parameters (continued)

Parameter	Description
Throttle timeout	Type the delay between polling events, in milliseconds, for the Windows Event Log device. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The larger the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The smaller the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 Click **Save**.

Step 6 Repeat this process to create and configure additional Microsoft IIS device plug-ins.

You are now ready to map your Microsoft IIS Server device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your Microsoft IIS device.

A mapping is created for your Microsoft IIS device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your Microsoft IIS device.

Step 8 Repeat this process to map additional Microsoft IIS devices.

The Microsoft IIS configuration is complete.

17 CONFIGURING THE MICROSOFT WINDOWS IAS DEVICE

The Microsoft Windows Internet Authentication Service (IAS) devices forward Remote Authentication Dial-in User Service (RADIUS) server events and proxy server events to QRadar SIEM. 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 log file formats for Microsoft Windows IAS and Microsoft Windows Network Policy Server (NPS). The Microsoft Windows IAS device supports NPS through IAS-formatted and database-compatible log files.

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1. Configure the Adaptive Log Exporter update site. For more information, see **Configuring the Update Site**.
2. Configure a destination for your Microsoft IAS Server events. For more information, see **Configuring Destinations**.

If these steps are complete, you are ready to configure your Microsoft IAS device plug-in and map your device to a destination.

Configuring a Microsoft IAS Device

The Windows IAS device plug-in allows you to configure the root log directory for your .log or .isa log files, configure polling options, and create a name and IP address to identify your device. After you configure your device, you can map your Windows IAS device to a syslog destination.

To configure a Microsoft Windows IAS device, you must:

1. Add and configure a Microsoft IAS device plug-in. For more information, see **Configuring the Windows IAS Device Plug-in**.
2. Map the device to a destination. For more information, see **Creating a Device Mapping**.

Configuring the Windows IAS Device Plug-in

To configure your Microsoft IAS device plug-in:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **Microsoft IAS** and select **Add Device**.

The device properties for adding a new Microsoft IAS device are displayed.

Step 4 Configure the following parameters:

Table 13-1 Microsoft IAS Plug-in Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your Microsoft IAS Server.
Root Log Directory	Click **Browse** or type the location of the server log files. QRadar SIEM monitors recently created files in the Root Log Directory that start with in or ias and end in .log. By default, IAS and NPS log files are located in the following directory: **`<windir>\System32\LogFiles`** Where **`<windir>`** is the drive letter and directory path of Windows, such as c:\Windows. ***Note:*** *Do not use the Microsoft IAS device plug-in to monitor files that can only be accessed over the network, such as a file share.*
Throttle timeout	Type the delay between polling events, in milliseconds, for the Microsoft IAS Server logs. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The larger the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 Click **Save**.

Step 6 Repeat this process to create and configure additional Windows IAS device plug-ins.

You are now ready to map your Microsoft IAS Server device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your Windows IAS device.

A mapping is created for your Windows IAS device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your Windows IAS device.

Step 8 Repeat this process to map additional Windows IAS devices.

The Windows IAS configuration is complete.

18 CONFIGURING THE MICROSOFT ISA DEVICE

The Microsoft Internet Security and Acceleration (ISA) Server provides you with network proxy and firewall service logs for Microsoft ISA and Microsoft Forefront Threat Management Gateway (TMG) 2010. The Windows ISA device plug-in for the Adaptive Log Exporters allows you to forward .w3c or .isa formatted log files.

CAUTION

Windows ISA Server files can contain payloads larger than 1024 bytes, which is the maximum payload size for the UDP protocol. We recommend that you configure a TCP syslog destination for Windows ISA device plug-ins reporting events for Windows ISA Servers.

Before you can configure any device plug-in for the Adaptive Log Exporter, you must complete the following steps from previous chapters:

1. Configure the Adaptive Log Exporter update site. For more information, see **Configuring the Update Site**.
2. Configure a destination for your Windows ISA events. For more information, see **Configuring Destinations**.

If these steps are complete, you are ready to configure your Windows ISA device plug-in and map your device to a destination.

Configuring Windows ISA

The Windows ISA device plug-in allows you to configure the root log directory for your .w3c or .isa log files, configure polling options, and create a name and IP address to identify your device. After you configure your device, you can map your Windows ISA device to a syslog destination.

To configure a Microsoft Windows ISA or Threat Management Gateway 2010 device:

1 Add and configure a Windows ISA device plug-in. For more information, see **Configuring Windows ISA**.

2 Map the device to a destination. For more information, see **Creating a Device Mapping**.

Configuring the Windows ISA Device Plug-in

To configure your Windows ISA device plug-in:

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

Step 2 Click the **Devices** tab.

Step 3 Right-click on **Microsoft ISA** and select **Add Device**.

The device properties for adding new a Microsoft ISA device are displayed.

Step 4 Configure the following parameters:

Table 14-1 Microsoft ISA Plug-in Parameters

Parameter	Description
Name	Type the name you want to assign this device. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Device Address	Type the IP address or hostname for your local or remote Windows host.

Table 14-1 Microsoft ISA Plug-in Parameters (continued)

Parameter	Description
Root Log Directory	Click **Browse** or type the location of the Microsoft ISA Server log files. QRadar SIEM monitors recently created files in the Root Log Directory ending with .w3c or .iis. By default, the ISA log files are located in the following directories: • For Microsoft ISA 2004: **<Program Files>\MicrosoftISAServer\ISALogs** Where **<Program Files>** is the drive letter and directory path of your Program Files directory, such as c:\Program Files. • For Microsoft ISA 2006: **<windir>\System32\LogFiles** Where **<windir>** is the drive letter and directory path of Windows, such as c:\Windows or d:\Windows. • For Microsoft Forefront Threat Management Gateway: **<Program Files>\<Forefront Directory>\Logs** Where: **<Program Files>** is the drive letter and directory path of your Program Files directory, such as c:\Program Files. **<Forefront Directory>** is the installation directory for your Microsoft Forefront Threat Management Gateway. ***Note:*** *Do not use the Windows ISA device plug-in to monitor files that can only be accessed over the network, such as a file share.*
Throttle timeout	Type the delay between polling events, in milliseconds, for the Microsoft ISA logs. The default throttle timeout is 500 milliseconds. The minimum value is 10 milliseconds. The larger the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs less often. The lower the value specified in the throttle timeout means that the Adaptive Log Exporter checks for updated device logs more often.

Step 5 Click **Save**.

Step 6 Repeat this process to create and configure additional Windows ISA device plug-ins.

You are now ready to map your Microsoft ISA device to a syslog destination.

Creating a Device Mapping

After you have configured your device, you must map your device to a destination.

To map a device to a destination:

Step 1 Click the **Destinations** tab.

Step 2 Click **+** to expand the available destinations.

If no **+** exists, you need to create a destination. For more information, see **Configuring Destinations**.

Step 3 Right-click on a destination and select **Add Device Mapping**.

Step 4 A list of configured devices is displayed.

Step 5 Select your Windows ISA device.

A mapping is created for your Windows ISA device to the destination.

Step 6 Click **Save**.

Step 7 Click **Deploy**.

After the deploy process completes your events are forwarded from the Adaptive Log Exporter to QRadar SIEM. These events are automatically discovered and added as a log source using the name and IP address of your Windows ISA device.

Step 8 Repeat this process to map additional Windows ISA devices.

The Windows ISA configuration is complete.

A ADAPTIVE LOG EXPORTER TROUBLESHOOTING

This section provides troubleshooting information to assist you in resolving issues with your Adaptive Log Exporter.

This section includes the following topics:

Troubleshooting Files

When you contact Customer Support for assistance, you may be requested to copy, compress, and send the following dirctories:

- C:\Program Files\Adaptive Log Exporter\config*.*
- C:\Program Files\Adaptive Log Exporter\logs*.*

On 64-bit operating systems, the folders are located at the following paths:

- C:\Program Files(x86)\Adaptive Log Exporter\config*.*
- C:\Program Files(x86)\Adaptive Log Exporter\logs*.*

The following table describes the log files you can use to troubleshoot your Adaptive Log Exporter issues:

Table A-1 Useful Log Files

Log File	Description
ALE_Code.log	Logs device mapping errors and plug-in launch threads.
ALE_Device.log	Logs connection and formatting messages.
ALE_System.log	Logs system level start messages.
ALE_Events.log	Logs events generated by the Adaptive Log Exporter when you have enabled a logger destination. For more information, see **Verifying Devices are Creating Events**.

Enabling Debug Mode

The Adaptive Log Exporter can be configured in debug mode for logging additional troubleshooting messages. Debug mode for the Adaptive Log Exporter is a feature specifically defined for advanced troubleshooting for customer support.

CAUTION

Debug mode should only be enabled for troubleshooting when requested by customer support. Enabling debug mode on the Adaptive Log exporter consumes additional resources, such as increased CPU usage and increased disk storage due to the number of logs and events being processed. Enabling debug mode can lead to significant performance issues on the host system. For more information, see **Contacting Customer Support**.

This section includes the following topics:

- **Enabling Debug Mode**
- **Restarting the Adaptive Log Exporter Service**

Enabling Debug Mode

To enable debug mode:

Step 1 Navigate to the following directory on the Adaptive Log Exporter host:

```
C:\Program Files\Adaptive Log Exporter\Config\
```

On 64-bit operating systems, this file location can be the following:

```
C:\Program Files (x86)\Adaptive Log Exporter\Config\
```

Step 2 Open the following file:

```
logconfig.txt
```

Step 3 Edit the root category priority from info to debug:

```
log4j.rootCategory=DEBUG, ApndrConsole
```

Step 4 Edit the code logs priority from info to debug:

```
# The Code logs.
log4j.category.Code=DEBUG, ApndrCode, ApndrConsole
```

Step 5 Edit the device logs priority from info to debug:

```
# The Device logs.
log4j.category.Device=DEBUG, ApndrDevice, ApndrConsole
```

Step 6 Edit the system logs priority from info to debug:

Step 7
```
# The System logs.
log4j.category.System=DEBUG, ApndrSystem, ApndrConsole
```

Step 8 Save the file.

You are now ready to restart the Adaptive Log Exporter Server.

Restarting the Adaptive Log Exporter Service

To enable any changes made to the log configuration, you must restart the Adaptive Log Exporter Service.

Step 1 On your desktop, select **Start > Run**.

The Run window is displayed.

Step 2 Type the following:

```
services.msc
```

Step 3 Click **OK**.

The Services window is displayed.

Step 4 Right-click on the **AdaptiveLogExporterService** and select **Restart**.

After the service restarts, the Adaptive Log Exporter is configured for debug mode. When you are done debugging your Adaptive Log Exporter installation, we recommend you disable debug mode by changing the log values back to debug.

Update Site Unreachable

If you click **Add Plugins** on the toolbar and receive an error indicating that the Adaptive Log Exporter site is unavailable or unreachable, you must correct the location of the update site in the Adaptive Log Exporter preferences. This issue often occurs when the default site has not been updated after the initial installation.

To configure an update site:

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

The Adaptive Log Exporter is displayed.

Step 2 On the main menu, select **File > Preferences**.

The Preferences window is displayed.

Step 3 Click the **+** icon to expand the Install/Update navigation tree.

Step 4 On the navigation menu, select **Update Site**.

Update Site parameters are displayed.

Step 5 In the **Update Site URL** field, type the location of your update site file.

For example,

- To update from a Windows share, type the path to your server:

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

- To update from a local file, type the path to the file:

  `file:///e:/UpdateSite`

NOTE

If you choose a Windows server or local file, you must download the ALEUpdateSite.zip file from the support website and extract the file to a Windows share or file repository. The update site file is located at the following address: *http://www.ibm.com/support/fixcentral/*. For more information, see **Configuring Updates for Off-line Sites**.

Step 6 Click **Apply**.

Step 7 Click **OK**.

Step 8 On the toolbar, click **Add Plugins**.

A status bar is displays the download status when retrieving updates. If you receive the message **No features found on the selected sites(s)**, then no updates are available.

Verifying Devices are Creating Events

If you have completed your device plug-in configuration and QRadar SIEM is not receiving the expected events, you can confirm that events are being created at the event source. We recommend you log the events to a file on the local disk by creating a logger destination for the Adaptive Log Exporter. A logger destination allows you to write a log file for your device to the logs folder in your Adaptive Log Exporter directory, allowing you to verify that events are created.

This section includes the following topics:

- **Creating a Logger Destination**
- **Deleting a Logger Destination**

CAUTION

Logging events to a file on the local disk consume large amounts of disk space very quickly. On high event per second hosts, we highly recommend that you

disable your logger destination after verifying that events are created. No method exists for cleaning up a log file after enabling an event logger for a device.

Creating a Logger Destination

To create a logger destination for your device:

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

The Adaptive Log Exporter is displayed.

Step 2 Click the **Destinations** tab.

Step 3 Right-click on **Logger** and select **Add Destination**.

Step 4 Configure the following values:

Table A-2 Adding a Destination

Parameter	Description
Name	Type the name you want to assign this destination. The name can include up to 50 alphanumeric characters, underscores (_), hyphens (-), and periods (.).
Description	Type a description for this device. The description can include up to 100 characters.
Logger Prefix	Type the heading you want to assign to the logs. The Logger Prefix must start with **Device.Events** and may contain letters, numbers and periods. For example, Device.Events.troubleshooting.
Prepend syslog header	Select this check box if you want the syslog header to be attached to the message in the logs.
Number of Threads	Type the number of concurrent processing threads you want run in this destination. The default is 1.

Step 5 Click **Save**.

The logger you created is saved and displayed on the **Destinations** tab.

Step 6 Right-click the logger you created and select **Add Device Mapping**.

Step 7 From the device menu, select the device you want to troubleshoot.

Step 8 Click **Deploy**.

The Adaptive Log Exporter should be logging device events to a file.

Step 9 Navigate to the following directory:

```
C:\Program Files\Adaptive Log Exporter\Logs
```

On 64-bit operating systems, this file location can be the following:

```
C:\Program Files (x86)\Adaptive Log Exporter\Logs
```

Step 10 Open the ALE_Events.log file to verify that events are created for your device.

Step 11 If events are created, we recommend that you delete the logger you created for troubleshooting.

Deleting a Logger Destination

After you have verified the Adaptive Log Exporter is writing events to a log file, we recommend you delete the logger destination.

To Delete your logger destination:

Step 1 Click the **Destinations** tab.

Step 2 Click the **+** to expand the logger destination list.

Step 3 Right-click on your troubleshooting logger and select **Delete Destination**.

Step 4 Click **Save**.

Step 5 Click **Deploy**.

After the deploy process completes, the logger stops logging events to the ALE_Events.log file.

Verifying QRadar SIEM is Receiving Events

After you have verified that the Adaptive Log Exporter is logging events for your device to a log file, you can then verify that your QRadar SIEM Console or Event Collector is receiving the syslog events. You can use the tcpdump packet analyzer through the Command Line Interface (CLI) to look for the IP address of your Adaptive Log Exporter device. This process determines if there is a network issue between the Adaptive Log Exporter and QRadar SIEM.

To verify QRadar SIEM is receiving Adaptive Log Exporter events:

Step 1 Using SSH, log in to QRadar SIEM as the root user.

Username: **`root`**

Password: **`<password>`**

Step 2 Type the following command:

```
tcpdump -nnAs0 -ieth0 'host <Device Address> and port 514'
```

Where **`<Device Address>`** is the Device Address on the **Devices** tab for your device in the Adaptive Log Exporter. If you installed the Adaptive Log Exporter using the command line, type the IP address or hostname from the **`/DeviceAddress=`** field.

For example,

```
tcpdump -nnAs0 -ieth0 'host 10.100.125.101 and port 514'
```

NOTE If the QRadar SIEM Console or Event Collector uses a different network interface, you must adjust the -i interface command.

Step 3 The output can resemble the following:

```
<13>Apr 03 20:20:41 10.100.125.101 AgentDevice=WindowsLog AgentLogFile=Security
PluginVersion=1.0.14 Source=Microsoft-Windows-Security-Auditing
```

```
Computer=TestWin7.IBM.COM User=   Domain=   EventID=5156  EventIDCode=5156
EventType=8  EventCategory=12810  RecordNumber=5981346  TimeGenerated=1333495239
TimeWritten=1333495239  Message=The Windows Filtering Platform has permitted a
connection. Application Information:  Process ID:928  Application Name:
\device\harddiskvolume2\windows\system32\svchost.exe  Network Information:
Direction:  Outbound  Source Address:192.168.125.101  Source Port:64307  Destination
Address:192.168.125.5  Destination Port:53  Protocol:17  Filter Information:  Filter
Run-Time ID:66565  Layer Name:Connect
```

Step 4 If no Windows or device plug-in events are displayed, contact your network administrator to verify that your Adaptive Log Export can communicate with your QRadar SIEM Console or Event Collector.

Configuring Adaptive Log Exporter Service Credentials

When using the Windows Event Log plug-in or NetApp Data ONTAP to retrieve events from remote machines, issues can occur with user credentials. The Adaptive Log Exporter polls for new events using a registry call to the remote Windows operating system. The registry for new events is read from the remote Windows host. The Adaptive Log Exporter uses NetBIOS to call dynamic-link library (DLL) files, which process the remote event logs. The Adaptive Log Exporter must be able to remotely access the C$ share, also known as the Administrative share on the remote machine.

If the Adaptive Log Exporter service does not have the proper permission level, the ALE_Device.log file can display the following error:

```
C:\Program Files\Adaptive Log Exporter\logs\ALE_Device.log:
2010-12-02 11:18:15,000 WARN
Device.WindowsLog.MessageFormatterBase.GetRawMessageFromFiles:
Could not load requested file
'\\Test\C$\WINDOWS\System32\MsAuditE.dll', Reason = 5
```

The error indicates that the Adaptive Log Exporter could not read a remote DLL file named MsAuditE.dll. You must configure the Adaptive Log Exporter service with the correct credentials to access the Windows host remotely. The permission level typically required is Domain Administrator.

To configure credentials for the Adaptive Log Exporter service:

Step 1 On your desktop, select **Start > Run**.

The Run window is displayed.

Step 2 Type the following:

```
services.msc
```

Step 3 Click **OK**.

The Services window is displayed.

Step 4 Right-click on the **AdaptiveLogExporterService** and select **Properties**.

Step 5 Click the **Log On** tab.

Step 6 Configure the following parameters:

Table A-3 Adaptive Log Exporter Credentials

Parameter	Description
This Account	Select this option, and then type or click **Browse** to assign a user account with Domain Administration credentials to the Adaptive Log Exporter service.
Password	Type the password for the user account.
Confirm password	Type the password again to confirm the password for the user account.

Step 7 Click **Apply**.

Step 8 Click **OK**.

The Services window is displayed.

Step 9 Right-click on **AdaptiveLogExporterService** and select **Restart**.

The Adaptive Log Exporter service is restarted.

After the Adaptive Log Exporter service has restarted, the configuration for remote Windows Event Log collection is complete.

Troubleshooting Common Error and Warning Messages

This section provides information on warning and error messages to assist you with finding resolving for common Adaptive Log Exporter issues.

Example: Remote Permissions

The following error message can indicate an additional error message when the Adaptive Log Exporter service does not have sufficient administrative privileges or when a DLL file is missing that is required to decode a specific portion of an event payload:

```
2011-02-07 13:42:12,000 WARN
Device.WindowsLog.MessageFormatterBase.GetRawMessageFromFiles :
Could not load requested file
'\\Test\C$\Windows\system32\adtschema.dll', Reason = 5
```

NOTE This error message only applies to the Windows Event Log plug-in when collecting events from remote hosts using the **Remote Machine** check box.

Warning messages for the following DLL files can indicate a credentials issue with the Adaptive Log Exporter service when attempting to read events from a Windows host remotely:

- adtschema.dll
- ws03res.dll
- xpsp2res.dll

- MsAuditE.dll

We recommend you examine the permissions provided to the Adaptive Log Exporter service. For more information, see **Configuring Adaptive Log Exporter Service Credentials**.

You can verify that the credentials for the Adaptive Log Exporter service are correct by opening a Remote Desktop session with the problematic Windows host. Attempting to log in remotely with the username and password for the Adaptive Log Exporter service can identify if the error is credential related. If the connection fails, the remote host you are attempting to connect to might not allow remote login attempts. Contact your network administrator to verify the configuration of the remote Windows host.

Example: Event Per Second Overload

When the event per second (EPS) rate of the host is greater than the Adaptive Log Exporter can process, events can be dropped. The following error message indicates that the Adaptive Log Exporter is unable to process events at the same rate that events are generated.

```
2010-12-13 12:02:33,000 WARN
Device.WindowsLog.EventLog.local.Security.Read : Reopening
event log due to falling too far behind (approx 205509 logs
dropped).
```

NOTE If your Adaptive Log Exporter is dropping events, we recommend you contact Customer Support to determine if your configuration can be optimized.

Example: Unexpected Value in Payload

The Adaptive Log Exporter reads Windows-based event data using the Windows Event Log device plug-in and assembles event messages as name value pairs. If an unexpected value is included in the Windows Event Log payload that the Adaptive Log Exporter cannot process, the following error message is generated:

```
2010-12-08 13:45:26,000 ERROR
Device.WindowsLog.MessageFormatterBase.GetRawMessageFromFiles :
FormatMessage failed with error code of 317
```

The Adaptive Log Exporter does not discard events with unexpected name value pairs. The events messages are forwarded to QRadar SIEM and parsed as an unknown or generic Windows event.

Enabling the Print Spooler

The print spooler service is required on each system hosting the Adaptive Log Exporter.

To enable the print spooler for the Adaptive Log Exporter service:

Step 1 On the desktop of the Windows host, select **Start > Run**.

The Run window is displayed.

Step 2 Type the following:

```
services.msc
```

Step 3 Click **OK**.

The Services window is displayed.

Step 4 Right-click on the **Print Spooler** service and select **Properties**.

Step 5 From the **Startup Type** list-box, select **Automatic**.

Step 6 Click **OK**.

Step 7 Right-click on the **Print Spooler** service and select **Restart**.

The Print Spooler service restarts.

Launching the Adaptive Log Exported in Windows 2008R2

After installing the Adaptive Log Exporter on Windows 2008R2 operating systems, the following message can be displayed when attempting to launch the Adaptive Log Exporter interface:

```
/org/eclipse/update/search/IUpdateSearchFilter
```

The error above indicates there is a compatibility issue occurring with the Adaptive Log Exporter and your installation of Windows 2008R2. We recommend you run the Adaptive Log Exporter in compatibility mode for Windows XP.

To configure compatibility mode for the Adaptive Log Exporter:

Step 1 On the desktop of the Windows host, select **Start > Adaptive Log Exporter**.

Step 2 Right-click on **Configure Adaptive Log Exporter** and select **Properties**.

Step 3 Click the **Compatibility** tab.

Step 4 From the Compatibility Mode pane, select the **Run this program in compatibility mode for** check box.

Step 5 From the list box, select **Windows XP (Service Pack 3)**.

Step 6 Click **Apply**.

Step 7 Click **OK**.

Step 8 On the desktop of the Windows host, select **Start > Adaptive Log Exporter > Configure Adaptive Log Exporter**.

The Adaptive Log Exporter interface is displayed. If the error persists, we recommend you contact Customer Support. For more information, see **Contacting Customer Support**.

B Updating Remote Windows Event Log Devices Using the CLI

The Adaptive Log Exporter can be installed remotely to a Windows host without the user interface with the command line installation parameters. This installation method is typical when the Adaptive Log Exporter is installed across a network. Without an interface, system administrators require a method for patching or updating the parameters of the Windows Event Log device plug-in. The ALE_WindowsEventLogPlugin_setup.exe is a file that can be used in the Command Line Interface (CLI) to perform the following tasks:

- **Patching** - The ALE_WindowsEventLogPlugin_setup file can run on the Windows host to patch the Windows Event Log device plug-in without changing the configured parameters. Patches typically corrects known issues or update event parsing and categorization for Windows events. For more information see **Patching the Windows Event Log Device**.
- **Updating** - The ALE_WindowsEventLogPlugin_setup can run on the Windows host to update the configuration parameters of local Windows Event Log device plug-in. The command line allows you to update event configuration parameters, such as the destination IP address, the name of the host forwarding events, or the transmission protocol. For more information, see **Updating a Windows Event Log Configuration**.

NOTE For examples of updating your Windows Event Log device configuration, see **Updating Examples**.

Patching the Windows Event Log Device

To patch the Windows Event Log device plug-in on the Adaptive Log Exporter:

Step 1 Download the ALE_WindowsEventLogPlugin_setup file from the IBM Fix Central website.

https://www.ibm.com/support/fixcentral/

Step 2 Copy the ALE_WindowsEventLogPlugin_setup.exe file to the system hosting the Adaptive Log Exporter.

Step 3 From the desktop of the remote Windows host, select **Start > Run**.

The Run window is displayed.

Step 4 Type the following command:

```
cmd
```

Step 5 Click **OK**.

The Command Line Interface (CLI) is displayed.

Step 6 Navigate to the directory containing the ALE_WindowsEventLogPlugin_setup.exe file.

Step 7 Type the following command to patch your Windows Event Log device plug-in:

```
ALE_WindowsEventLogPlugin_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES /PATCHONLY
```

Table B-4 Patching Command Line Parameters

Parameter	Description
`/SP-`	Allows the initial installation setup message to be suppressed.
`/VERYSILENT`	Allows the installation to run in the background.
`/SUPPRESSMSGBOXES`	Allows setup message to be suppressed during the installation.
`/PATCHONLY`	Allows you to update your Windows Event Log and apply the latest fixes without modifying any existing device plug-in configurations. This command should only be used with the /SP-, /VERYSILENT, and /SUPPRESSMSGBOXES options.

NOTE The Adaptive Log Exporter CLI installation instructions include an example of using a batch script to install the Adaptive Log Exporter. The batch script example includes the **/PATCHONLY** command, which installs the Adaptive Log Exporter. and patches the Windows Event Log device plug-in simultaneously. For more information, see **Batch File Command Line Install Script**.

Updating a Windows Event Log Configuration

You can use the ALE_WindowsEventLogPlugin_setup to update the configuration parameters of a Windows Event Log device plug-in.

To update a Windows Event Log configuration using the CLI:

Step 1 Download the ALE_WindowsEventLogPlugin_setup file from the IBM Fix Central website.

https://www.ibm.com/support/fixcentral/

Step 2 Copy the ALE_WindowsEventLogPlugin_setup.exe file to the system hosting the Adaptive Log Exporter.

Step 3 From the desktop of the Windows host, select **Start > Run**.

The Run window is displayed.

Step 4 Type the following command:

```
cmd
```

Step 5 Click **OK**.

The Command Line Interface (CLI) is displayed.

Step 6 Navigate to the directory containing the ALE_WindowsEventLogPlugin_setup.exe file.

Step 7 Update the parameters for your Windows Event Log device plug-in:

Table B-5 Updating Windows Event Log Parameters

Parameter	Description
/SP-	Allows the initial installation setup message to be suppressed.
/VERYSILENT	Allows the installation to run in the background.
/SUPPRESSMSGBOXES	Allows setup message to be suppressed during the installation.
/MONITOR	Allows you to specify the list of event logs you want to monitor on the Windows operating system. The following Windows event logs can be monitored: • Application • Security • System • **Directory Service • **DNS Server • **File Replication The event log types must be separated using a comma-separated list. For example, **/MONITOR="Application","Security","System","Directory Service","DNS Server"** ***Note:*** *The ** indicates that these Windows Event Logs can be configured using the CLI to collected events, but the check boxes for these event types are not displayed in the configuration until you update your Windows Event Log device plug-in.*
/MONITORDEST	Allows you to specify the syslog destination that you want to receive the events. The IP address you type must be the address of your QRadar SIEM Console or Event Collector. For example, **/MONITORDEST=10.100.100.100:514** If you do not specify a port number, the default of port 514 is used for forwarding syslog events.

Table B-5 Updating Windows Event Log Parameters (continued)

Parameter	Description
/MONITORPROTO	Allows you to select the protocol to use when sending syslog events to QRadar SIEM. The protocol can be specified as TCP or UDP. For example, **/MONITORPROTO=TCP** or **/MONITORPROTO=UDP** If this parameter is not defined, the Adaptive Log Exporter service defaults to sending events using the UDP protocol.
/DEVICEADDRESS	Type the hostname or IP address for the device that sends the Windows events to QRadar SIEM. For example, **/DEVICEADDRESS=10.100.100.100** or **/DEVICEADDRESS=workstation102** or **/DEVICEADDRESS=%computername%** ***Note:*** *The device address field allows you to include system variables for bulk installations of the Adaptive Log Exporter. For example, %computername%.*

For example, to changed the destination IP address for QRadar SIEM from 10.100.100.100 to 10.100.1.1, type the following:

```
ALE_WindowsEventLogPlugin_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES /MONITORDEST=10.100.1.1:514
/DEVICEADDRESS=%COMPUTERNAME%
```

The /MONITORDEST parameter is updated for the Windows Event Log device plug-in.

The Windows Event Log device plug-in parameters are updated.

Updating Examples

This section provides several examples of using the Command Line Interface (CLI) to update your Windows Event Log device plug-in:

- **Updating the Device Address for the Windows Host**
- **Update Logs Monitored for Windows Event Log Device**
- **Updating the Windows Event Log Protocol**

Updating the Device Address for the Windows Host

To update the IP address of the Window Event Log device plug-in, type the following command:

```
ALE_WindowsEventLogPlugin_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES /DEVICEADDRESS=Device hostname or IP address
```

Update Logs Monitored for Windows Event Log Device

To update the event logs monitored by the Windows Event Log device plug-in, type the following command:

```
ALE_WindowsEventLogPlugin_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES /MONITOR="Application","Security","System",
"Directory Service","DNS Server","File Replication Service"
```

Updating the Windows Event Log Protocol

To update the Windows Event Log device plug-in to forward events using the TCP protocol, type the following command:

```
ALE_WindowsEventLogPlugin_setup.exe /SP- /VERYSILENT
/SUPPRESSMSGBOXES /MONITORPROTO=TCP
```

C SUPPORTED DEVICE PLUG-INS

Table C-1 provides information on the device plug-ins supported by the Adaptive Log Exporter.

IBM Security QRadar SIEM integrates with many manufacturers and vendors of security produc
plug-ins and documentation is updated regularly. If your device is not listed in this document, co
representative.

Table C-1 Supported Log Types and Files

Manufacturer	Product	Log Files Collected	Device Plug-in	Default Log File Directory
Cisco	ACS	Comma-separated event logs	Cisco ACS	Cisco ACS log files are stored in a log name: <ACS Directory>\<Service Name>\Log
Cisco	CSA	logfile.txt	Cisco CSA	Cisco CSA log files are stored in the fo C:\alerts\
Juniper Networks	Steel-Belted Radius	Comma-separated event logs, for example: • accepts_yyyymmdd.csv • rejects_yyyymmdd.csv • unknownClient_yyyymmdd.csv • badSharedSecret_yyyymmdd.csv	Juniper SBR	Juniper Networks Steel-Belted Radius following folder of the installation direct <SBR directory>\authReports\
Microsoft	Windows 2000, Windows 2003 Server, Windows 2008 Server, Windows XP, and Windows 7	• Application • Security • System • Directory Service • DNS • File Replication	Windows Event Log	None required. Selecting an event type Adaptive Log Exporter to retrieve event required data.

Table C-1 Supported Log Types and Files (continued)

Manufacturer	Product	Log Files Collected	Device Plug-in	Default Log File Directory
Microsoft	DHCP Server	DhcpSrvLog, or DhcpV6SrvLog	Windows DHCP	Microsoft DHCP log files are stored in <windir>\system32\dhcp\
Microsoft	Exchange 2003	SMTP files that end in .log and begin with one of the following: • (u_)ex - For W3C formatted log files. • (u_)nc - For NCSA formatted log files. • (u_)in - For IIS formatted log files.	Microsoft Exchange Server SMTP Logs	Microsoft Exchange SMTP log files ar directory: <windir>\System32\LogFiles\SMTPSV
Microsoft	Exchange 2003 or Exchange 2007	OWA files that end in .log and begin with one of the following: • (u_)ex - For W3C formatted log files. • (u_)nc - For NCSA formatted log files. • (u_)in - For IIS formatted log files.	Microsoft Exchange Server OWA Logs	Microsoft Exchange OWA log files are directory: <windir>\System32\LogFiles\W3SVC1
Microsoft	IAS Server	IAS log files ending in one of the following formats: • .ias • .log	Windows IAS	Microsoft IAS log files are stored in th C:\windows\system32\LogFiles\
Microsoft	IIS	• Web logs • FTP logs • IIS SMTP Logs • NNTP logs	Microsoft IIS	Microsoft IIS log files are stored in the C:\windows\system32\LogFiles\

Table C-1 Supported Log Types and Files (continued)

Manufacturer	Product	Log Files Collected	Device Plug-in	Default Log File Directory
Microsoft	ISA and Forefront Threat Management Gateway	ISA log files that end in one of the following formats: • .w3c • .isa	Windows ISA	Log directory for Microsoft ISA 2004: <Program Files>\MicrosoftISAServer\ Log directory for Microsoft ISA 2006: <windir>\System32\LogFiles\ Log directory for Microsoft Forefront T Gateway: <Program Files>\<Forefront Directory
Microsoft	SQL Server 2000, 2005, and 2008	ERRORLOG	Microsoft SQL Server	Microsoft SQL Server logs are stored C:\Program Files\Microsoft SQL Serve
NetApp	Data ONTAP	Event log files that end in .evt.	NetApp	NetApp Data ONTAP logs are stored /etc/log
Trend Micro	InterScan VirusWall	System and virus log files.	Trend Micro InterScan VirusWall	The InterScan VirusWall event logs ca following directory locations: • **<installation folder>\Log** • **Program Files\InterScan\lo**

D NOTICES AND TRADEMARKS

What's in this appendix:

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the

capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *www.ibm.com/legal/copytrade.shtml*.

The following terms are trademarks or registered trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.