

TECHNICAL NOTE

INSTALLING AND CONFIGURING ALE USING A CLI

APRIL 2010

If you want to install the Adaptive Log Exporter without the installation wizard, this document provides information about installing the Adaptive Log Exporter using a command line interface (CLI) utility. This CLI utility allows you to deploy your Adaptive Log Exporter to multiple remote systems in your deployment using any third-party product that allows remote or batch installs, for example, MSI Packaging Tools or Message-Oriented Middleware (MOM).



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

This document includes:

- [Installing the Adaptive Log Exporter](#)
- [Updating Your Windows Event Log Device](#)
- [Examples](#)

Installing the Adaptive Log Exporter

To install the Adaptive Log Exporter using a CLI:

- Step 1** Obtain the Adaptive Log Exporter CLI utility from the Juniper customer support web site:

`http://www.juniper.net/support/`



Note: Once you download the Adaptive Log Exporter CLI utility, you must select a distribution method to deploy the Adaptive Log Exporter to remote systems in your deployment.

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

- Step 3** In a Windows CLI, enter the following command:

```
AdaptiveLogExporter_setup /SP- /VERYSILENT /SUPPRESSMSGBOXES
```



Note: The SP-, VERYSILENT, and SUPPRESSMSGBOXES parameters are required parameters for each command entry.

- Step 4** Enter parameters, as necessary.

For more information, see [Parameters](#).

Parameters When entering the CLI utility options, the following parameters are available:

- [Required Parameters](#)
- [Optional Parameters](#)
- [Windows Event Log Monitoring Parameters](#)



Note: All parameters are case sensitive.

Required Parameters

The following parameters are required for the CLI utility:

`/SP- /VERYSILENT /SUPRESSMSGBOXES`

Optional Parameters

The following table provides the optional parameters for use with the CLI utility:

Table 1 Optional Parameters

Parameter	Description
<code>/DIR</code>	Specify the fully qualified path name to the destination directory for the Adaptive Log Exporter installation files. By default, the Adaptive Log Exporter is installed in the Program Files/Adaptive Log Exporter directory.
<code>/COMPONENTS</code>	Specify the list of Adaptive Log Exporter components you want to install. The options are: <ul style="list-style-type: none"> • main - Mandatory. You must specify this parameter to install the base components of the Adaptive Log Exporter service. • ui - Specify this parameter to install the user interface. If you do not specify any parameters in the <code>/COMPONENTS</code> option, the main and ui components are installed by default.
<code>/NOICONS</code>	Specify if you do not want to include the Adaptive Log Exporter icon to appear in your Start menu options.
<code>/GROUP</code>	By default, the Start menu displays the application as Adaptive Log Exporter. This parameter allows you to define a new group name.

Windows Event Log Monitoring Parameters

The Windows event log monitoring parameters allow you to automatically create a Windows event log device and a corresponding syslog destination. All of the below parameters must be included in the command.

The following table provides the Windows event log monitoring parameters:

Table 1-1 Windows Event Log Monitoring Parameters

Parameter	Description
<code>/MONITOR</code>	Specify using a comma separated list of event logs you want to monitor. For example: <code>/MONITOR=Application,Security,System</code>
<code>/MONITORDEST</code>	Specify the syslog destination that you want to receive the logs. You can specify this value in an <code><IP address or hostname>:<port></code> format. The port number defaults to 514 if not specified.
<code>/MONITORPROTO</code>	Specify the protocol to use when sending syslog log files. The protocol can be specified as TCP or UDP. The protocol defaults to UDP if not specified.
<code>/DEVICEADDRESS</code>	Specify the hostname or IP address you want to use in the syslog header when events are created. To the syslog receiver, this will appear as though this device address generated the message.

Updating Your Windows Event Log Device

Once you have installed the Adaptive Log Exporter using the CLI utility (see [Installing the Adaptive Log Exporter](#)), you can use the CLI utility to update your Windows Event Log Device configuration.

Your Windows Event Log Device must be configured in your deployment before you update your Windows Event Log Device using the CLI. Also, ensure your Windows Event Log Device configuration includes the default configuration values before you apply the update.

To update your Windows Event Log Device configuration:


- Step 1** Download the Windows Event Log Device plug-in from the Qmmunity web site:
<https://qmmunity.qllabs.com/>
- Step 2** Close all other active applications before installing the Windows Event Log Device plug-in.
- Step 3** In a Windows CLI, enter the following command:
`ALE_WindowsEventLogPlugin_setup.exe /SP- /VERYSILENT /SUPPRESSMSGBOXES`
-  **Note:** The `SP-`, `VERYSILENT`, and `SUPPRESSMSGBOXES` parameters are required parameters for each command entry.
- Step 4** Enter parameters, as necessary.

Table 1-2 Windows Event Log Monitoring Parameters

Parameter	Description
<code>/MONITOR</code>	Specify using a comma separated list of event logs you want to monitor. For example: <code>/MONITOR=Application,Security,System</code>
<code>/MONITORDEST</code>	Specify the syslog destination that you want to receive the logs. You can specify this value in an <code><IP address or hostname>:<port></code> format. The port number defaults to 514 if not specified.
<code>/DEVICEADDRESS</code>	Specify the hostname or IP address you want to use in the syslog header when events are created. To the syslog receiver, this will appear as though this device address generated the message.
<code>/PATCHONLY</code>	Specify this parameter if you update your configuration to a later version of the Windows Event Log plug-in without modifying the existing configuration.

Examples

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

- [Install Service Only](#)
- [Service Only Monitoring Windows Security Log](#)
- [Full Install](#)
- [Full Install Monitoring Windows Security Logs](#)

Install Service Only

If you want to install the Adaptive Log Exporter functionality without the user interface, enter the following command:

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

Service Only Monitoring Windows Security Log

If you want to install the Adaptive Log Exporter functionality without the user interface, and you also want to monitor Windows security logs and send events using the default syslog port (UDP port 514), enter the following command:

```
AdaptiveLogExporter_setup /SP- /VERYSILENT /SUPPRESSMSGBOXES
/COMPONENTS=main /MONITOR=Security /MONITORDEST=10.10.100.100
/DEVICEADDRESS=YourWindowsSystem.here.com
```

Full Install

If you want to the fully install the Adaptive Log Exporter, including the user interface and requiring no further configuration, enter the following command:

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

**Full Install
Monitoring Windows
Security Logs**

If you want to fully install the Adaptive Log Exporter, including the user interface and the ability to monitor Windows Security Logs, enter the following command:

```
AdaptiveLogExporter_setup /SP- /VERYSILENT /SUPPRESSMSGBOXES  
/COMPONENTS=main,ui /MONITOR=Security  
/MONITORDEST=10.10.100.100  
/DEVICEADDRESS=YourWindowsSystem.here.com
```

**Update IP Address
for Windows Event
Log Device**

If you install the Windows Event Log Device plug-in and want to modify the IP address of the Window Event Log Device, enter the following command:

```
ALE_WindowsEventLogPlugin_setup.exe /SP- /VERYSILENT  
/SUPPRESSMSGBOXES /DEVICEADDRESS=System.here.com
```

**Update Logs
Monitored for
Windows Event Log
Device**

If you install the Windows Event Log Device plug-in and want to change the type of logs you are monitoring, enter the following command:

```
ALE_WindowsEventLogPlugin_setup.exe /SP- /VERYSILENT  
/SUPPRESSMSGBOXES /MONITOR=Security,System
```

**Copy Files for
Windows Event Log
Configuration**

If you install the Windows Event Log Device plug-in and want to preserve your existing configuration while copying the necessary updated files from a patch, enter the following command:

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

Copyright Notice

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

Published: 2010-04-01