

TECHNICAL NOTE

FORWARDING WINDOWS EVENT LOG CONFIGURATION

APRIL 2010

This technical note provides information about gathering Windows event logs from multiple Windows systems in your deployment. This is useful if your deployment includes multiple Windows systems with the exact same username, password, and domain and you want to apply the same Windows Event Log Protocol configuration to multiple systems.

This document provides information on using the utility including:

- [Before You Begin](#)
- [Using the Utility](#)

Before You Begin

Before you use the utility to apply your Windows Event Log Protocol configuration to multiple systems in your deployment, you must:

Step 1 Install the Windows Event Log Protocol.

For more information, see the *Log Sources Users Guide*.

Step 2 Choose one of the following:

- If you are using STRM 2008.3, create a Windows Event Log Protocol entry.

For more information, see the *Managing Sensor Devices Guide*.

- If you are using STRM 2009.1, create a Microsoft Windows log source using the Windows Event Log protocol source.

For more information, see the *Log Sources Users Guide*.

Step 3 Create a .txt file that contains a hostnames or IP addresses of Windows systems in your deployment that you want to apply the Windows Event Log Protocol configuration. Each IP address or hostname must be listed on a separate line.

You are now ready to use the utility to apply the created Windows Event Log Protocol entry created in the STRM interface to multiple systems in your deployment. See [Using the Utility](#).

Using the Utility

To forward the Windows Event Log Protocol configuration to multiple systems in your deployment:

Step 1 Go to the Juniper customer support web site:

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

Step 2 Download the utility from **Products > DSMs** to your system hosting STRM.

Step 3 Log in to STRM, as root.

Step 4 Enter the following command:

```
chmod u+x BulkWindowsImport.py
```

Step 5 Determine the list of deployed Event Collectors and protocols:

```
BulkWindowsImport.py -d
```

The list of deployed Event Collectors and protocols appears.

Step 6 Enter the necessary command parameters. The command provides the following structure:

```
BulkWindowsImport.py -i <input file> -p <Windows Event Log Protocol Configuration ID> -e <EC ID>
```

The following table provides the available parameters:

Table 1-1 Utility Parameters

Parameter	Description
-i <input file>	Specify the full path to the input file containing the system hostnames or IP addresses you want to import. The file must contain the IP addresses or hostnames of all Windows system that you want to apply the configuration. Each system must be listed on a separate line. For more information, see Before You Begin .
-p <Windows Event Log Protocol configuration ID>	Specify the ID of the protocol to which these devices will belong. You can obtain a list of available protocols using the -d command. For more information, see Step 5 . For more information, see Before You Begin
-e <EC ID>	Specify an Event Collector identifier from which the logs will be gathered. You can obtain a list of available Event Collectors using the -d command. For more information, see Step 5 . If an invalid Event Collector ID is entered, the script prints out a list of valid IDs before exiting and no modifications are deployed. To determine a list of valid Event Collector IDs, enter 0 as the Event Collector ID.



Note: To view the additional information regarding parameters, enter `-h` for the help information.

Step 7 Log in to the STRM interface.

https://<IP Address>

Where <IP Address> is the IP address of the STRM system.

Step 8 In the main STRM interface, click the **Admin** tab.

The Admin interface appears.

Step 9 Click the **Deploy Changes** icon.

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