
Micro Focus Security ArcSight Micro Focus Security ArcSight Connectors

Software Version: 00.00

Optional. See [_HP_Cover.htm](#) for details.

SmartConnector for Microsoft Network Policy Server File

Document Release Date: June, 2018

Software Release Date: June, 2018



Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Copyright Notice

© Copyright 2006 – 2017; 2018 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

[ArcSight Product Documentation on the Micro Focus Security Community](#)

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Document Revision History

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to [ArcSight Product Documentation Community on the Micro Focus Security Community](#).

Document Changes

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
07/15/2017	Removed platform support for Windows 2003.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
11/15/2012	Added information about CIFS mount for Connector Appliance to Installation section.
05/15/2012	Added new installation procedure.
11/15/2011	Added support for DTS format.
09/30/2011	Updated configuration information to remove DTS format selection.
11/15/2010	Renamed connector from Microsoft IAS File; added support for Microsoft Windows Server 2008 version of Network Policy Server.

Contents

SmartConnector for Microsoft Network Policy Server File	7
Product Overview	8
Configuration	9
Microsoft NPS Configuration	9
Accounting Configuration Wizard	9
Configure NPS Log File Properties	10
Configure SQL Server Logging in NPS	11
Microsoft IAS Configuration	12
Select Requests to be Logged	12
Configure Event Logging	13
Configure Log File Properties	13
Install the SmartConnector	15
Prepare to Install Connector	15
Install Core Software	15
Set Global Parameters (optional)	16
Select Connector and Add Parameter Information	18
Select a Destination	19
Complete Installation and Configuration	19
Run the SmartConnector	21
Device Event Mapping to ArcSight Fields	22
Network Policy Server IAS Format Mappings to ArcSight Fields	22
Network Policy Server DTS Format Mappings to ArcSight Fields	23
Reason Codes	25
Microsoft Field Types and Descriptions	27
Microsoft DTS Reason Codes	33

Microsoft DTS Application Protocols	34
Specify the Locale for Determining Current Date for File Names	35
Send Documentation Feedback	36

SmartConnector for Microsoft Network Policy Server File

This guide provides information for installing the SmartConnector for Microsoft Network Policy Server File and configuring the device for event collection. Microsoft Windows Server 2008 versions of Network Policy Server are supported.

Product Overview

Network Policy Server (NPS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in Windows Server 2008. As a RADIUS server, Network Policy server performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless, authenticating switch, dial-up, and virtual private network (VPN) remote access, and router-to-router connections.

Configuration

Microsoft NPS Configuration

For complete information about the Microsoft Network Policy Server, see [Network Policy Server](#) in the Microsoft Windows Server 2008 documentation, from which Information in this section has been extracted.

NPS logging is also called *RADIUS accounting*. To configure NPS logging, you must configure which events you want logged and viewed with Event Viewer, and then determine which other information you want to log. You also must determine whether you want to log user authentication and accounting information to text log files stored on the local computer or to a SQL Server database on either the local computer or a remote computer.

There are three types of logging for Network Policy Server (NPS):

- Event logging. Used primarily for auditing and troubleshooting connection attempts. You can configure NPS event logging by obtaining the NPS server properties in the NPS console.
- Logging user authentication and accounting requests to a local file. Used primarily for connection analysis and billing purposes. Also useful as a security investigation tool because it provides a method for tracking the activity of a malicious user after an attack. You can configure local file logging using the Accounting Configuration wizard.
- Logging user authentication and accounting requests to a Microsoft SQL Server XML-compliant database. Used to let multiple servers running NPS have one data source. Also provides the advantages of using a relational database. You can configure SQL Server logging by using the Accounting Configuration wizard.

Accounting Configuration Wizard

By using the Accounting Configuration wizard in the NPS console, you can configure the following four accounting settings:

- **SQL logging only.** Use this setting to configure a data link to a SQL Server that lets NPS connect to and send accounting data to the SQL server. The wizard also can configure the database on the SQL Server to ensure that the database is compatible with NPS SQL server logging.
- **Text logging only.** Use this setting to configure NPS to log accounting data to a text file.

- **Parallel logging.** Use this setting to configure the SQL Server data link and database, as well as configure text file logging so that NPS logs simultaneously to the text file and the SQL Server database.
- **SQL logging with backup.** Use this setting to configure the SQL Server data link and database. In addition, you can configure text file logging that NPS uses if SQL Server logging fails.

In addition to these settings, both SQL Server logging and text logging allow you to specify whether NPS continues to process connection requests if logging fails. You can specify this in Logging failure action section in local file logging properties, in SQL Server logging properties, and while you are running the Accounting Configuration wizard.

To run the Accounting Configuration Wizard:

- 1 Open the NPS console or the NPS Microsoft Management Console (MMC) snap-in.
- 2 In the console tree, click **Accounting**.
- 3 In the details pane, in **Accounting**, click **Configure Accounting**.

Configure NPS Log File Properties

Note that membership in the Domain Admins group is the minimum required to perform this procedure. To configure NPS log file properties:

- 1 Open the NPS console.
- 2 In the console tree, click **Accounting**.
- 3 In the details pane, in **Log File Properties**, click **Change Log File Properties**. The **Log File Properties** dialog box opens.
- 4 In **Log File Properties**, on the **Settings** tab, in **Log the following information**, ensure that you choose to log enough information to achieve your accounting goals. For example, if your logs need to accomplish session correlation, select all check boxes.
- 5 In **Logging failure action**, select **If logging fails, discard connection requests** if you want NPS to stop processing Access-Request messages when log files are full or unavailable for some reason. If you want NPS to continue processing connection requests if logging fails, do not select this check box.
- 6 In the **Log File Properties** dialog box, click the **Log File** tab.
- 7 On the **Log File** tab, in **Directory**, enter the location where you want to store NPS log files. The default location is the systemroot\System32\LogFiles folder.



If you do not supply a full path statement in **Log File Directory**, the default path is used. For example, if you enter **NPSLogFile** in **Log File Directory**, the file is located at %systemroot%\System32\NPSLogFile.

8 In **Format**, click **DTS Compliant** or **IAS (Legacy)**.

9 In **Create a new log file**, to configure NPS to start new log files at specified intervals, click the interval that you want to use:

- For heavy transaction volume and logging activity, click **Daily**.
- For lesser transaction volumes and logging activity, click **Weekly** or **Monthly**.
- To store all transactions in one log file, click **Never (unlimited file size)**.
- To limit the size of each log file, click **When log file reaches this size**, and then type a file size, after which a new log is created. The default size is 10 megabytes (MB).

10 If you want NPS to delete old log files to create disk space for new log files when the hard disk is near capacity, ensure that **When disk is full delete older log files** is selected. This option is not available, however, if the value of **Create a new log file** is **Never (unlimited file size)**. Also, if the oldest log file is the current log file, it is not deleted.

Configure SQL Server Logging in NPS

Note that membership in Domain Admins, or equivalent, is the minimum required to complete this procedure. To configure SQL Server logging in NPS:

1 Open the NPS console or the NPS Microsoft Management Console (MMC) snap-in.

2 In the console tree, click **Accounting**.

3 In the details pane, in **SQL Server Logging Properties**, click **Change SQL Server Logging Properties**. The **SQL Server Logging Properties** dialog box opens.

4 In **Log the following information**, select the information you want to log:

- To log all accounting requests, click **Accounting requests**.
- To log authentication requests, click **Authentication requests**.
- To log periodic accounting status, click **Periodic accounting status**.
- To log periodic status, such as interim accounting requests, click **Periodic status**.

5 To configure the number of concurrent sessions allowed between the server running NPS and the SQL Server, enter a number in **Maximum number of concurrent sessions**.

6 To configure the SQL Server data source, in **SQL Server Logging**, click **Configure**. The **Data Link Properties** dialog box opens. On the **Connection** tab, specify the following:

- To specify the name of the server on which the database is stored, enter or select a name in **Select or enter a server name**.
 - To specify the authentication method with which to log on to the server, click **Use Windows NT integrated security**. Or, click **Use a specific user name and password** and then enter credentials in **User name** and **Password**.
 - To allow a blank password, click **Blank password**.
 - To store the password, click **Allow saving password**.
 - To specify which database to connect to on the computer running SQL Server, click **Select the database on the server**, and then select a database name from the list.
- 7** To test the connection between NPS and SQL Server, click **Test Connection**. Click **OK** to close **Data Link Properties**.
- 8** In **Logging failure action**, select **Enable text file logging for failover** if you want NPS to continue with text file logging if SQL Server logging fails.
- 9** In **Logging failure action**, select **If logging fails, discard connection requests** if you want NPS to stop processing Access-Request messages when log files are full or unavailable for some reason. If you want NPS to continue processing connection requests if logging fails, do not select this check box.

Microsoft IAS Configuration

Select Requests to be Logged

- 1** Open Internet Authentication Service (IAS) (click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Internet Authentication Service**).
- 2** In the console tree, click **Remote access logging**.
- 3** In the details pane, right-click **Local File**, then click **Properties**.
- 4** On the **Settings** tab, select one or more check boxes for recording authentication and accounting requests in the log files:
 - To capture requests and responses, select **Accounting requests**.
 - To capture authentication requests, Access-Accept messages, and Access-Reject messages, select **Authentication requests**.
 - To capture periodic status updates, such as interim accounting packets, select **Periodic status**.

Configure Event Logging

To configure event logging:

- 1 Open Internet Authentication Service (IAS).
- 2 Right-click **Internet Authentication Service (IAS)** and click **Properties**.
- 3 On the **General** tab, select each required option; then click **OK**.

Notes:

- Rejected, discarded, and successful authentication requests are logged by default.
- Selecting **Successful** authentication requests can result in logging extremely large volumes of data. Before selecting this option, verify that the Event Viewer is configured with a maximum log size that will accommodate this type of event logging.

Configure Log File Properties

To configure log file properties:

- 1 Open Network Policy Server.
- 2 In the console tree, click **Remote Access Logging**.
- 3 In the details pane, right-click **Local File**, then **Properties**.
- 4 On the **Log File** tab, in **Directory**, enter the location at which log files are to be stored. The default location is the *systemroot*\System32\LogFiles folder.
- 5 In **Format**, click **IAS**.
- 6 To open new log files at specific intervals, click the interval that you want to use:
 - For heavy transaction volume and logging activity, click **Daily**.
 - For lesser transaction volumes and logging activity, click **Weekly** or **Monthly**.
 - To store all transactions in one log file, click **Never (unlimited file size)**The **When log file reaches this size** option is not supported by the SmartConnector.
- 7 To automatically delete log files when the disk is full, click **When disk is full delete older log files**. If the oldest log file is the current log file, it is not deleted.

Notes:

- To log accounting information to a remote server, specify the log file name by entering a Universal Naming Convention (UNC) name, such as \\MyLogServer\LogShare.

- If you do not supply a full path statement in **Log File Directory**, the default path is used. For example, if you enter **IASLogFile** in **Log File Directory**, the file is located at `systemroot\System32\IASLogFile`.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.



Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

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

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

Install Core Software

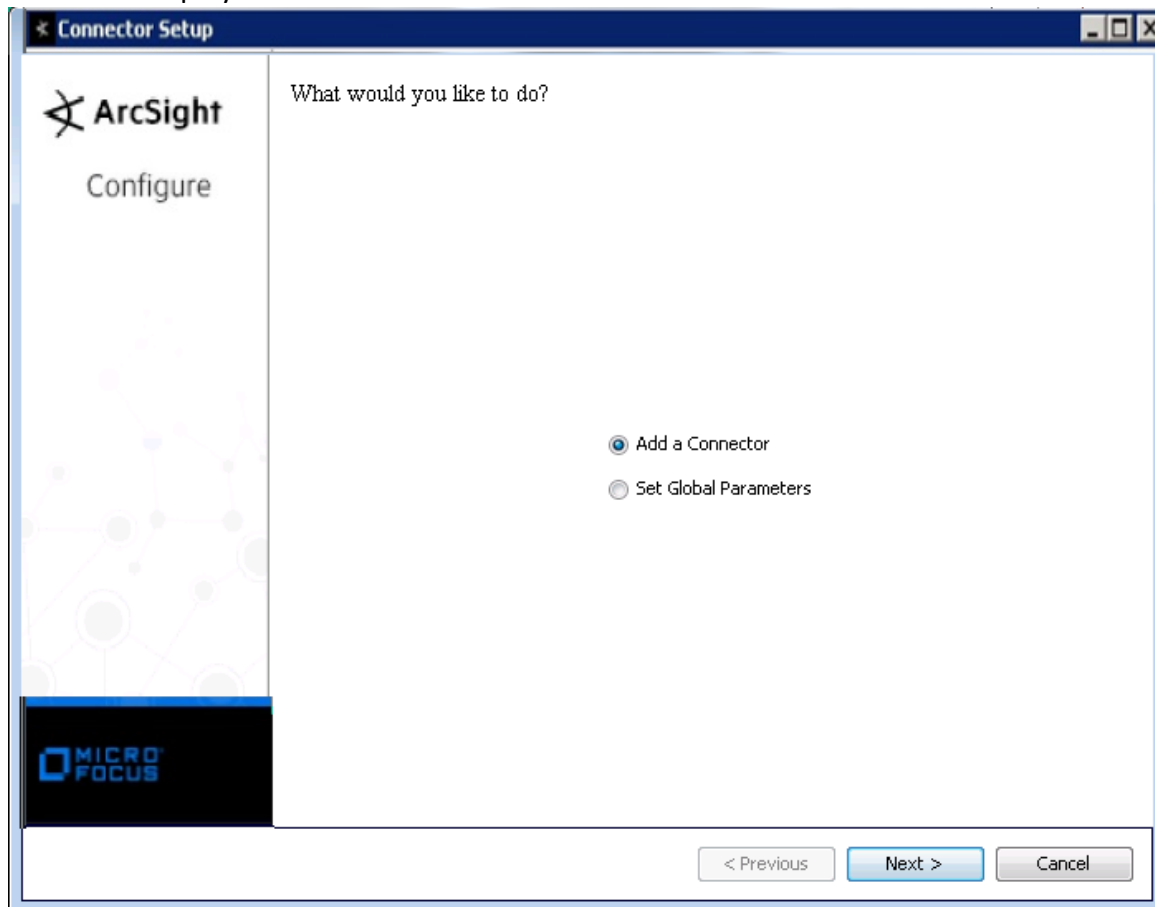
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 1 Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
- 2 Start the SmartConnector installation and configuration wizard by running the executable.

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

Introduction
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...

3 When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector"

window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

- 1 Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
- 2 Select **Microsoft Network Policy Server File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Connector Setup

ArcSight
Configure

Enter the parameter details

Log File Home: C:\WINDOWS\system32\LogFiles

New Log Time Period: Daily

Log File Type: IAS

< Previous Next > Cancel

Parameter	Description
Log File Home	Enter the value of 'Log file directory' from Enter the path to the folder containing the Network Policy Server log files (for example, C:\WINDOWS\system32\LogFiles).
New Log Time Period	From the drop-down menu, choose the time period you selected in the Extended Logging Properties window. Selections supported by the connector include 'Hourly', 'Daily', 'Weekly', 'Monthly', or 'Unlimited file size'. The 'When file size reaches:' selection is not supported.
Log File Type	Select 'IAS' for IAS (Legacy) format; select 'DTS' for DTS format. See step 8 in "Configure NPS Log File Properties" for information about selecting format.

Select a Destination

- 1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.
- 2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.
- 3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.
- 4 If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

- 1 Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.
- 2 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.
- 3 If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4 Click **Next** on the summary window.

5 To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

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

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

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

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

Device Event Mapping to ArcSight Fields

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

Network Policy Server IAS Format Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Medium when Device Severity = Access-Reject; Low when Device Severity = Access-Accept, Accounting-Request
Application Protocol	protocol
Bytes In	Acct-Input-Octets
Bytes Out	Acct-Output-Octets
Destination Address	Login-IP-Host
Destination Port	Login-TCP-Port
Destination Process Name	Login-Service
Device Action	Acct-Status-Type ("1=Start","2=Stop")
Device Custom Number 2	Acct-Session-Time
Device Custom String 1	Class (see "Microsoft IAS Field Types and Descriptions")
Device Custom String 2	Service-Type
Device Custom String 3	ClientFriendlyName
Device Custom String 4	Acct-Input-Packets
Device Custom String 5	Acct-Output-Packets
Device Custom String 6	Called-Station-Id
Device Event Class Id	Packet-Type (1=Access-Request, 2=Access-Accept, 3=Access-Reject, 4=Accounting-Request)
Device Host Name	NAS-Identifier
Device Severity	Packet-Type (1=Access-Request, 2=Access-Accept, 3=Access-Reject, 4=Accounting-Request)
Device Version	MS-RAS-Version

ArcSight ESM Field	Device-Specific Field
External ID	Acct-Session-ID
Message	Reason-Code
Name	Packet-Type (1=Access-Request, 2=Access-Accept, 3=Access-Reject, 4=Accounting-Request)
Source Host Name	Calling-Station-ID
Source Port	NAS-Port
Source Translated Address	Framed-IP-Address
Transport Protocol	protocol

Network Policy Server DTS Format Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Medium = Access-Reject; Low = Access-Request, Access-Accept, Accounting-Request, Access-Challenge
Application Protocol	Authentication-Type
Bytes In	Acct-Input-Octets
Bytes Out	Acct-Output-Octets
Destination Address	One of (NAS-IP-Address, Client-IP-Address)
Destination Host Name	One of (Client-Friendly-Name, NAS-Identifier)
Destination NT Domain	User-Name
Destination Port	NAS-Port
Destination Process Name	Login-Service
Destination User Name	User-Name
Device Action	Acct-Status-Type (1=Start, 2=Stop)
Device Address	Class
Device Custom Number 1	Session-Timeout
Device Custom Number 2	Acct-Session-Time
Device Custom Number 3	Acct-Interim-Interval
Device Custom String 1	Class

SmartConnector for Microsoft Network Policy Server File
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	Service-Type (2=Framed)
Device Custom String 3	Calling-Station-Id
Device Custom String 4	Provider-Type (0 = No authentication occurred, 1 = Authentication occurs on the local NPS server, 2 = Connection request is forwarded to a remote RADIUS server for authentication)
Device Custom String 5	MS-CHAP-Domain
Device Custom String 6	Tunnel-Type (1-PPTP)
Device Event Class ID	One of (Packet-Type, Acct-Status-Type)
Device Host Name	Computer-Name
Device Process Name	Event-Source
Device Product	'NPS'
Device Receipt Time	Timestamp
Device Severity	Packet-Type
Device Vendor	'Microsoft'
Device Version	MS-RAS-Version
External ID	Acct-Session-Id
Message	Reason-Code
Name	One of (Packet-Type, Acct-Status-Type)
Source Translated Address	Framed-IP-Address
Transport Protocol	Framed-Protocol (1=PPP)

Reason Codes

Code	Meaning
0	Success
1	Internal error
2	Access denied
3	Malformed request
4	Global catalog unavailable
5	Domain unavailable
6	Server unavailable
7	No such domain
8	No such user
16	Authentication failure
17	Password change failure
18	Unsupported authentication type
19	No reversibly encrypted password is stored for the user account
32	Local users only
33	Password must be changed
34	Account disabled
35	Account expired
36	Account locked out
37	Invalid logon hours
38	Account restriction
48	Did not match remote access policy
49	Did not match connection request policy
64	Dial-in locked out
65	Dial-in disabled
66	Invalid authentication type
67	Invalid calling station

Code	Meaning
68	Invalid dial-in hours
69	Invalid called station
70	Invalid port type
71	Invalid restriction
80	No record
96	Session timed out
97	Unexpected request

Microsoft Field Types and Descriptions

User-Name: Text

The user identity, as specified by the user.

NAS-IP-Address: Text

The IP address of the NAS originating the request.

NAS-Port: Number

The physical port number of the NAS originating the request.

Service-Type: Number

The type of service that the user has requested.

Framed-Protocol: Number

The protocol to be used.

Framed-IP-Address: Text

The framed address to be configured for the user.

Framed-IP-Netmask: Text

The IP netmask to be configured for the user.

Framed-Routing: Number

The Routing method to be used by the user.

Filter-ID: Text

The name of the filter list for the user requesting authentication.

Framed-MTU: Number

The maximum transmission unit to be configured for the user.

Framed-Compression: Number

The compression protocol to be used.

Login-IP-Host: Number

The IP address of the host to which the user should be connected.

Login-Service: Number

The service that connects the user to the login host.

Login-TCP-Port: Number

The TCP port to which the user should be connected.

Reply-Message: Text

The message displayed to the user when an authentication request is accepted.

Callback-Number: Text

The callback phone number.

Callback-ID: Text

The name of a location to be called by the access server when performing callback.

Framed-Route: Text

The routing information that is configured on the access client.

Framed-IPX-Network: Number

The IPX network number to be configured on the NAS for the user.

Class: Text

The attribute sent to the client in an Access-Accept packet, which is useful for correlating Accounting-Request packets with authentication sessions. The format is:

- Type Contains the value 25 (1 octet).
- Length Contains a value of 20 or greater (1 octet).
- Checksum Contains an Adler-32 checksum that is computed over the remainder of the Class attribute (4 octets).
- Vendor-ID Contains the ID of the access server vendor (4 octets). The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the vendor in network byte order, as defined in RFC 1007 "Vendor SMI Network Management Private Enterprise Codes".
- Version Contains the value of 1 (2 octets).
- server-Address Contains the IP address of the RADIUS server that issued the Access-Challenge. For multihomed servers, this is the address of the network interface that received the original Access-Request (2 octets).
- Service-Reboot-Time Specifies the time at which the first serial number was returned (8 octets).
- Unique-Serial-Number Contains a unique number to distinguish an individual connection attempt (8 octets).
- String Contains information that is used to classify accounting records for additional analysis (0 or more octets). In IAS, the Class attribute from the profile is copied into the String field.
- The Class attribute is used to match the accounting and authentication records if the Class attribute is sent by the network access server in the accounting request packets. The combination of Serial-Number, Service-Reboot-Time, and server-Address must be a unique identification for each authentication that the server accepts.

Vendor-Specific: Text

The attribute that is used to support proprietary NAS features.

Session-Timeout: Number

The length of time (in seconds) before a session is terminated.

Idle-Timeout: Number

The length of idle time (in seconds) before a session is terminated.

Termination-Action: Number

The action that the NAS should take when service is completed.

Called-Station-ID: Text

The phone number that is dialed by the user.

Calling-Station-ID: Text

The phone number from which the call originated.

NAS-Identifier: Text

The string that identifies the NAS originating the request.

Login-LAT-Service: Text

The host with which the user is to be connected by LAT.

Login-LAT-Node: Text

The node with which the user is to be connected by LAT.

Login-LAT-Group: Text

The LAT group codes for which the user is authorized.

Framed-AppleTalk-Link: Number

The AppleTalk network number for the serial link to the user (this is used only when the user is a router).

Framed-AppleTalk-Network: Number

The AppleTalk network number that the NAS must query for existence in order to allocate the user's AppleTalk node.

Framed-AppleTalk-Zone: Text

The AppleTalk default zone for the user.

Acct-Status-Type: Number

The number that specifies whether an accounting packet starts or stops a bridging, routing, or Terminal server session.

Acct-Delay-Time: Number

The length of time (in seconds) for which the NAS has been sending the same accounting packet.

Acct-Input-Octets: Number

The number of octets received during the session.

Acct-Output-Octets: Number

The number of octets sent during the session.

Acct-Session-ID: Text

The unique numeric string that identifies the server session.

Acct-Authentic: Number

The number that specifies which server has authenticated an incoming call.

Acct-Session-Time: Number

The length of time (in seconds) for which the session has been active.

Acct-Input-Packets: Number

The number of packets received during the session.

Acct-Output-Packets: Number

The number of packets sent during the session.

Acct-Terminate-Cause: Number

The reason that a connection was terminated.

Acct-Multi-SSN-ID: Text

The unique numeric string that identifies the multilink session.

Acct-Link-Count: Number

The number of links in a multilink session.

Event-Timestamp: Time

The date and time that this event occurred on the NAS.

NAS-Port-Type: Number

The type of physical port that is used by the NAS originating the request.

Port-Limit: Number

The maximum number of ports that the NAS provides to the user.

Login-LAT-Port: Number

The port with which the user is connected by Local Area Transport (LAT).

Tunnel-Type: Number

The tunneling protocols to be used.

Tunnel-Medium-Type: Number

The transport medium to use when creating a tunnel for protocols. For example, L2TP packets can be sent over multiple link layers.

Tunnel-Client-Endpt: Text

The IP address of the tunnel client.

Tunnel-server-Endpt: Text

The IP address of the tunnel server.

Acct-Tunnel-Connection: Text

An identifier assigned to the tunnel.

Password-Retry: Number

The number of times a user can try to be authenticated before the NAS terminates the connection.

Prompt: Number

A number that indicates to the NAS whether or not it should (Prompt=1) or should not (Prompt=0) echo the user's response as it is typed.

Connect-Info: Text

Information that is used by the NAS to specify the type of connection made. Typical information includes connection speed and data encoding protocols.

Configuration-Token: Text

The type of user profile to be used (sent from a RADIUS proxy server to a RADIUS proxy client) in an Access-Accept packet.

Tunnel-Pvt-Group-ID: Text

The group ID for a particular tunneled session.

Tunnel-Assignment-ID: Text

The tunnel to which a session is to be assigned.

Tunnel-Preference: Number

A number that indicates the preference of the tunnel type, as indicated with the Tunnel-Type attribute when multiple tunnel types are supported by the access server.

Acct-Interim-Interval: Number

The length of interval (in seconds) between each interim update sent by the NAS.

Ascend-to-255: Text

The vendor-specific attributes for Ascend. For more information, see the Ascend documentation.

Client-IP-Address: Text

The IP address of the RADIUS client.

NAS-Manufacturer: Number

The manufacturer of the NAS.

MS-CHAP-Error: Number

The error data that describes an MS-CHAP transaction.

Authentication-Type: Number

The authentication scheme that is used to verify the user.

Client-Friendly-Name: Text

The friendly name for the RADIUS client.

SAM-Account-Name: Text

The user account name in the Security Accounts Manager (SAM) database.

Fully-Qualified-User-Name: Text

The user name in canonical format.

EAP-Friendly-Name: Text

The friendly name that is used with Extensible Authentication Protocol (EAP).

Packet-Type: Number

The type of packet, which can be:

1=Access-Request

2=Access-Accept

3=Access-Reject

4=Accounting-Request

NP-Policy-Name: Text

The friendly name of a remote access policy.

Microsoft DTS Reason Codes

- 1 = Access-Request
- 2 = Access-Accept
- 3 = Access-Reject
- 4 = Accounting-Request
- 5 = Accounting-Response
- 11 = Access-Challenge

Microsoft DTS Application Protocols

- 1 = PAP
- 2 = CHAP
- 3 = MS-CHAP
- 4 = MS-CHAP v2
- 5 = EAP
- 7 = None
- 8 = Custom
- 11 = PEAP-MSCHAP

Specify the Locale for Determining Current Date for File Names

An advanced parameter named `localeforfilename` has been added to specify the locale used for determining the current date for file names. If not specified, the default locale will be used, which normally works unless the default locale is Thailand, which numbers years differently. For Thailand, the parameter should be set to `en_US`.

To set advanced parameters for your SmartConnector, after connector installation, edit the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`. Locate the `localeforfilename` parameter and set its value to `en_US`. Save the file and restart the connector for your changes to take effect.

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on SmartConnector for Microsoft Network Policy Server File (Micro Focus Security ArcSight Connectors 00.00)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arcsight_doc@microfocus.com.

We appreciate your feedback!