



ArcSight SmartConnectors

Software Version: CE 24.3

Configuration Guide for Microsoft Network Policy Server File SmartConnector

Document Release Date: July 2024

Software Release Date: July 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft Network Policy Server File SmartConnector	4
Product Overview	5
Configuring the SmartConnector	6
Configuring Microsoft NPS	6
Accounting Configuration Wizard	6
Configuring NPS Log File Properties	7
Configuring SQL Server Logging in NPS	9
Installing the SmartConnector	11
Preparing to Install the SmartConnector	11
Installing and Configuring the SmartConnector	11
Device Event Mapping to ArcSight Fields	13
Network Policy Server IAS Format Mappings to ArcSight Fields	13
Network Policy Server DTS Format Mappings to ArcSight Fields	14
Reason Codes	16
Microsoft Field Types and Descriptions	18
Microsoft DTS Reason Codes	23
Microsoft DTS Application Protocols	24
Specifying the Locale for Determining Current Date for File Names	25
Setting Advanced Parameters for the SmartConnector	25
Send Documentation Feedback	26

Configuration Guide for Microsoft Network Policy Server File SmartConnector

This guide provides information for installing the SmartConnector for Microsoft Network Policy Server File and configuring the device for event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

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

Configuring the SmartConnector

Configuring Microsoft NPS

NPS logging is also known as RADIUS accounting.

To configure NPS logging, you must configure the events you want to log and view using the Event Viewer, and then determine the relevant information you want to log. It is necessary to determine whether you want to log user authentication and accounting information to text log files stored on the local computer or to an SQL Server database on either a local computer or a remote computer.

Following are the types of logging used for NPS:

- **Event logging:** This is used for auditing and troubleshooting connection attempts. You can configure NPS event logging by obtaining the NPS server properties in the NPS console.
- **User authentication and accounting requests to a local file logging:** This is used for connection analysis and billing purposes. This is also used as a security investigation tool because it provides a method for tracking the activity of a malicious user after an attack.
- **User authentication and accounting requests to a Microsoft SQL Server XML-compliant database logging:** This is used for multiple servers that are running on NPS and have one data source. This also provides the advantages of using a relational database.



Note: Accounting Configuration wizard can be used to configure SQL Server logging and local file logging.

For more information regarding the Microsoft Network Policy Server, see the Network Policy Server section in the [Microsoft documentation](#).

Accounting Configuration Wizard

The following accounting settings can be configured by using the Accounting Configuration wizard in the NPS console:

- **SQL logging only:** This setting is used to configure a data link to an SQL Server that connects NPS to send accounting data to the SQL server. You can also configure the

database on the SQL Server to ensure that the database is compatible with NPS SQL server logging.

- **Text logging only:** This setting is used to configure NPS to log accounting data to a text file.
- **Parallel logging:** This setting is used to configure the SQL Server data link and database. You can also configure text file logging so that NPS logs simultaneously to the text file and the SQL Server database.
- **SQL logging with backup:** This setting is used to configure the SQL Server data link and database. You can also configure text file logging that NPS uses if SQL Server logging fails.

Both SQL Server logging and text logging allows you to specify whether NPS will continue to process connection requests if logging fails. This can be specified while running the Accounting Configuration wizard in the **SQL Server logging properties > Local File Logging properties > Logging failure action** section.

Perform the following to run the Accounting Configuration Wizard:

1. Open the NPS console or the NPS Microsoft Management Console (MMC) snap-in.
2. Navigate to the console tree and click **Accounting > Configure Accounting**.

Configuring NPS Log File Properties

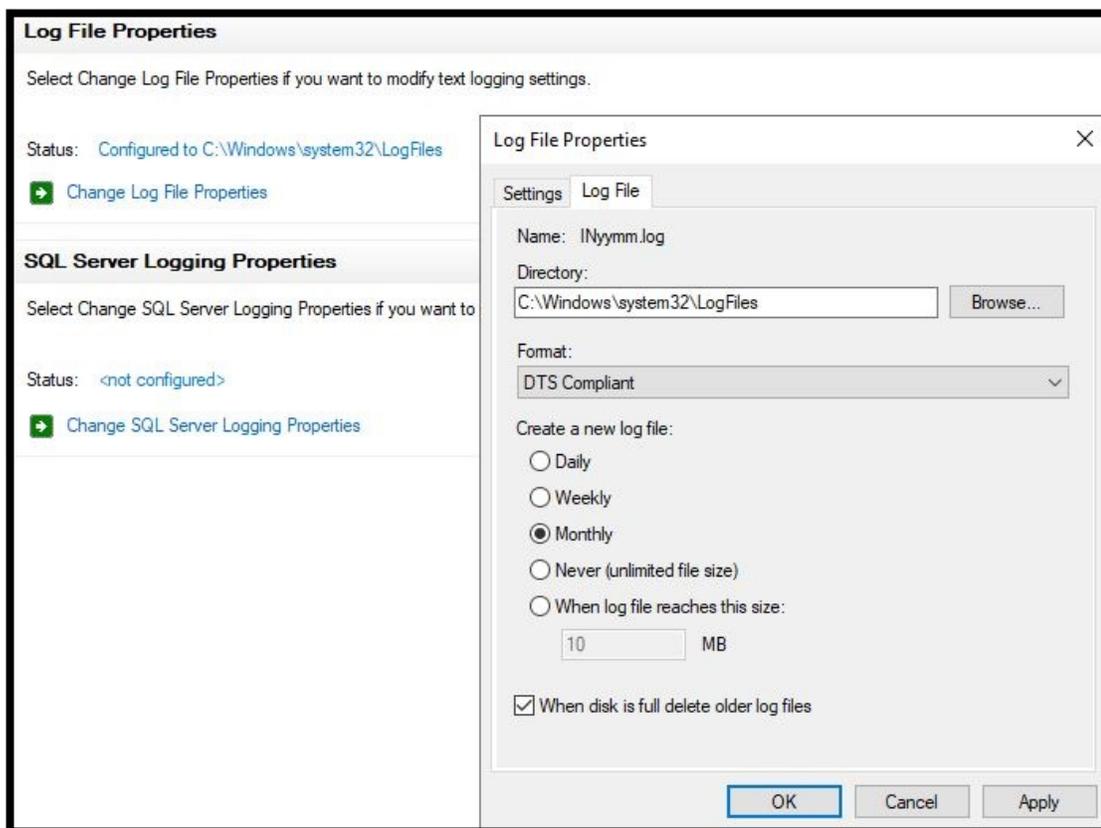


Note: Membership in the Domain Admins group is the minimum required permission to perform this procedure.

Perform the following to configure NPS log file properties:

1. Open the NPS console or the NPS Microsoft Management Console (MMC) snap-in.
2. Navigate to the console tree and click **Accounting**.
3. Navigate to **Log File Properties > Change Log File Properties** and then click **Settings**.
4. Under **Log the following information**, ensure to select the option that will ensure to collect enough log information to achieve your accounting goals. For example, select all check boxes if your logs need to accomplish session correlation.
5. Under **Logging failure action**:
 - Select the **If logging fails, discard connection requests** check box if you want NPS to stop processing Access-Request messages when log files are full or unavailable.

- Clear the **If logging fails, discard connection requests** check box if you want NPS to continue processing connection requests if logging fails.
6. Click **Log File** and perform the following:
- a. In the **Directory** field, enter the path for the directory where you want to store the NPS log files. The default location is the %systemroot%\System32\LogFiles folder if no further changes are made.
 - b. In the **Format** list, click **DTS Compliant** or **IAS (Legacy)**.
 - c. To configure NPS to start creating new log files at specified intervals under **Create a new log file**, select one of the following:
 - Click **Daily** for heavy transaction volume and logging activity.
 - Click **Weekly** or **Monthly** for lesser transaction volumes and logging activity.
 - Click **Never (unlimited file size)** to store all transactions in one log file.
 - Click **When log file reaches this size** to limit the size of each log file, and type a file size to create a new log. The default size is 10 megabytes.



7. Ensure to select the **When disk is full delete older log files** check box to create disk space for new log files when the hard disk is near capacity. However, this option remains unavailable if the value of the new log file is selected as **Never (unlimited file**

size).

8. Click **Apply** to apply the changes and then click **OK**.

Configuring SQL Server Logging in NPS

Perform the following to configure SQL Server logging in NPS:



Note: Membership in Domain Admins, or equivalent, is the minimum required to complete this procedure.

1. Open the NPS console or the NPS Microsoft Management Console (MMC) snap-in.
2. Navigate to the console tree and click **Accounting**.
3. Navigate to the **SQL Server Logging Properties > Change SQL Server Logging Properties**.
4. Under **Log the following information**, select one of the following:
 - Click **Accounting requests** to log all accounting requests.
 - Click **Authentication requests** to log authentication requests.
 - Click **Periodic accounting status** to log periodic accounting status.
 - Click **Periodic status** to log periodic status, such as interim accounting requests.
5. Enter a desired number for the **Maximum number of concurrent sessions** to configure the number of concurrent sessions allowed between the server running NPS and SQL.
6. To configure the SQL Server data source:

Under **SQL Server Logging**, click **Configure**. Navigate to **Data Link Properties > Connection**, and specify the following:

 - Enter or select a name in the **Select or enter a server name** field to specify the name of the server on which the database is stored.
 - Select **Use Windows NT integrated security** to specify the authentication method with which to log on to the server. Or, select **Use a specific user name and password** and enter the **User name** and **Password**.
 - Select **Blank password** to allow a blank password.
 - Select **Allow saving password** to store the password.
 - Click **Select the database on the server** to specify the database for connecting to

the computer running the SQL Server, and select the desired database name from the list.

7. Click **Test Connection** to test the connection between NPS and SQL Server and then click **OK**.
8. Under **Logging failure action**, select the following:
 - If you want NPS to continue with text file logging if the SQL Server logging fails, select the **Enable text file logging for failover** check box.
 - If you want NPS to stop processing Access-Request messages when log files are full or unavailable, select the **If logging fails, discard connection requests** check box. Ensure to clear the check box, if you want NPS to continue processing connection requests if logging fails.



Note: The Microsoft Network Policy Server File connector supports only text-based logs, and not SQL logging.

Installing 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](#) section in the [ArcSight Management Center Administrator's Guide](#).

Preparing to Install the SmartConnector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

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

Installing and Configuring the SmartConnector

The installation steps described in this section are specific to the Microsoft Network Policy Server File SmartConnector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure the Microsoft Network Policy Server File SmartConnector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.

- From the **Type** drop-down list, select **Microsoft Network Policy Server File** as the type of connector, and then click **Next**.
- Enter the following parameters to configure the SmartConnector, and then click **Next**.

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 list, choose the time period that you selected in the Extended Logging Properties window. The options include Hourly , Daily , Weekly , Monthly , or Unlimited file size . The File size reaches limit selection is not supported.
Log File Type	Select IAS for IAS (Legacy) format; select DTS for DTS format.

- Select a [destination and configure parameters](#).
- Specify a name for the connector.
- (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

- Select whether you want to install the connector as a service or in the standalone mode.
- Complete the installation.
- [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

Device Event Mapping to ArcSight Fields

The following section lists the mapping of ArcSight data fields to the device's specific event definitions.

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
External ID	Acct-Session-ID

ArcSight ESM Field	Device-Specific Field
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
Device Custom String 2	Service-Type (2=Framed)
Device Custom String 3	Calling-Station-Id

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

ArcSight ESM Field	Device-Specific Field
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
68	Invalid dial-in hours
69	Invalid called station

Configuration Guide for Microsoft Network Policy Server File SmartConnector
Reason Codes

70	Invalid port type
71	Invalid restriction
80	No record
96	Session timed out
97	Unexpected request

Microsoft Field Types and Descriptions

Field Type	Data Type	Description
User-Name	Text	The specified identity.
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.
Framed-Protocol	Number	The protocol to be used.
Framed-IP-Address	Text	The configured framed address.
Framed-IP-Netmask	Text	The configured IP netmask.
Framed-Routing:	Number	The routing method.
Filter-ID	Text	The name of the filter list for requesting authentication.
Framed-MTU	Number	The maximum configured transmission unit.
Framed-Compression	Number	The compression protocol used.
Login-IP-Host	Number	The IP address of the host.
Login-Service	Number	The service that will connect to the login host.
Login-TCP-Port	Number	The TCP port.
Reply-Message	Text	The displayed message when an authentication request is accepted.
Callback-Number	Text	The callback phone number.
Callback-ID	Text	The name of a location by the access server while performing callback.
Framed-Route	Text	The configured routing information on the access client.
Framed-IPX-Network	Number	The configured IPX network number on the NAS.

Field Type	Data Type	Description
Class	Text	<p>The attribute sent to the client in an Access-Accept packet. This is useful for correlating Accounting-Request packets with authentication sessions. The format is as follows:</p> <ul style="list-style-type: none"> • Type: Specifies the value 25 (1 octet). • Length: Specifies a value of 20 or greater (1 octet). • Checksum: Specifies an Adler-32 checksum that is computed over the remainder of the Class attribute (4 octets). • Vendor-ID: Specifies 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: Specifies the value of 1 (2 octets). • Server-Address: Specifies the IP address of the RADIUS server that issued the Access- Challenge. For multi-home servers, this is the address of the network interface that receives 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: Specifies a unique number to distinguish an individual connection attempt (8 octets). • String: Specifies 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. • Class attribute: Specifies the combination of Serial-Number, Service-Reboot-Time, and Server-Address that must be a unique identification for each authentication that the server accepts. This 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.
Vendor-Specific	Text	The attribute 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 must take when service is completed.
Called-Station-ID	Text	The dialed phone number.

Field Type	Data Type	Description
Calling-Station-ID	Text	The origin phone number for the call.
NAS-Identifier	Text	The string that identifies the NAS originating the request.
Login-LAT-Service	Text	The host used for connection by Local Area Transport (LAT).
Login-LAT-Node	Text	The node used for connection by LAT.
Login-LAT-Group	Text	The authorized LAT group codes.
Framed-AppleTalk-Link	Number	The AppleTalk network number for the serial link (this is used only in case of a router).
Framed-AppleTalk-Network	Number	The AppleTalk network number that is required for the NAS query exists to allocate the AppleTalk node.
Framed-AppleTalk-Zone	Text	The AppleTalk default zone.
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 identifying the multilink session.
Acct-Link-Count	Number	The number of links in a multilink session.
Event-Timestamp	Time	The date and time for the event occurring on the NAS.
NAS-Port-Type	Number	The type of physical port used by the NAS for originating the request.
Port-Limit	Number	The maximum number of ports provided by the NAS.
Login-LAT-Port	Number	The connection port used by LAT.
Tunnel-Type	Number	The tunneling protocols to be used.

Field Type	Data Type	Description
Tunnel-Medium-Type	Number	The transport medium for creating a tunnel for protocols. For example, L2TP packets can be sent to 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 required for authentication before the NAS terminates the connection.
Prompt	Number	A number that indicates to the NAS whether it should (Prompt=1) or should not (Prompt=0) echo the 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 profile 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 assigned to a session.
Tunnel-Preference	Number	A number that indicates the preference of the tunnel type. This is 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 used for verification.
Client-Friendly-Name	Text	The name for the RADIUS client.
SAM-Account-Name	Text	The account name in the Security Accounts Manager (SAM) database.
Fully-Qualified-User-Name	Text	The user name in canonical format.

Configuration Guide for Microsoft Network Policy Server File SmartConnector
Microsoft Field Types and Descriptions

Field Type	Data Type	Description
EAP-Friendly-Name	Text	The name that is used with Extensible Authentication Protocol (EAP).
Packet-Type	Number	The type of packet, which can be as follows: 1=Access-Request 2=Access-Accept 3=Access-Reject 4=Accounting-Request
NP-Policy-Name	Text	The name of a remote access policy.

Microsoft DTS Reason Codes

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

Microsoft DTS Application Protocols

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

Specifying the Locale for Determining Current Date for File Names

The locale that is used to determine the current date for file names can be specified using the `localeforfilename` parameter. The default locale will be used if nothing is specified. This usually works unless Thailand is selected as the default locale, in which the numbers for the years are modified. The parameter needs to be set to `en_US` for Thailand.

Setting Advanced Parameters for the SmartConnector

After the SmartConnector has been installed, perform the following to set the advanced parameters:

1. Modify the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`.
2. Locate the `localeforfilename` parameter and set its value to `en_US`. Save the file and restart the connector.

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 Configuration Guide for Microsoft Network Policy Server File SmartConnector (SmartConnectors CE 24.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!