



Micro Focus Security ArcSight Connectors

SmartConnector for Microsoft Windows Event
Log – Unified

Configuration Guide

August 15, 2017

Configuration Guide

SmartConnector for Microsoft Windows Event Log – Unified

August 15, 2017

Copyright © 2008 – 2018 Micro Focus or one of its affiliates.

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2010 - 2018 Micro Focus or one of its affiliates.

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.

Revision History

Date	Description
08/15/2017	Updated steps in installation procedure for importing certificates. Added troubleshooting information regarding random JCIFS name when installing connector on Linux.
07/15/2017	Added troubleshooting information.
05/15/2017	Removed Windows 2003 due to end of support. Added a troubleshooting issue for reading event logs from Windows 2012 R2 systems.
11/30/2016	Update to installation procedure to add “Set Global Parameters”.
05/16/2016	When importing .csv files to populate table entry parameters, it is now noted that there should be a carriage return (only one CR) at the last entry in the .csv file for the import to work.
02/15/2016	Removed requirement for Power User for setting up local user with a standard local user account from Windows Vista workgroup hosts.

Date	Description
09/30/2015	Added information about enabling remote management at the end of the Installation section.
09/30/2014	Removed Windows XP and 2000 support.
05/15/2014	GA of support for Windows Server 2012 R2.

Contents

Product Overview	6
Features and Enhancements	6
Operating Systems Supported	6
Collecting from Windows Event Collector Host	7
Events Supported	7
NTLMv2 Authentication	7
Internationalization	7
SID Translation	7
GUID Translation	8
GUID translation with Global Catalog with SSL Connection	8
Host Browsing	8
Known Limitations	9
Configuration	10
Enable Microsoft Windows Event Log Audit Policies	10
Audit a Local System	11
Audit Within a Domain	12
Set Up an Audit Policy for a Domain	13
Set Up Standard User Accounts	13
With Standard Domain User Account	13
With a Standard Local User Account from Windows Vista Workgroup Hosts	14
Configure NTLMv2 Authentication	15
Add Security Certifications when Using SSL	16
Collect Forwarded Events	18
Windows Event Forwarding Use Case	18
Event Collector for Windows Event Forwarding	19
Windows OS Version	19
Active Directory as Source for OS Version	19
File as Source for OS Version	20
Update Command	20
Source Hosts	21
Install the SmartConnector	22
Install Core Software	22
Run the SmartConnector	30
Customize Event Source Mapping	31
To Make it Work	31
Examples	31
Event Parsing in a Clustered Environment	31

Windows Event Forwarding	32
Specify Custom Log Names.....	33
Create and Deploy Parsers for System and Application Events	34
Configure Advanced Options	36
Advanced Common Configuration Parameters.....	36
Advanced Configuration Parameters per Host.....	37
Event Poll Count	37
Advanced Configuration Parameters for Automatic Host Browsing	37
Advanced Configuration Parameters for SID and GUID Translation.....	38
Advanced Configuration Parameters for Global Catalog.....	38
Troubleshooting	39
Problems with Random JCIFS Name when Installing on Linux	39
Why are RenameFileInTheSameDirectory and DeleteFile parameters not functioning as expected?	39
Problems reading event logs from Windows 2012 R2 systems (all versions up to 7.3.0)	39
Hung connector cannot collect events	40
Loss of host connectivity	40
Out of memory exceptions and missing events.....	41
Excessive Security:578 Success events generated.....	41
Untranslated SID values	42
Locked out account.....	42
Unable to create rpc handle.....	42
Optimize performance.....	42
Keys for security events.....	43
Cannot determine Microsoft OS version	45
Connector unable to process events.....	46
Remote/local machine event collection.....	46
Forwarded Event Collection.....	47

SmartConnector for Microsoft Windows Event Log – Unified

This guide provides information for installing the SmartConnector for Microsoft Windows Event Log – Unified and configuring the device for event log collection. This SmartConnector is supported for installation on all Windows, Linux, and Solaris platforms specified in the *SmartConnector Product and Platform Support* document.

ArcSight SmartConnectors provide easy, scalable, audit-quality collection of all logs from all event-generating sources across the enterprise for realtime and forensic analysis. The SmartConnector for Microsoft Windows Event Log – Unified is optimized for a large number of hosts.



This connector is designed to work with a large number of Windows hosts. If you experience any problems in the performance of this connector in an environment consisting of a large number of hosts, contact Micro Focus Software Support.

Product Overview

System administrators use the Windows Event Log for troubleshooting errors. Each entry in the event log can have a severity of **Error**, **Warning**, **Information**, and **Success** or **Failure** audit.

The SmartConnector for Microsoft Windows Event Log – Unified can connect to local or remote machines, inside a single domain or from multiple domains, to retrieve events from all types of event logs. This connector supports event collection from Microsoft Windows Vista, Server 2008, Server 2008 R2, Windows 7, Windows Server 2012, and Windows 8.



Note that Security events are not audited by default. Be sure to specify the type of security events to be audited (see "Enable Microsoft Windows Event Log Audit Policies" in this document).

See the appendix of this document for a comparison of features supported by the Windows Unified connector versus the Windows Domain connector.

See the supplemental Windows Event Log document *Windows 2008/2012 Security Event Mappings* for security event mappings to ArcSight fields.

Features and Enhancements

Specific features for the SmartConnector for Microsoft Windows Event Log – Unified include:

Operating Systems Supported

Support for Windows Event Log Security, System, and Application event collection from hosts running the following Microsoft OS versions:

- Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8

Collecting from Windows Event Collector Host

Support is provided for collecting events forwarded from source hosts to a Windows Event Collector (WEC) as well as from WEC hosts is available for these operating systems:

- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Events Supported

Windows Event Log parsing support for:

Event Type	Event Header	Event Description
Security	yes	yes
Application	yes	no*
System (Service Control Manager and WINS event sources)	yes	yes
Other System events	yes	no*

* However, support is provided for a Flex-Connector-like framework that lets users create and deploy their own parsers for parsing the event description for all system and application events. See "Create and Deploy Parsers for System and Application Events" later in this guide for more information.

NTLMv2 Authentication

Support for NTLMv2 authentication (see "[Configure NTLMv2 Authentication](#)" later in this guide).

Internationalization

Support for the localization of security events for the Simplified and Traditional Chinese, French, and Japanese languages. The locale can be specified during SmartConnector installation.

SID Translation

SID Translation: The SmartConnector for Windows Event Log – Unified can perform SID translation and is configured to translate SIDs by default. If the first SID translation attempt fails, the connector retries three times. If translation still fails, SID translation can be configured in multi-threaded mode. The number of SID translation threads to be pooled is configurable. The connector can also create new translation threads automatically when required.

- Translated values of SIDs are stored in caches with a configurable size for faster future accesses. Each domain has its own SID cache. SIDs for workgroup hosts are stored in a separate common cache.
- Translated values of SIDs can be expired from the caches at a configurable periodic interval. The time-to-live for each SID entry in the cache is also configurable. By default, the connector expires the entries of the unresolved SIDs only.

- Translated values of SIDs from the caches are persisted to disk files at a configurable periodic interval and also before the connector shuts down. Each domain's SID cache is persisted to a separate disk file. SID cache for workgroup hosts is persisted to a separate common disk file. This lets the connector load all the translated values of the SIDs from the disk files back to the memory caches when the connector restarts.
- The connector logs the most recently used unresolved SIDs in the status. Each domain's list of such SIDs is logged separately. SIDs for workgroup hosts are logged in a separate shared list.

GUID Translation

- The SmartConnector for Microsoft Windows Event Log – Unified can perform GUID translation for GUIDs within a forest by querying the Global Catalog Server. See "[Install the SmartConnector](#)" for more information about configuring the Global Catalog parameters. The connector is not configured to translate GUIDs by default. See "Advanced Configuration Parameters for SID and GUID Translation" for more information about enabling GUID translation.
- The connector translated GUIDs from events collected from domain hosts. The connector does not perform GUID translation for workgroup hosts.
- GUID translation is also supported in multi-threaded mode, which can be enabled or disabled. The number of GUID translation threads to be pooled is configurable. The connector can also create new translation threads automatically when required.
- Translated values of GUIDs are stored in a memory cache with a configurable size for faster future accesses.
- Translated values of GUIDs can be expired from the memory cache at a configurable periodic interval. The time-to-live for each GUID entry in the memory cache is also configurable. By default, the connector expires the entries of the unresolved GUIDs only.
- Translated values of GUIDs from the memory cache are persisted to a disk file at a configurable periodic interval and also before the connector shuts down. This lets the connector load all the translated values of the GUIDs from the disk files back to the memory caches when the connector restarts.
- The connector also logs the most recently used unresolved GUIDs in the status.

GUID translation with Global Catalog with SSL Connection

If GUID translation feature is enabled, and Global Catalog uses the Active Directory server parameters, SSL connection is assumed automatically if Active Directory has SSL connection enabled. If Global Catalog uses a different server, you can specify the correct parameters during connector installation and configuration with the Global Catalog configuration parameters. See step 6 in the "Install the SmartConnector" section of this guide.

Host Browsing

Host Browsing Feature during connector installation

The connector can discover and retrieve information about the hosts registered in an Active Directory using the Host Browsing feature. The host information includes the name of IP address along with its operating system version. This information is populated automatically in the connector Host Table parameters.

Automatic Host Browsing Feature when the Connector is running

The connector can be configured to discover and retrieve information about new hosts registered in an Active Directory while the connector is running. It sends an internal event notifying the user of the newly discovered host. The information in the internal event will include the device host name or IP address, along with its operating system version.

Host Browsing with SSL Connection

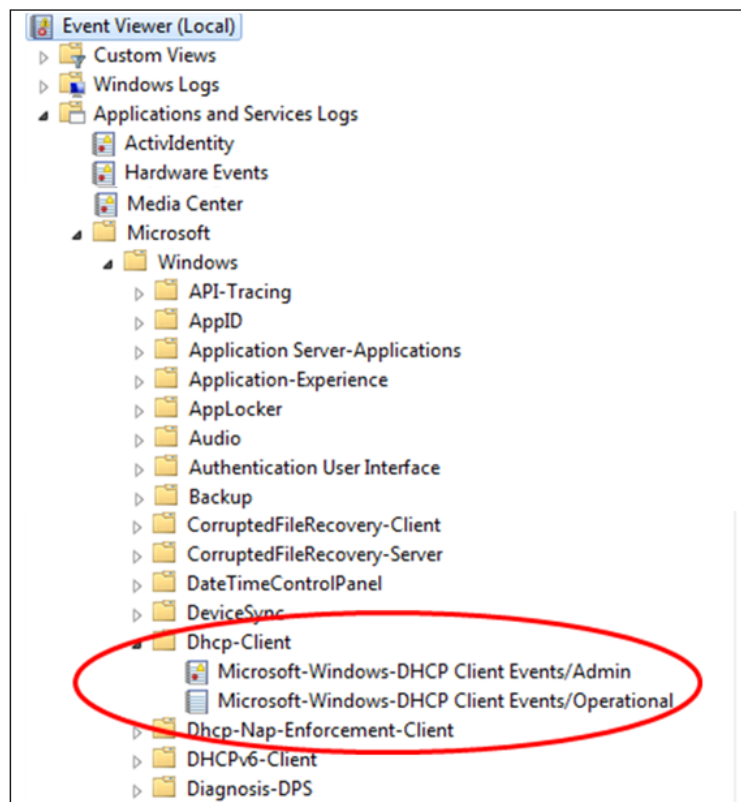
Since SmartConnector release 5.1.7, the Host Browsing feature has been available with SSL connections. To enable host browsing, first obtain and import certificates from your AD domain server, following certificate import instructions. Then enable the SSL connection and enter the appropriate port when filling in connector parameters. The default is port 636. See "[Add Security Certifications when Using SSL](#)" later in this guide.

Known Limitations

The following known limitations exist for the current release of this connector:

- The Microsoft Windows Event Log Unified connector currently is unable to collect and process events from nested event logs. If the connector is configured to collect from a nested log, it could retrieve random application or system logs, which may not be relevant to the configured log.

Nested event logs can be described as the event logs within **Application and Service Logs** in the Event Viewer, where the application logs are contained within a subsection or subdirectory structure as shown in the following figure.



- In some cases, the description of specific Windows events may not be captured into individual ArcSight event fields. When this is the case, the missing information is captured in the Raw Event field and the agent log displays a warning that it has received an unmatched number of keys and values for a particular Windows event ID. See the "[Keys for security events](#)" section in Troubleshooting for an example of how to resolve these key values.
- With Microsoft's security feature User Account Control (UAC) turned on, the connector cannot connect to the host or retrieve events with a local user. Use a domain user account to avoid this problem.
- SID translation is supported on a best-effort basis, but there may be a few instances when SIDs cannot be successfully translated. This could happen due to network issues, the host could be busy and may not respond, or the SID could be unresolvable, which results in the connector being unable to translate the SID. The connector attempts to translate all the SIDs by default. If the first translation attempt fails, the connector retries three times. If translation still fails, SID translation can be enabled in multi-threaded mode by setting the parameter `sidguidtranslationmultithreaded` to `true`. See "[Untranslated SID values](#)" in Troubleshooting or "[Advanced Configuration Parameters for SID and GUID Translation](#)" for more configuration information.
- Translation of GUIDs of deleted objects is not supported.

Configuration

Enable Microsoft Windows Event Log Audit Policies

Because event information generated by Windows servers is based upon which auditing policies are enabled, you should ensure the appropriate auditing policies are enabled on those Windows servers from which ArcSight will be collecting information. By default, none of the Windows auditing features are turned on.

When planning which events to audit, keep in mind that auditing events consumes system resources such as memory, processing power, and disk space. The more events you audit, the more of these resources are consumed. Auditing an excessive number of events may dramatically slow down your servers.



You must be logged on as an administrator or a member of the Administrators group to set up audit policies. If your computer is connected to a network, network policy settings might also prevent you from setting up audit policies.

The method used to create an audit policy varies slightly depending upon whether the policy is being created on a member server, a domain controller, or a stand-alone server.

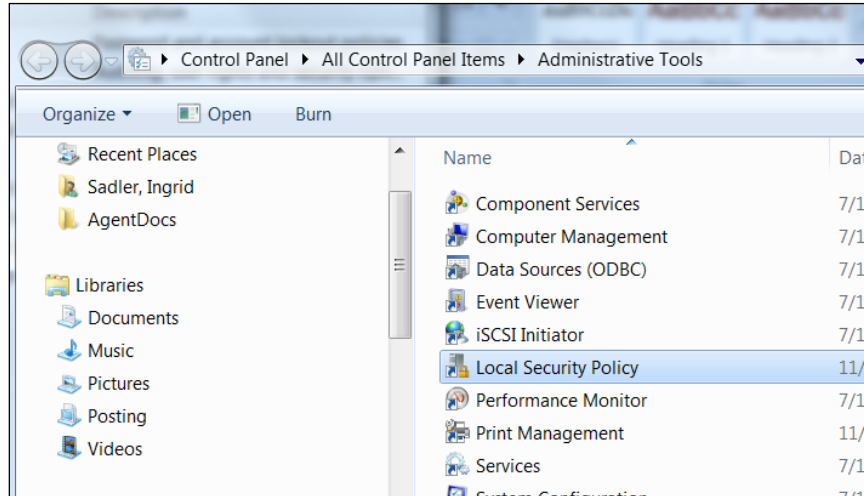
To configure a domain controller, member server, or workstation, use **Active Directory Users and Computers**.

To configure a system that does not participate in a domain, use **Local Security Settings**.

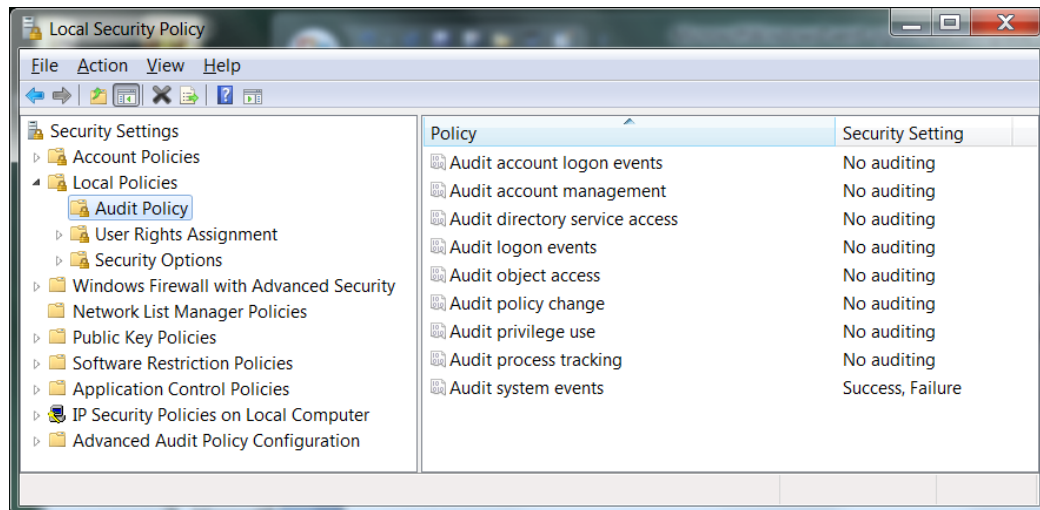
Audit a Local System

To establish an audit policy on a local system:

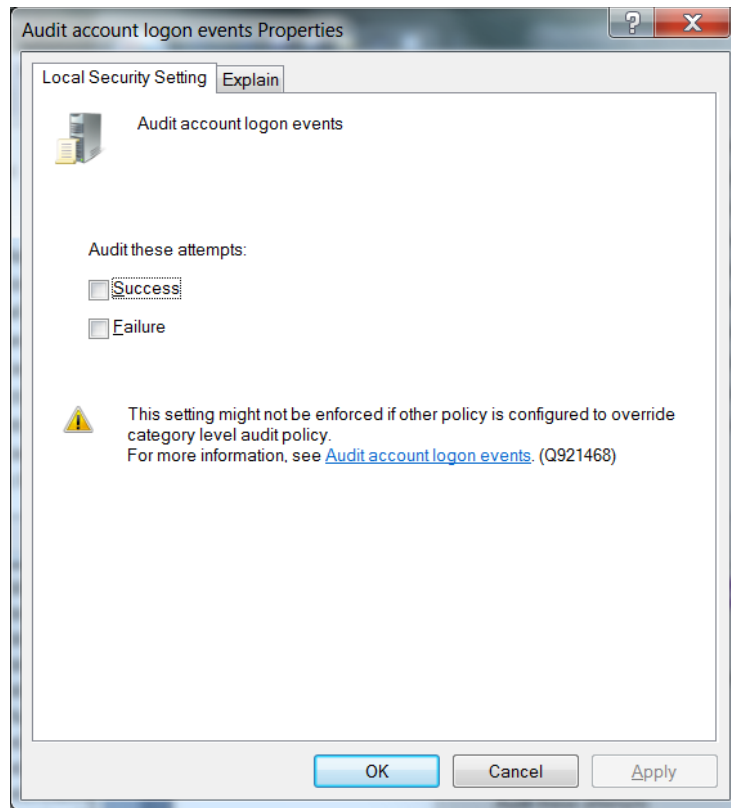
- 1 Select **Start -> Control Panel -> Administrative Tools -> Local Security Policy**.



- 2 Double-click on **Local Policy** in the **Security Settings** tree to expand it.



- 3 Select **Audit Policy** from the tree. Doing so reveals the auditing information for that system.
- 4 To enable auditing for any of the areas, double-click on the type of audit; a dialog box such as the following is displayed, letting you choose to perform a Success or a Failure audit (or both) on that type of event.



To audit objects such as the Registry, printers, files, or folders, select the **Object Access** option. Otherwise, when you attempt to enable auditing for these objects, an error is displayed instructing you to make the necessary adjustments to the local audit policy (or, in the case of a domain environment, to the domain audit policy).

Once you have enabled auditing, go through the system and fine-tune the type of events that will be audited in each category.

Audit Within a Domain

To set up an audit policy for a domain controller:

- 1 Choose **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.
- 2 Navigate through the console tree to the domain you want to work with. Expand the domain.
- 3 Beneath the domain, you will see a **Computers** object and a **Domain Controllers** object. Select the appropriate object for your system and right-click on **Domain Controllers**. The Domain Controller's properties sheet is displayed.
- 4 Select the **Group Policy** tab. Select the group policy to which you want to apply the audit policy and click **Edit**.
- 5 Navigate through the tree to **Default Domain Controllers Policy -> Computer Configuration -> Windows Settings -> Security Settings Local Policies -> Audit Policy**.

- 6 When you select **Audit Policy**, a list of audit events is displayed in the right pane. To audit a group of events, double-click on the group; a dialog box is displayed that lets you enable Success, Failure, or both audits for that group of events.

After enabling auditing for a group of events, fine-tune the exact events you want to audit.

Set Up an Audit Policy for a Domain

To set up auditing for all computers under a domain:

- 1 Click **Start -> Administrative Tools -> Domain Security Policy**.
- 2 Open **Default Domain Security Settings**.
- 3 Expand **Security Settings** if it is not already open.
- 4 Expand **Local Policy** and double-click on **Audit Policy**. A list of audit events is displayed in the right pane.
- 5 To audit a group of events, double-click on the group; a dialog box is displayed that lets you enable Success, Failure, or both audits for that group of events.

Set Up Standard User Accounts

Although a domain administrator account is required for system and custom application event collection (including Forwarded Events Collection), the SmartConnector for Microsoft Windows Event Log – Unified does not require domain administrator privileges to collect Security events from Windows hosts.

To let the SmartConnector for Microsoft Windows Event Log – Unified use a Standard User account to collect Security events only from the target hosts, follow the steps provided in the following sections.

These steps indicate how to configure and assign the privileges by creating a single user account such as 'arcsight'. You can also create a group of users instead and follow the same steps provided for the configuration, assigning all the minimum privileges to the user group instead of the single user.



Sometimes, although we have assigned appropriate privileges to the standard user, there could be other policies in your environment preventing the user account from accessing the security event logs. You can start identifying this problem by checking Settings -> Control Panel -> Administrative Tools -> Local Security Policy -> Security Settings -> Local Policies -> Security options. There are many security policies defined that would require investigation; however, one policy to check right away is the 'Network Access: Sharing and security model for local accounts'. Make sure this is set to 'Classic – local users authenticate as themselves'.

With Standard Domain User Account

From Windows Server 2008/2012 Domain Controllers

On the Windows Server 2008 Domain Controller:

- 1 Go to **Settings -> Control Panel -> Administrative Tools -> Active Directory Users and Computers -> {Domain of interest} -> Users**.
- 2 Create a new Domain User, such as **arcsight**.

- 3 Go to **Settings -> Control Panel -> Administrative Tools -> Active Directory Users and Computers -> {Domain of interest} -> BuiltIn**.
- 4 Open the properties of the security principal **Event Log Readers**.
- 5 From the **Members** tab, add this new Domain User **arcsight** to this security principal.
- 6 This Group Policy may take some time to take effect. To bring it into effect faster, run the following command at the command prompt: `GPUpdate /Force`. Be aware that modifications to any group policy being made at the same time will also go into effect.

From Windows Vista Domain Members

On the Windows Server 2008/2012 Domain Controller:

- 1 Go to **Settings -> Control Panel -> Administrative Tools -> Active Directory Users and Computers -> {Domain of interest} -> Users**.
- 2 Create a new Domain User, such as **arcsight**.
- 3 Go to **Settings -> Control Panel -> Administrative Tools -> Group Policy Management -> Default Domain Policy -> Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment**.
- 4 Open the **Manage auditing and security log** policy.
- 5 Enable **Define these Policy Settings** and add this new Domain User **arcsight** to this policy.
- 6 This Group Policy may take some time to take effect. To bring it into effect faster, run the following command on the command prompt: `GPUpdate /Force`. Be aware that modifications to any group policy being made at the same time will also go into effect.

On the Windows Vista Domain Member:

- 1 To bring the Group Policy into effect faster, run the following command on the command prompt: `GPUpdate /Force`. Be aware that modifications to any group policy being made at the same time will also go into effect.

With a Standard Local User Account from Windows Vista Workgroup Hosts

On the Windows Vista Workgroup host:

- 1 Go to **Settings -> Control Panel -> Administrative Tools -> Computer Management -> System Tools -> Local Users and Groups -> Users**.
- 2 Create a new Local User, such as **arcsight**.
- 3 Go to **Settings -> Control Panel -> Administrative Tools -> Computer Management -> System Tools -> Local Users and Groups -> Groups**.
- 4 Open the **Event Log Readers** group and add this new Local User **arcsight** to this group.
- 5 Go to **Settings -> Control Panel -> Administrative Tools -> Local Security Policy -> Security Settings -> Local Policies -> Security Options**.

- 6 Open the **Network access: Sharing and security model for local accounts** policy.
- 7 Set this policy to the option: **Classic – local users authenticate as themselves**.

Configure NTLMv2 Authentication

The connector now provides support for NTLMv2 authentication, which can be configured by the security policy **Network security: LAN Manager authentication level**. This security policy setting determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers as follows:

- **Send LM & NTLM responses:** Clients use LM and NTLM authentication and never use NTLMv2 session security; domain controllers accept LM, NTLM, and NTLMv2 authentication.
- **Send LM & NTLM - use NTLMv2 session security if negotiated:** Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLMv2 authentication.
- **Send NTLM response only:** Clients use NTLM authentication only and use NTLMv2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLMv2 authentication.
- **Send NTLMv2 response only:** Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLMv2 authentication.
- **Send NTLMv2 response only\refuse LM:** Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers refuse LM (accept only NTLM and NTLMv2 authentication).
- **Send NTLMv2 response only\refuse LM & NTLM:** Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers refuse LM and NTLM (accept only NTLMv2 authentication).

Default values:

On servers and domain members, send LM & NTLM responses

On workstations, undefined

The connector provides support for all authentication levels.

- In order to change the authentication level, the security policy **Network security: LAN Manager authentication level** can be set by following the path on the Windows host as follows:
- **Managing it as a Group Policy for the entire domain on a Windows Server Domain Controller:** `Settings -> Control Panel -> Administrative Tools -> Group Policy Management -> Default Domain Policy -> Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> Network Security -> Policy`

- **Managing it as a Local Security Policy on Windows Servers:** Settings -> Control Panel -> Administrative Tools -> Local Security Policy -> Security Settings -> Local Policies -> Security Options
- **Managing it as a Local Security Policy on Windows Vista:** Settings -> Control Panel -> Administrative Tools -> Local Security Policy -> Security Settings -> Local Policies -> Security Options

Important:

By upgrading the connector to this released version, the connector will be using an updated authentication package to support NTLMv2 authentication. If authentication for any host fails for your existing connector configuration, see the "[Install the SmartConnector](#)" section for more information. If you still have any issues with authentication, contact Micro Focus SSO.

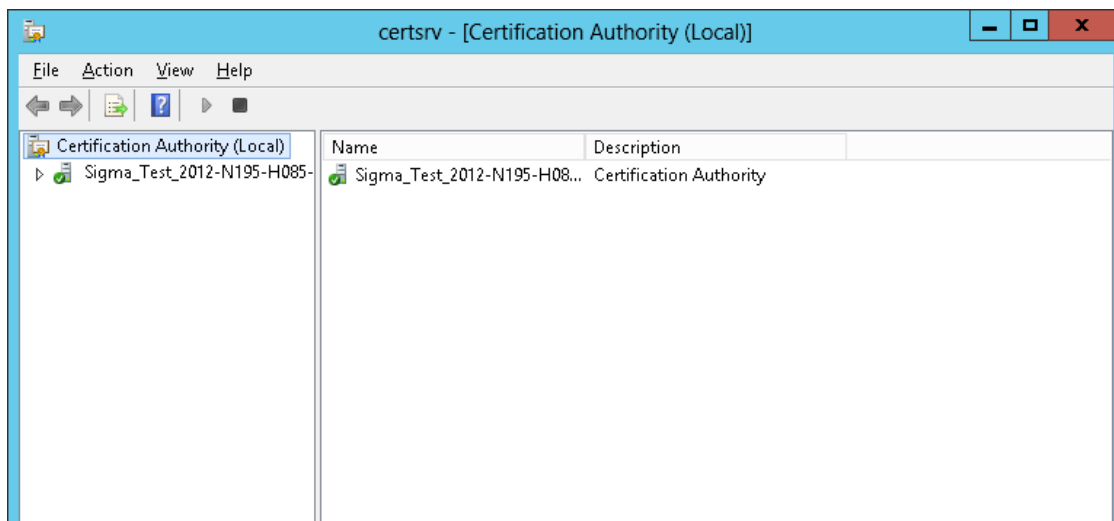
Add Security Certifications when Using SSL

If you choose to use SSL as the connection protocol, you will be required to add security certificates for both the Windows Domain Controller Service and for the Active Directory Server. Installing a valid certificate on a domain controller permits the LDAP service to listen for, and automatically accept, SSL connections for both LDAP and global catalog traffic.

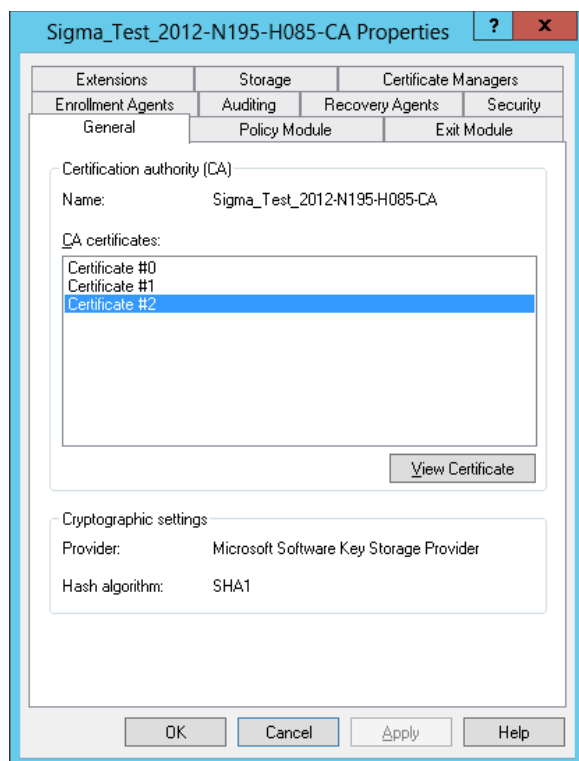
The following steps assume Windows Server 2012 as the operating system; steps may vary with different Windows versions.

To export the certificates:

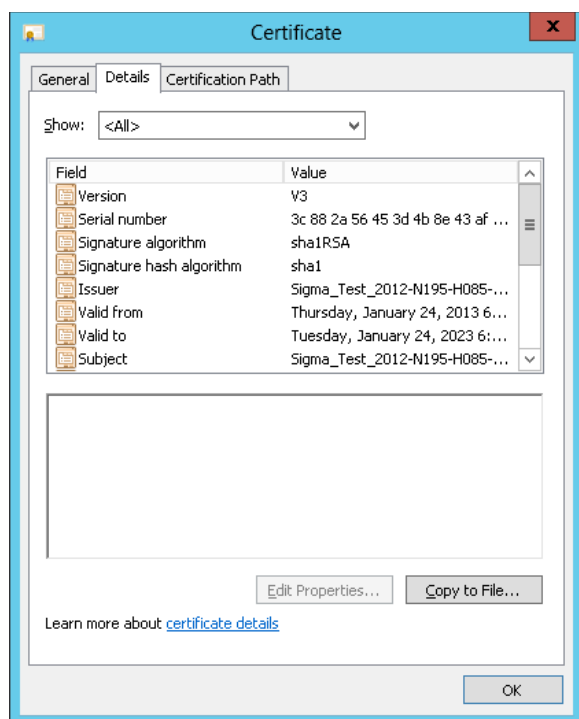
1. From the Windows **Start** menu, select **Administrative Tools**.
2. Select and double-click **Certification Authority**; one or more Domain Certificate Authority servers are shown.



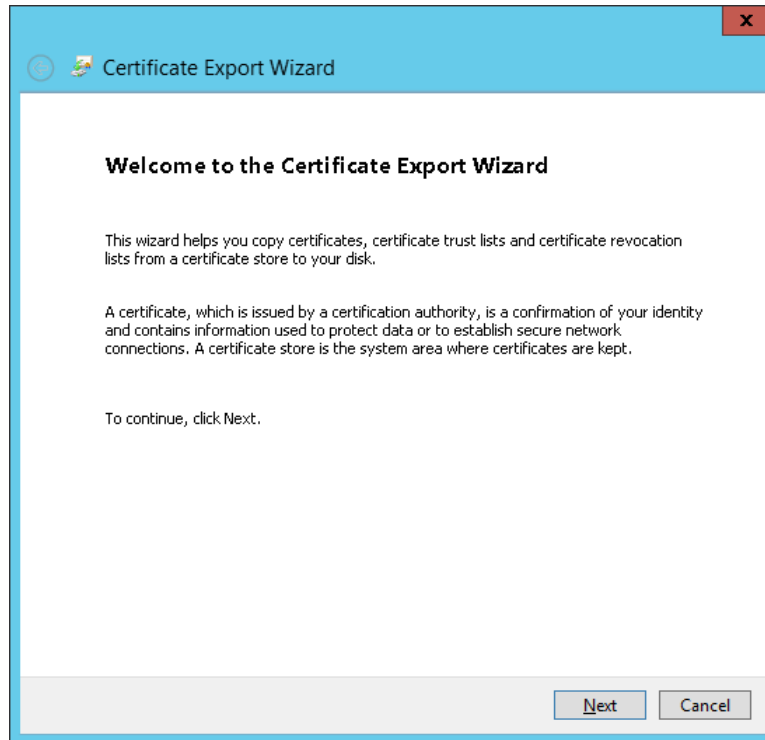
3. Select the Domain Certificate Authority server for the domain to which the Active Directory server belongs, right-click, and select **Properties** to open the Properties window.



4. Click **View Certificate**
5. Click the **Details** tab, and **Copy to File...**



6. Follow the steps in the Certificate Export wizard to complete the export.



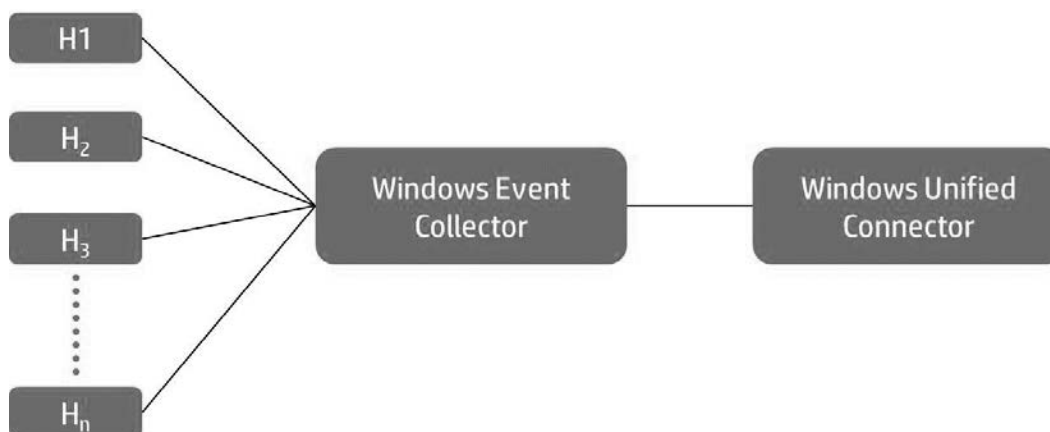
Collect Forwarded Events

The SmartConnector for Microsoft Windows Event Log – Unified provides a feature to read events forwarded to a Windows Event Collector host. Event forwarding is a Microsoft technology that lets a host collect events from multiple sources. Collecting forwarded events is somewhat different than the traditional event collection because the events are from multiple sources.

With Microsoft Windows Event Collector, you can subscribe to receive and store events on a local computer (event collector) that are forwarded from a remote computer (event source). Before using this feature, read about Windows Event Collector to understand how it works in the Microsoft Windows documentation.

Windows Event Forwarding Use Case

The Windows Event Log Unified connector can be used for collecting and processing events from a Windows Event Collector. This is illustrated in the following figure.



Collection of Forwarded Events using Windows Event Log Unified Connector

The Windows Event Collector host in the figure refers to the host that collects events from other (event source) hosts.

Event Collector for Windows Event Forwarding

You can forward events from a source host to any log type on the collector machine to which the Unified connector would normally have access. Micro Focus recommends that you forward application events to Application and system events to System.



Security events cannot be forwarded to Security on a collector machine, but can be forwarded to other types. Micro Focus supports using HardwareEvents as the default destination. The ForwardedEvents specification is not currently in use. During connector configuration, enable Forwarded Events Collection and add HardwareEvents to the Custom Log Names field.

Windows OS Version

When processing the Windows event, the Windows OS version of the event source host must be known by the Windows Unified connector as the event format can be different across different Windows OS versions. In the traditional Unified connector, the Windows OS version is provided through the configuration wizard as the events are directly collected from the event source host.

However, when the events are collected from a Windows Event Collector (WEC) host, the event source host may not be the same version as the host from which the events are collected. Therefore, the event source host information needs to be provided to the connector. There are two ways to do this. One is to provide the host name as well as the Windows OS version information in a file, and another is through Active Directory. If the Windows OS version is not specified or specified incorrectly, Windows 2008 R2 is used.

Active Directory as Source for OS Version

When this selection is chosen during connector configuration, the connector pulls the host information (host name and version) from the configured Active Directory to identify the event source host Windows version information. Automatic host browsing discovers newly added hosts, hence a newly added host is managed automatically without reconfiguring the connector itself.

Active Directory information is checked upon connector startup and every 24 hours. (To change the time setting, locate the `agent.properties` file and modify the `hostbrowsingthreadsleeptime` to set it to the number of milliseconds between host browsing queries.)

In order for the Windows Event Log Unified connector to be able to browse the Active Directory to retrieve source host Windows version information (required for parsing the events correctly), the connector should be placed within the same forest as the collector hosts.

File as Source for OS Version

When this selection is chosen during connector configuration, make sure you have created a source hosts file (specifying the source host information, including full name and version), named it as `sourcehosts.csv`, created a windows subdirectory at `$ARCSIGHT_HOME/user/agent/` and copied the file to the windows subdirectory.

The `$ARCSIGHT_HOME/user/agent` directory is installed during the connector installation and configuration process; when you see the screen for selecting “Add a connector”, create a windows subdirectory at `$ARCSIGHT_HOME/user/agent` and copy the `sourcehosts.csv` file into this directory before continuing connector configuration.

An example of the source hosts file could be:

```
hostsa.domaina.com,Windows 7
hostsb.domainb.com,Windows 8
hostsc.domainb.com,Windows 2012
```

If Active Directory is used as the source, providing a source host file is optional as the Windows Unified connector can update the host information via LDAP query (when Active Directory credentials are available and browsing is allowed for WEC sources).

Update Command

You can update hosts on the ArcSight Console (from **Connector Command** tab, **Send Command -> Windows Unified Commands -> Collect Source Hosts, Info Updates**) when you have made changes to the `sourcehosts.csv` file and the updated information to be added to memory for the connector. For the Connector Appliance, select the **Windows Unified Commands/Collector Service Hosts, Info Update** command from the **Destination Commands** tab.

Connector Appliance

When running the connector from Connector Appliance, to use a `sourcehosts.csv` file, create a new repository with this file and apply to the appropriate container. Note that you should **NOT** check **Delete before upload** if the **Delete relative path** field is blank as the contents of the `user/agent` directory will be deleted.

The screenshot shows the 'Edit WEF no AD Setting' dialog box. The left sidebar contains a tree view with 'Logs' (CA Certs, Upgrade AUP, Content AUP, Remote Management AUP, Emergency Restore) and 'Repositories' (+ New Repository, WEF no AD, Backup Files, Map Files, Parser Overrides, Flex Connector Files, Connector Properties, JDBC Drivers). The main area is titled 'Edit WEF no AD Setting' and contains the following fields:

- Name: **windows**
- Display name: WEF no AD
- Item display name: sourcehosts.csv
- Recursive: ☐
- Sort priority: -1
- Restart connector process: ☐
- Filename prefix: sourcehosts
- Download**
 - Relative path:
 - Include regular expression:
 - Exclude regular expression:
- Upload**
 - Delete before upload: ☐
 - Delete groups: ☐
 - Relative path:
 - Delete relative path:
 - Delete include regular expression:
 - Delete exclude regular expression:
- Cancel button

For more information, see the *Connector Appliance Administrator's Guide*.

Source Hosts

The source host version information is loaded from the source file, and from LDAP query. Any time a duplicate entry is found, the host version information is overwritten by the later operation.

Windows OS Versions recognized by the connector when reading from sourcehosts.csv are:

- Windows Vista
- Windows Server 2008 | Windows Server 2008 R2
- Windows 7
- Windows 8
- Windows Server 2012 | Windows Server 2012 R2

In addition, the connector will attempt to recognize the following strings in the source file to match them with the actual name:

- Vista
- 2008
- 2008 R2
- 7
- 8
- 2012
- 2012 R2

Install the SmartConnector

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). This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

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 the connector to the ArcSight Management Center (ArcMC), 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

If you will be using Forwarded Event Collection, note the following:

- The full computer name and OS version of source hosts must be available for use either through Active Directory or a `sourcehosts.csv` file. See [Active Directory as Source for OS Version](#) and [File as Source for OS Version](#) for more information.
- MICRO FOCUS recommends that, for best performance, the Unified connector be installed locally on the Windows Event Collector host and be configured with one forwarded event log.

Install Core Software

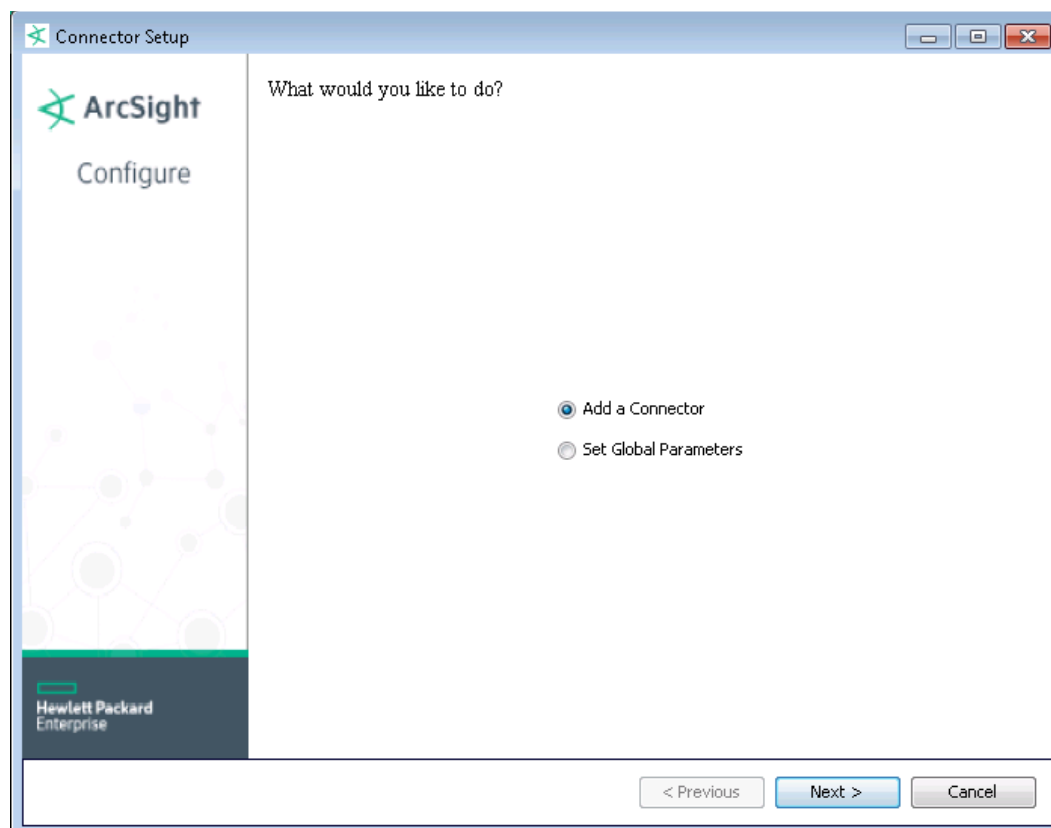
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the MICRO FOCUS SSO and Protect 724 sites.

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

Follow the installation 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.



If you select Set Global Parameters and want to perform any of the operations shown in the following table, do so before adding your connector. After installing core software, you can set the following parameters:

Global Parameter	Setting
Set FIPS mode	Not applicable.
Set Remote Management	Set to 'Enable' 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 'Disable'.
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	Only IPv4 is supported with this connector.

If you are using SSL for connector connection, follow these steps; otherwise, continue with step 4.

To import the certificates to the connector's certificate store, click **Cancel** to exit the wizard:

- A From `$ARCSIGHT_HOME\current\bin`, execute the **keytool** application to import the two certificates (see "Add Security Certifications when Using SSL" earlier in this guide):

```
arcsight agent keytoolgui
```

The graphical interface asks you to open a keystore.

- B** Select `jre/lib/security/cacerts`, then select `import cert` to import your certificate. Verify that the correct certificate has been imported.

- C** When prompted **Trust this certificate?**, click **Yes**.

Repeat this process for the second certificate.

- D** Save the keystore.

- E** Verify the imported certificates by entering this command from `$ARCSIGHT_HOME\current\bin`:

```
arcsight agent keytool -list -store clientcerts
```

The new certificates are listed.

- F** Return to the configuration wizard by executing the `runagentsetup` command from `$ARCSIGHT_HOME\current\bin`.

- 4** Select **Add a Connector** and click **Next**. Note that the parameters in “Set Global Parameters” are not applicable for this connector.)



When using a `sourcehosts.csv` file to import your host information during connector configuration, create a windows subdirectory at `$ARCSIGHT_HOME/user/agent/` and copy the `sourcehosts.csv` file into that directory at this point.

- 5** The Configuration Wizard displays a list of available SmartConnectors you can configure. Select **Microsoft Windows Event Log – Unified** and click **Next**
- 6** Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.
 - A** Enter the credentials of the user account that will be used to collect Windows events from the target hosts in the window displayed. The domain name, user name, and password fields entered in this step will be used by default for all the configured target hosts, unless they are specified to use a different user account in step 9D.

Parameter	Description
Forwarded Events Collection	<p>Select Disable when you are not using Windows Event Forwarding.</p> <p>Select Enable, use AD for sources for the connector to pull the host information from the configured Active Directory to identify the event source host.</p> <p>Select Enable, do not use AD for source when source hosts information is provided through a source hosts file with the name <code>sourcehosts.csv</code> in the <code>\$ARCSIGHT_HOME/user/agent/windows</code> directory.</p> <p>For more information, see “Collect Forwarded Events”.</p>
Domain Name	Enter the name of the domain to which the host belongs. If you are using a Domain User account for a target host, fill in the Domain Name field. If you are using a Local User account for the target host, leave the Domain Name field blank. If the target host is a Workgroup host that does not belong to a domain, leave the Domain Name field blank.
Domain User Name	Enter the name of the user account with adequate privileges to collect Windows events from the target host. This will be the user name only, without the domain
Domain User Password	Enter the password for the user specified in Domain User Name.
Active Directory Server	Enter the Active Directory Host Name or IP address required for authentication to the MS Active Directory for the Host Browsing feature
Active Directory Base DN	<p>Enter the Active Directory Base DN, which is required for automatic host browsing. The Base DN is the starting point in the MS Active Directory hierarchy at which the search is to begin. It can contain Common Names (cn), Organizational Units (ou), and Domain Components (dc).</p> <p>Some examples are:</p> <pre>dc=mydomain,dc=com</pre> <pre>ou=California,ou=West Coast,dc=MySubDomain,dc=MyDomain,dc=com</pre>

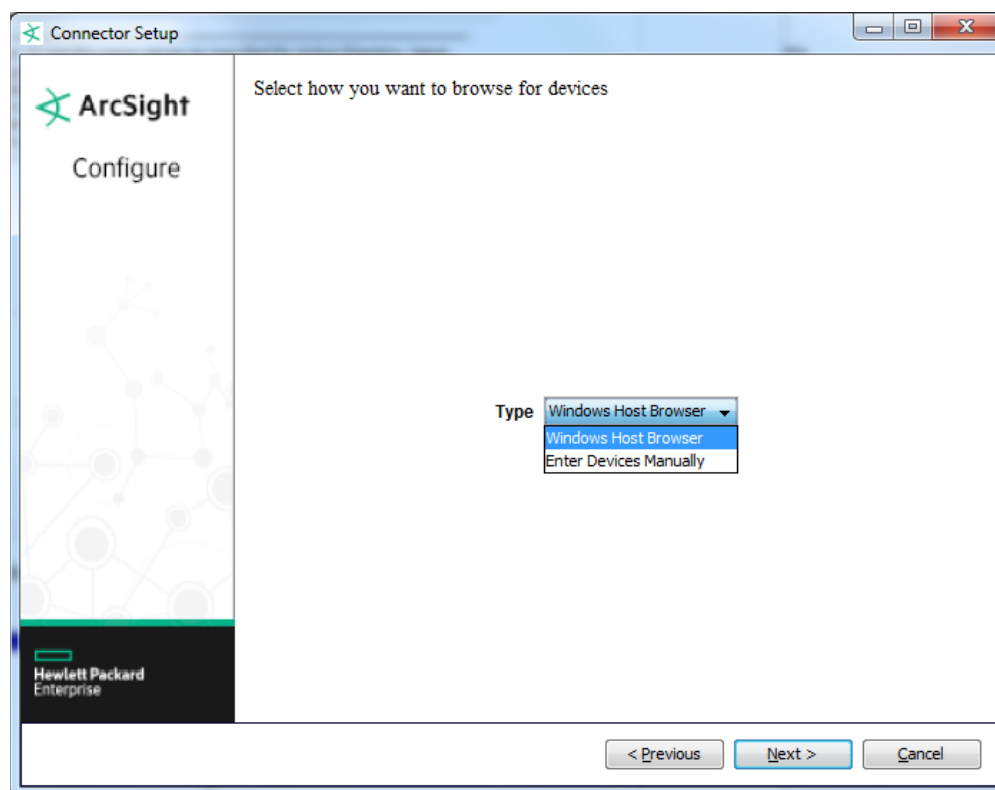
Parameter	Description
Active Directory Filter	<p>Enter the Active Directory Filter required for automatic host browsing to filter hosts by name, operating system, and creation time.</p> <p>The filter can contain attributes for Common Names (cn), Operating System (operatingsystem) and Creation Time (whencreated) in 'YYMMDDHHmmSSZ' format, where YY=Last two digits of the year, MM=Month, DD=Date, HH=Hours, mm=Minutes, SS=Seconds in 24-hour format.</p> <p>The filter can also contain wildcard characters (*) to match the attributes to different values.</p> <p>This filter is reused when "Enable, use AD for sources" is selected during connector configuration of the Forwarded Events Collection feature. See "Collect Forwarded Events" for more information.</p> <p>Examples:</p> <ul style="list-style-type: none"> To get all hosts created at any point of time, use the default filter, which is set to <code>(&(cn=*)(operatingsystem=*)(whencreated=*))</code> To get hosts with host name starting with the letter 'a', and created at any point of time, set the filter to <code>(&(cn=a*)(operatingsystem=*)(whencreated=*))</code> To get hosts created at a specific point of time, set filter to <code>(&(cn=*)(operatingsystem=*)(whencreated~='YYMMDDHHmmSSZ'))</code> To get hosts created after and inclusive of a specific point in time, set filter to <code>(&(cn=*)(operatingsystem=*)(whencreated>='YYMMDDHHmmSSZ'))</code> To get hosts created between and inclusive of two specific points in time, set filter to <code>(&(cn=*)(operatingsystem=*)(whencreated>='YYMMDDHHmmSSZ')(whencreated<='YYMMDDHHmmSSZ'))</code> To get hosts with host name containing the letter 'a', and created between and inclusive of the two timestamps '2009/07/01 00:00:00' and '2009/08/1 00:00:00', set filter to <code>(&(cn=*a*)(operatingsystem=*)(whencreated>=090701000000Z)(whencreated<=090801000000Z))</code>
Active Directory User Name	Enter the Active Directory User Name for access to Active Directory. This is required for authentication to the MS Active Directory for the Host Browsing feature.
Active Directory User Password	Enter the password associated with the Active Directory User Name. This is required for authentication to the MS Active Directory for the Host Browsing feature.
Active Directory Protocol	<p>Select whether the protocol to be used is non_ssl (the default value) or SSL.</p> <p>Note: For SSL protocol, be sure to import the Active Directory security certificate to the connector before starting the connector. See "Add Security Certifications when Using SSL" for more information.</p>
Active Directory Port	<p>Enter the port number to which the connector will listen: the default for the non_ssl protocol is 389; the default for the SSL protocol is 636.</p> <p>Note: For SSL protocol, be sure to import the Active Directory security certificate to the connector before starting the connector. See "Add Security Certifications when Using SSL" for instructions.</p>
Active Directory Max Page Size	Enter a maximum page size for the Active Directory query. This lets the connector read all hosts by repeating query for max page size hosts as many times as needed. The default value is 300.

Parameter	Description
Global Catalog Server	Global Catalog Server IP or Host Name is required for GUID translation. <i>To use the Active Directory Server as the Global Catalog Server, leave this field empty.</i>
Global Catalog Base DSN	Global Catalog Base DN is required for GUID translation. <i>To use the Active Directory Base DN as the Global Catalog Base DN, leave this field empty.</i>
Global Catalog User Name	Global Catalog User name required for GUID translation. This can be a Domain Admin User or even a Standard Domain User. <i>To use the Active Directory User Name and Active Directory User Password as the Global Catalog User Name and Global Catalog User Password, respectively, leave this field empty.</i>
1. Global Catalog User Password	2. Global Catalog User Password required for GUID translation. <i>To use the Active Directory User Name and Active Directory User Password as the Global Catalog User Name and User Password, respectively, leave the Global Catalog User Name field empty.</i>



For Global Catalog user information, to use the same values as specified for Active Directory, leave the Global Catalog parameters empty. To use differing user information for the Global Catalog, in addition to specifying the Server, Base DSN, User Name, and User Password, you can access the connector's advanced parameters to specify Global Catalog Protocol as needed. See "Advanced Configuration Parameters for Global Catalog" later in this guide. The port (3268 for non-ssl) will adjust automatically to standard SSL connection port for Global Catalog, which is 3269.

- B** To enter devices manually, select **Enter Devices Manually** and click **Next** to continue. Then continue with step **D**.



For ease of configuration, if you have relatively few Windows Events Collector hosts from which you will collect events, enter hosts manually rather than use the Host Browsing feature.

- C** Select **Windows Host Browser** if you want to populate the parameter entry table automatically with a list of all the hosts located within the domain specified in the first parameter entry window



The Host Browser feature will only fill the Host Name and the Microsoft OS Version fields. The Domain Name, Username, and Password fields will not be populated since these hosts will use the default user account credentials configured in step 9A. You can fill in these fields if you need to override the credentials with another user account.

- D** Click **Add** and fill in the required fields.

For a host, when the domain name, user name, and password fields are all empty in the host table, the default domain name, user name, and password will be used for such hosts.

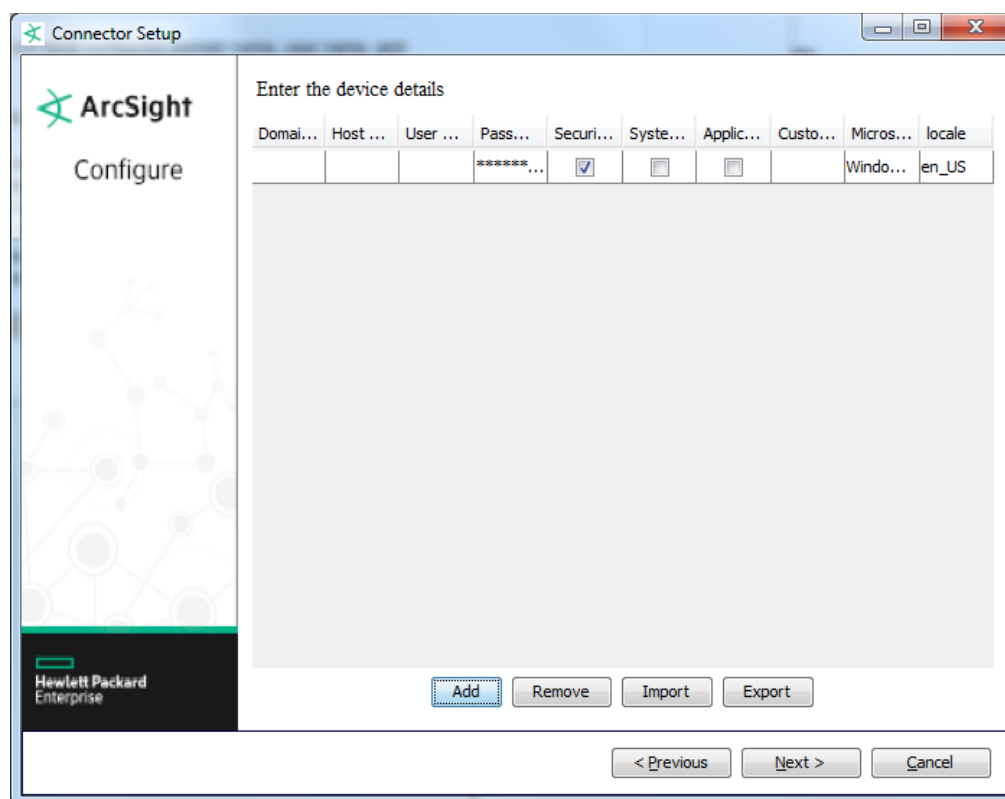
For a host, when the domain name is configured in the host table but the user name and password fields are empty, the host table domain name (with the domain user name and password as provided in the first step of configuration) will be used. This is useful when configuring hosts from different domains that have the same domain user name and password.

For a host for all other cases, the host table configured domain name, user name, and password will be used.

When using Forwarded Event Collection, specify only the Event Collector hosts.

You can click the 'Export' button to export the host name data you have entered into the table into a CSV file; you can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. When importing, there should be a carriage return (only one CR) at the last entry in the .csv file otherwise the import may not work.

Note that, with the new column for Custom Log Names, the number of columns is now different than with previous release of this connector; however, as long as the header is provided correctly, backward compatibility should not be an issue. See the *SmartConnector User's Guide* for more information.



Parameter	Description
Domain Name	Name of the domain to which the host belongs. If you are using a Domain User account for a target host, fill in the Domain Name field. If you are using a Local User account for the target host, leave the Domain Name field blank. If the target host is a Workgroup host that does not belong to a domain, leave the Domain Name field blank.
Host Name	Host name or IP address of the target Windows host.
User Name	Name of the user account with adequate privileges to collect Windows events from the target host. This will be the user name only, without the domain.
Password	Password for the user specified in User Name.
Security Logs	Select 'true' for security events to be collected from this host; select 'false' if you do not want to collect security events. The default value is 'true.'
System Logs	Select 'true' for system events to be collected from this host; select 'false' if you do not want to collect system events. The default value is 'false.'
Application	Select 'true' for application events to be collected from the Common Application Event Log of this host; select 'false' if you do not want to collect such application events. The default value is 'false.'
Custom Log Names	Specify the custom application log names, separated by a comma (such as "Exchange Auditing, Directory Service"). For Windows Event Collector servers, use "HardwareEvents". Note that "ForwardedEvents" is not currently supported. See Specify Custom Log Names for more information.
Microsoft OS Version	Select the Microsoft Operating System version this host is running.
locale	Enter the code for your locale; possible values are 'en_US' (United States English), 'ja_JP' (Japanese), 'zh_CN' (Simplified Chinese), 'zh_TW' (Traditional Chinese), 'fr_CA' (French). The default value is 'en_US'.

- 7 Make sure **ArcSight Manager (encrypted)** is selected and click **Next**. For information about the other destinations listed, see the *ArcSight SmartConnector User Guide* as well as the Administrator's Guide for your ArcSight product.
- 8 Enter the **Manager Host Name**, **Manager Port**, and a valid ArcSight **User Name** and **Password**. This is the same user name and password you created during the ArcSight Manager installation. Click **Next**.
- 9 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.
- 10 The certificate import window for the ESM 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.

- 11 Review the **Add connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.
- 12 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 12. If you choose to run the connector as a service, the wizard prompts you to define service parameters.
- 13 Enter the service parameters and click **Next**. The **Install Service Summary** window is displayed.
- 14 Click **Next**.
- 15 To complete the installation, choose **Exit** and click **Next**.

For some SmartConnectors, a system restart is required before the configuration settings you made take effect. If a **System Restart** window is displayed, read the information and initiate the system restart operation.



Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

Complete any additional configuration required, such as customizing mapping, then continue with "Run the SmartConnector".

For connector upgrade or install instructions, see the *ArcSight SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in standalone 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 installed standalone, the SmartConnector must be started manually, and is not automatically active when a host is re-started. If installed as a service or daemon, the SmartConnector runs automatically

when the host is re-started. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User's Guide*.

For connectors installed standalone, to run all installed SmartConnectors 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.

Customize Event Source Mapping

The Windows Event Log Unified application/system event parser loading mechanism relies on the event source for each event and attempts to load a parser with the following name convention

```
event_log_type.event_source_name.sdkkeyvaluefilereader.properties
```

This convention works in the vast majority of cases but sometimes must be made a bit more flexible. For that purpose, a solution has been introduced that lets you customize where to find these parsers by redirecting these two variables (event log type and event source name). For even more flexibility, the input event source name can be matched against a regular expression to avoid duplicate entries with minimal changes.

To Make it Work

Navigate to `$ARCSIGHT_HOME/current/user/agent/fcp/windowsfg/` and create an override map file with the name `customeventsource.map.csv` with the following four columns (if you already have a map file from a previous connector version, no changed is needed):

```
Original_Event_Log_Type, Original_Event_Log_Source, Target_Event_Log_Source, Target_Event_Log_Type
```

The `Original_Event_Log_Source` value can be a string or a regular expression.

If there is no `windowsfg` subdirectory at `$ARCSIGHT_HOME/current/user/agent/fcp`, create one.

The last field `Target_Event_Log_Type` is optional and, if empty, will be understood as the same as `Original_Event_Log_Type`.

Note that the map file is not provided in the Windows version-specific folder. Rather it is generic and the appropriate Windows version-specific parser is loaded automatically based upon the host version for the event. See the following for examples of why and how to use this feature.

Examples

Event Parsing in a Clustered Environment

The default parser filename convention can cause a problem in clustered environments, where the same event from different clusters can have different customized event source names. For example, SQL Server application events have the source names as `MSSQLSERVER`, resulting in the parser name as `application.mssqlserver.sdkkeyvaluefilereader.properties`.

In a clustered environment for SQL Server installations, you can customize and configure the event source names for each cluster as `SQLSERVER01`, `SQLSERVER02`, and so on. The connector is

expecting MSSQLSERVER, so the default parser as above will not be loaded, causing the parsing to fail for the events with event source names SQLSERVER01 and SQLSERVER02.

With the `customeventsource.map.csv` file, you can overcome this challenge easily by funneling all these source names into one. Example entries based on the above clustered environment are:

```
Application, MSSQLSERVER01, MSSQLSERVER, Application
```

or

```
Application, MSSQLSERVER\d*, MSSQLSERVER, Application
```

or

```
Application, MSSQLSERVER.*, MSSQLSERVER , Application
```

The complete contents of a sample `customeventsource.map.csv` file with two entries may appear as:

#Original_Event_Log_Type	Original_Event_Log_Source	Target_Event_Log_Source	Target_Event_Log_Type
System,	Service.*,	service_control_manager,	System
Application,	MSSQLSERVER.*,	MSSQLSERVER,	Application

Windows Event Forwarding

The default installation of the connector's Windows event forwarding support should get you through our recommended use of forwarding, with Security events going to your collector's HardwareEvents log, and the remainder going to their corresponding twin destination. But if your Windows event forwarding setup is different, for instance if you send all forwarded events to HardwareEvents, you must add that customization to `customeventsource.map.csv` to avoid any issue. . Note that ForwardedEvents is not currently supported as Original Event Log Type.

For example, your mappings could look like:

#Original_Event_Log_Type	Original_Event_Log_Source	Target_Event_Log_Source	Target_Event_Log_Type
HardwareEvents,	Service.*,	service control manager,	System
HardwareEvents,	dhcp.*,	DHCP,	System
HardwareEvents,	Microsoft Forefront.*,	Microsoft_forefront_protection,	Application
HardwareEvents,	FSCController,	fsccontroller,	Application
HardwareEvents,	FSCVSSWriter,	fscvsswriter,	Application
MyFwdSecurityLog,	.*,	security,	Security

This is assuming that you have the appropriate parsers corresponding to the target file name according to the convention, if they are not already present in the default SmartConnector installation.

Note that you can also use this map file to declare a forwarding destination for security events that is not the HardwareEvents supported by default.

For reference, here is the base table used by a default connector installation (which you also can override if need be) to be able to collect and process forwarded Security events using the existing Security parsers.

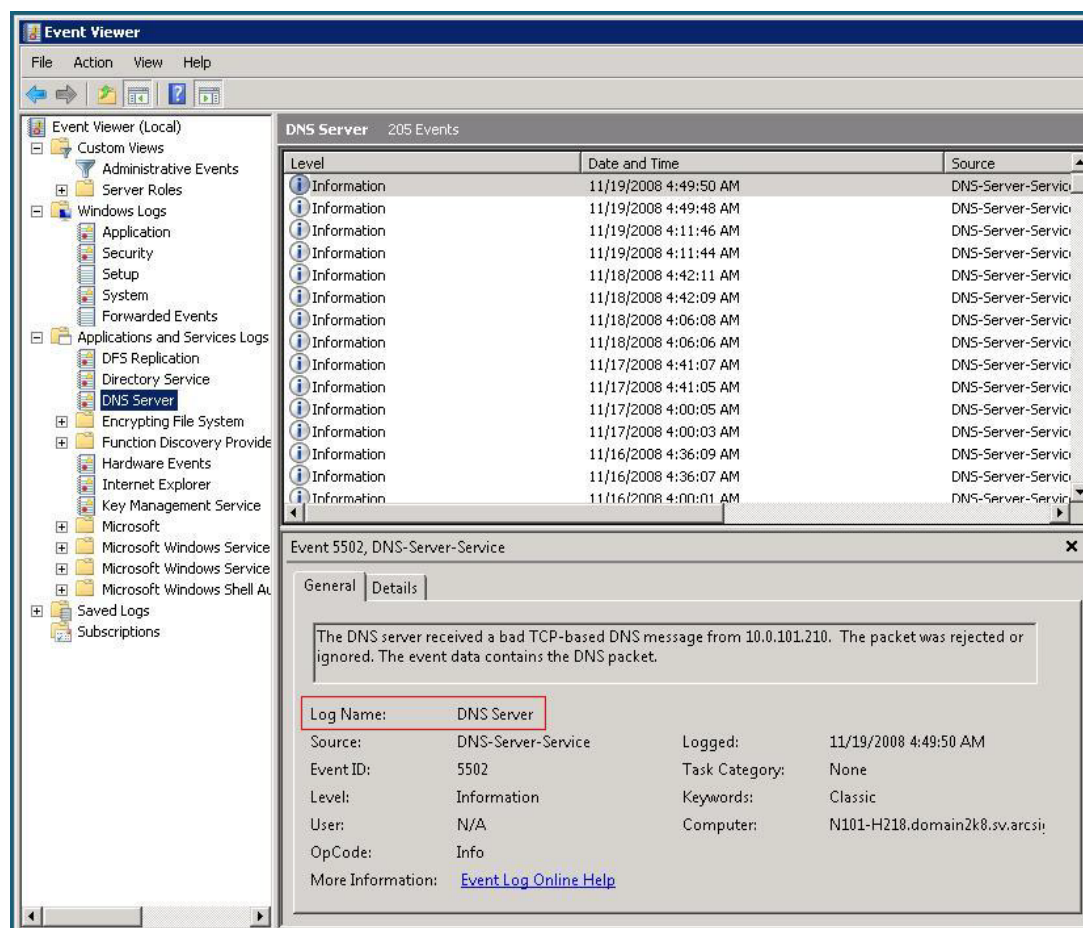
```
HardwareEvents, Security.*, , Security
HardwareEvents, Microsoft-Auditing-Security.*, , Security
```


Specify Custom Log Names

In the Windows Host parameters window, a column for the **Custom Log Names** parameter lets you specify names of custom event logs, including the forwarded security event log names for Windows Event Collector. Applications also can generate events for a custom application event log, such as DNS Server, Directory Service, Exchange Auditing, and so on. For example, specify *Directory Service* for Active Directory and *Exchange Auditing* for Microsoft Exchange Audit.

To identify the Custom Event Log Name to be for *Windows Vista / Server 2008*, select the Custom Application Event Log in MS Event Viewer to open and view one of its events.

Use the value specified in the **Log Name** field of the event as shown in the following figure:



For more information about setting this parameter, see "[Advanced Configuration Parameters per Host](#)" in this guide.

Create and Deploy Parsers for System and Application Events

The SmartConnector for Windows Event Log – Unified provides complete parsing of both the Windows event header and event description for all security events and some system events, as specified earlier in this guide.

For all System and Application events, the connector provides complete parsing of the Windows event header. Also, the connector provides a framework for users to create and deploy their own parsers to parse the event description. Such a parser can parse events specific to an Event Source, Event Log, and Microsoft OS version.

When collecting events from System Event logs (such as NTServicePack, Service Control Manager, WINS), select **System** for Windows Log type.

When collecting events from application event logs (such as Microsoft Forefront Protection 2010 for Exchange, Microsoft SQL Server Audit), select **Application** for Windows Log type.

Before creating a parser:

- 1 Generate the System or Application events of interest.
- 2 Configure the connector to collect the System or Application events and be sure to preserve the raw events.
- 3 Run the connector to collect the System or Application events and to generate the ArcSight raw events. The raw events will contain key-value pairs. The raw event body will contain key-value pairs with generic keys, such as Key[0], Key[1],... , Key[n-1]. Map the values matching these generic keys to the ArcSight event schema fields by creating a parser file. Note that not all raw events will have generic keys in the event body. Such events do not require that you create a parser to map any generic keys to the ArcSight event schema fields. But you can choose to create a parser to map the event name or description for such events.
- 4 Based on these generated raw events, follow the steps provided below to create parser files to parse the System or Application events of interest. (Note that parsers need not be created for every "cannot load key value parser" warning in the logs.)

To create and deploy your own parser:

- 1 Based upon the Microsoft OS version of the host generating the events, determine the directory location for deploying the parser file with the help of the following table:

Microsoft OS Version	Parser File Location
Windows Vista Windows Server 2008 Windows Server 2008 R2 Windows 7	\$ARCSIGHT_HOME\user\agent\fcg\windowsfg\windows_2008
Windows Server 2012 Windows Server 2012 R2 Windows 8	\$ARCSIGHT_HOME\user\agent\fcg\windowsfg\windows_2012

- Identify the Event Log Type for the events that need to be parsed (for example: System, Application, Directory Service, DNS Server, Key Management Service, and so on).
- Identify the Event Source of the events that need to be parsed, since events collected from a single event log can be generated by multiple event sources. For example, events collected from Event Log Type: System can be generated by Event Sources: Service Control Manager, WINS, and so on.
- Create a key value parser file with the following naming convention, in the directory location identified in Step 1.

```
{Normalized Event Log Type}.{Normalized Event
Source}.sdkkeyvaluefilereader.properties
```

Normalize the Event Log Type and Event Source by converting all the characters into lowercase, and then replacing each character with an underscore character (_), with the exception of English characters and numbers. This includes all kinds of special characters and spaces. For example: The key value parser file name for Event Log: "System" and Event Source: "Service Control Manager" will be:

```
system.service_control_manager.sdkkeyvaluefilereader.properties
```

- Create the mappings in this key value parser per your requirements by using conditional mappings based upon the ArcSight **externalId** field, which is already mapped to the Windows Event ID.

Also, because the connector already maps the Windows event header fields to ArcSight event fields as previously mentioned, those mappings need not be re-defined in this parser (unless you need to over-ride the mapping values). The only mappings required are for mapping the specific event description.

The following example parser can be used for reference (be sure no trailing spaces appear in your file after you copy and paste this example):

```
key.delimiter=&&
key.value.delimiter==
key.regexp=([^\&=]+)

additionaldata.enabled=true

event.deviceVendor=__getVendor(Device Vendor)
event.deviceProduct=__stringConstant(Device Product)

conditionalmap.count=1
conditionalmap[0].field=event.externalId
```

```

conditionalmap[0].mappings.count=3

#Key[0]=ABC&&Key[1]=10.0.0.1
conditionalmap[0].mappings[0].values=101
conditionalmap[0].mappings[0].event.destinationUserName=Key[0]
conditionalmap[0].mappings[0].event.destinationHostName=Key[1]
conditionalmap[0].mappings[0].event.message=__concatenate("User ",Key[0]," logged
in from host ",Key[1])

#Key[0]=ABC&&Key[1]=10.0.0.1
conditionalmap[0].mappings[1].values=102
conditionalmap[0].mappings[1].event.sourceUserName=Key[0]
conditionalmap[0].mappings[1].event.sourceHostName=Key[1]
conditionalmap[0].mappings[1].event.message=__concatenate("User ",Key[0]," logged
out from host ",Key[1])

#Key[0]=Windows Messenger Service&&Key[1]=entered&&Key[2]=stopped
conditionalmap[0].mappings[2].values=5061
conditionalmap[0].mappings[2].event.destinationServiceName=Key[0]
conditionalmap[0].mappings[2].event.deviceAction=__concatenate(Key[1],Key[2])
conditionalmap[0].mappings[2].event.message=__concatenate("Service ",Key[0],"
",Key[1]," the ",Key[2]," state")

```

6 Start the connector.

For more information about creating parsers, see the *ArcSight FlexConnector Developer's Guide*, available from the Micro Focus SSO and Protect 724 sites.

Be sure to check categorization of new events; additional categorization could be required. For information about categorization, see the Technical Note "ArcSight Categorization: A Technical Perspective" available from the Micro Focus SSO site.

Configure Advanced Options

This section documents some of the advanced configuration parameters available with this connector. You can modify parameters by editing the `agent.properties` file, which can be found in the `$ARCSIGHT_HOME\current\user\agent` folder. The tables detail the parameters you may choose to adjust, depending upon your enterprise's needs.

Advanced Common Configuration Parameters

Specify	Parameter	Default
The time in milliseconds (ms) after which the connection to a previously down host is to be retried	<code>reconnectinterval</code>	120000
Number of threads to use for the connector	<code>threadcount</code>	10
The amount of time in milliseconds to sleep before collecting more events from the hosts (-1 means disable sleeptime). This parameter can be used for bandwidth control.	<code>sleeptime</code>	-1
The amount of time in milliseconds to sleep if no events are retrieved from the configured hosts	<code>inactivitysleeptime</code>	50
Time interval in ms to wait before checking for log rotation	<code>logrotationcheckinterval</code>	5000
Whether to preserve the last ID processed before connector terminated or device went down	<code>preservestate</code>	true
Event count before writing the preserve state	<code>preservedstatecount</code>	100

Specify	Parameter	Default
Time interval in ms before writing the preserve state	preservedstateinterval	10000

Advanced Configuration Parameters per Host

Specify	Parameter	Default
Whether to get the real-time events or read from the beginning of the event logs	startatend	true
How many events to get from this host each polling cycle (can be used to control the bandwidth usage). This is only an estimated number and does not necessarily represent an exact count of events retrieved by the connector. See "Event Poll Count" for more information.	eventpollcount ¹	50
This is the buffer size per average record in an event log. The size of the packet requested from Microsoft Event Log via JCIFS API equals the event buffer size multiplied by specific event log event poll count.	eventbuffersize	512
To collect application events from Custom Application event logs, provide a comma separated list of the Custom Application event Logs. Workgroup hosts have their separate shared SID cache.	eventlogtypes	null

Event Poll Count

The `eventpollcount` parameter works at two levels. In addition to setting the `eventpollcount` for the host, you can tune the `eventpollcount` parameter to have a rate consistent with the event generation rate for the specific log type. For example, for a particular host, the Security Log events are generated at a rate of about 40 events per second, and the System events are generated at about 5 events per minute. For this host, you can set `eventpollcount = 60` for the Security Log events and `eventpollcount = 2` for the System events.

When the internal `eventpollcount` parameter is set to a value of 1023 or less for Windows 2008 hosts, the connector is able to process events as expected. But when it is set to a value of 1024 or greater, the connector is unable to process events and sends a DCERPC handle error.

The root cause of this behavior is that the connector transport to the target hosts has a limit on how much data (in total bytes) can be transferred safely without any corruption and without exceeding the maximum buffer size.



An `eventpollcount` greater than 500 to 600 is not advised due to the possible impact on network performance. An `eventpollcount` of 10 to 200 results in better network performance.

Advanced Configuration Parameters for Automatic Host Browsing

Specify	Parameter	Default
To enable the automatic host browsing feature when the connector is running	enableautohostbrowsing	false
To specify the interval in ms at which the automatic host browsing feature is to discover new hosts when the connector is running	hostbrowsingthreadsleeptime	86400000

Advanced Configuration Parameters for SID and GUID Translation

Specify	Parameter	Default
To enable SID translation	enablesidtranslation	true
To enable SID translation for SIDs that Microsoft does not translate in some Windows events	enablesidtranslationalways	false
Number of times to retry SID translation after the first attempt fails	sidtranslationretrycount	3
To enable GUID translation	enableguidtranslation	false
Size of the cache to store the SIDs and their translated values. Each domain has its own SID cache. This cache size is per domain. Workgroups hosts have their separate common SID cache.	sidcachesize	50000
Time-to-live in ms for the SID entries in the caches	sidcachetimetolive	600000
To expire only the entries of the unresolved SIDs from the caches	expirebadsidcacheentriesonly	true
Size of the cache to store the GUIDs and their translated values	guidcachesize	50000
Time-to-live in ms for the GUID entries in the caches	guidcachetimetolive	600000
To expire only the entries of the unresolved GUIDs from the caches	expirebadguidcacheentriesonly	true
Interval in milliseconds (ms) at which the SID and GUID entries are to be expired from the caches	sigguidcacheexpirationthreadsleeptime	600000
Interval in ms at which the SID and GUID caches are persisted to disk files. Each domain's SID cache is persisted to a separate disk file. The SID cache for workgroup hosts is persisted to a separate shared disk file.	sidguidcachepersistencethreadsleeptime	600000
Number of the most recently used unresolved SIDs and GUIDs to be logged in the status. Each domain's list of such SIDs is logged separately. SIDs for workgroup hosts are logged in a separate shared list.	unresolvedidstatuscount	5
To enable SID and GUID translation in multi-threaded mode	sidguidtranslationmultithreaded	false
Number of translation threads to be used for SID and GUID translation in multi-threaded mode	sidguidtranslationthreadcount	5
Number of SID translation requests that can be queued for SID translation in multi-threaded mode	sidqueuesize	50000
Number of GUID translation requests that can be queued for GUID translation in multi-thread mode	guidqueuesize	50000

Advanced Configuration Parameters for Global Catalog

Specify	Parameter	Default
To specify protocol when Global Catalog server protocol is not the same as the Active Directory Server protocol	globalcatalog.securityprotocol	non-ssl

Troubleshooting

Problems with Random JCIFS Name when Installing on Linux

When installing the Microsoft Windows Event Log – Unified connector on Linux, when viewing an event in the Windows Event Viewer, a random JCIFS name is shown for the Workstation Name (for example, JCIFSS4_140_AE). This random name causes problems with connector operation.

To avoid these problems, you can manually add the `jcifs.netbios.hostname` parameter to the `agent.wrapper.conf` file; for example: `wrapper.java.additional.10=Djcifs.netbios.hostname=mcJcifsTest`. Start the connector. Note that there is a 15-character limit for this parameter.

Now, when viewing the event in the Windows Event Viewer, the Workstation Name shows the value you entered in the `agent.wrapper.conf` file, and connector processing should work as expected.

Why are `RenameFileInTheSameDirectory` and `DeleteFile` parameters not functioning as expected?

The `usenonlockingwindowsfilereader` parameter must be set to **true** in Windows environments for the `RenameFileInTheSameDirectory` and `DeleteFile` parameters to work as expected.

Problems reading event logs from Windows 2012 R2 systems (all versions up to 7.3.0)

More likely than not, the Windows Server 2012 system you are trying to connect to does not have the optional feature for SMB 1.0 support (FS-SMB1) installed. SMB 2 and 3 protocols are not supported by this connector. SMB1 must be manually installed and enabled on Windows 2012 R2 servers. (By default, in Windows 2012 R2, the SMB1 protocol is either not installed or deactivated, preventing event log readout.) Follow these steps to enable SMB1 protocol:

- 1 To confirm SMB1 protocol is not installed, run the following PowerShell command on the Windows Server 2012 R2 system:

```
Get-WindowsFeature -Name FS-SMB1
```

In the **Install State** column, **Available** will be displayed for a system where the SMB1 is not installed. **Installed** will be displayed for a system where SMB1 is installed.

- 2 To enable SMB1 protocol, run the following PowerShell command:

```
Add-WindowsFeature -Name FS-SMB1
```

- 3 Restart the Windows Server 2012 R2 system for it to complete the necessary changes.

If the feature is installed but you are still experiencing issues, follow these steps:

- 1 Run the following PowerShell command to determine if SMB 1.0 protocol is actually enabled in the server configuration on the Windows Server 2012 R2 system:

```
Get-SmbServerConfiguration | Select EnableSMB1Protocol
```

- 2 If the value returned is `False`, then enable the SMB1 protocol by running the following PowerShell command:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $True
```

Hung connector cannot collect events

- 1 For each Windows Event Log – Unified connector in your container or JVM, identify the number of event collection threads used by that connector as follows:
 - a Get the value of the `threadcount` connector parameter.
 - b Get the value of the `windowshoststable.count` connector parameter.
 - c Choose the minimum value of these connector parameters. This minimum value is the number of event collection threads used by that connector.
- 2 Calculate the sum total of the number of event collection threads for each Windows Event Log – Unified connector in your container or JVM.
- 3 If the sum total equals or exceeds 45, increase the value of the `windowssfjg.jcifs.smb.maxbuffers` connector parameter to a value greater than 45.
- 4 Restart the connector.

Loss of host connectivity

Two advanced parameters have been added to handle situations in which connectivity to a host is lost while the host is online.

```
enableautothreadrestart  
maxtimesautothreadrestart
```

When `enableautothreadrestart` is enabled (it is disabled by default), and a reader for the particular host detects that a host had been disconnected for longer than 20 minutes, the reader stops the thread execution for this host. This can be done up to the value entered for `maxtimesautothreadrestart`, which is 2 by default, but not greater than the limit of 3 times per host.

An internal event is generated to notify the customer that the thread was stopped and for which host. For example:

```
Stopped Connection Thread for host [10.0.1.2]. Not connected for [1202527]  
ms
```

The connector then restarts the reader's thread as it would do in the case of an exception termination. Another internal event is generated, stating the thread had been replaced with a new one; for example:

```
Connection Thread Restarted Connection Thread for host [ new thread name  
[WUC[qPP1LC8BABCD5y7dYFVvCQ==] (1) ]]. Not connected for [0] ms
```

See [“Access Advanced Parameters”](#) for how to access and change these parameters.

Out of memory exceptions and missing events

Previously, the connector's JVM would throw an "out of memory" error and restart continuously when the connector attempted to process a corrupted log file. This problem has been fixed, as described below.

When the connector attempts to process events from a corrupted event log file, it gets "Out of Memory" exceptions and dumps an error that flags a host and event log type. After that, the connector restarts. Upon restart, it reads the error log, which shows a corrupted event log file was found, and creates a flag file named `ps.<host>_<eventlogtype>.error` in the `$ARCSIGHT_HOME\current\user\agent\agentdata` directory that flags this situation (for example, `ps.badHostNameOrip_Security.error`)

Upon the next automatic restart, the connector sees the flag file and knows the host and log type that should not be processed in order to avoid an out-of-memory error. The connector does not attempt to process the corrupted file until the error causing the corruption has been corrected.

If you notice the absence of events from any of your logs, check for the message in `agent.log` and `agent.wrapper.log` for "PRESENCE OF CORRUPTED EVENT LOG REPORTED FOR HOST". Fix the corrupted event log, then remove the flag file from the `agentdata` directory for the connector to process this event log. If you have problems removing this file, contact Micro Focus SSO.

Excessive Security:578 Success events generated

Why are excessive "Security:578,Success" events generated when Privileged Use Success auditing is enabled?

The Security Event ID 578 is recorded as a result of using the **SeSecurityPrivilege** privilege. **SeSecurityPrivilege** privileges are required to make Windows NT Event Log calls. This requires the **Audit Privilege Usage** policy to be enabled for both success and failure.

A *Failure Audit* of the Security Event ID 578 means that the token used does not have the **SeSecurityPrivilege** privilege, and it therefore failed to access the event log file. If the token does not have **SeSecurityPrivilege** privilege, Security Event ID 578 is logged. Because the default administrator token has the **SeSecurityPrivilege** disabled and Local Remote Procedure Calls (LRPC) remove non-enabled attributes across the call, this privilege is also removed from this token. When the Windows NT Event Log calls are then made, Windows NT Event Log does not see the **SeSecurityPrivilege** privilege, and so it logs Security Event ID 578.

A *Success Audit* of the Security Event ID 578 indicates that a user had successfully used its privileges on that computer. A typical privilege listed is **SeSecurityPrivilege**. This means that whenever a user has successfully accessed the event log, the Windows NT Event Log service generates Security Event ID 578.

Because we cannot control this behavior, we can workaround by creating a filter to filter such events with Security Event ID 578 generated on that host by the user configured for the Windows Event Log – Unified (WUC) connector. The filter should match the following criteria:

```
Device Event Class ID = "Security:578"
Device Severity = "Audit_success"
Source User Name = "<WUC User Name>"
```



This does not occur on all Windows versions.

Untranslated SID values

I see some events do not have SID values translated for them; is there anything I can do about it?

The connector attempts to translate all the SIDs by default. If the first translation attempt fails, the connector retries three times. If the translation still fails, SID translation can be enabled in multi-threaded mode by setting the parameter `sidguidtranslationmultithreaded` to **true**. The connector attempts to translate SIDs on a best-effort basis and may not always be successful. There could be network issues, the host could be busy and may not respond, or the SID could be unresolvable, which results in the connector being unable to resolve the SID. See "[Advanced Configuration Parameters for SID and GUID Translation](#)" for specific SID parameters and settings.

Locked out account

How do I resolve this message: "The referenced account is currently locked out and may not be logged on to."?

This message generally mean that the authentication information is incorrect. Verify that your user account has adequate remote access privilege. Check whether there is a firewall installed on your remote hosts; if yes, ensure port number 445 is enabled on those hosts.

Unable to create rpc handle

How do I resolve this message: "Unable to create the rpc handle for host [hostname], user [arcsight_user]"?

This message has several causes, including:

- The device is not approachable due to network failure; check your network connection.
- The device is shut down and hence cannot be connected to.
- Authentication failure due to wrong credentials or possibly the account by which you are attempting to connect has been locked out due to multiple failed attempts.
- Authorization failure due to insufficient privileges.

Optimize performance

How can I optimize performance when using the event forwarding feature?

For best performance for forwarded event collection and processing, install and configure the connector locally on the Windows Event Collect host box.

If the hosts are generating events at a lower rate than the connector is able to read, how can I optimize the performance of connector?

If only a few of the hosts are generating events at a low rate, you can increase the `sleeptime` parameter value for these specific hosts to ensure that the event polling occurs less frequently. Alternatively, if all the hosts are generating events at a low rate, you can decrease the `eventpollcount` parameter value to make sure only a small number of events are retrieved at a time.

If the hosts to which I'm connecting to receive events have a slow network connection or link, what can I do to optimize the connector performance?

Increase the `eventpollcount` and `sleeptime` parameter values to make sure the polling occurs less frequently and more events are retrieved at one time.

I am having some performance issues with the connector and would like to fine tune the configuration parameters; how can I do that?

You can create a property in the `agent.properties` file with the following prefix to set appropriate configuration parameters for the library:

```
windowsfg.jcifs.<parameter path>
```

For example, `windowsfg.jcifs.smb.maxbuffers=20` will set the number of buffers to use for collecting events to 20 rather than the default value of 16.

Keys for security events

How can I fix the following message, which appears in `agent.log`?

```
No keys have been defined for an event with Event ID = [<EventID>], Event
Log Type = [<EventLogType>], Event Source = [<EventSource>], for Microsoft
OS family = [<WindowsFamilyName>]. Please create or update the file
[windowsfg\windows_<version>/security.keymap.csv] with the appropriate keys
for the event.
```

This message means that the parsing of Security Event ID `<EventID>` is currently not supported by the connector.

The actual windows event consists of keys, all of which the connector is missing in order to map the event values completely. In such cases, the connector will map the values to key names generated based upon the index of the value. For example:

```
Key[0]=ABC&&Key[1]=10.0.0.1&&Key[2]=Interactive Log On
```

To fix this problem, create or update the file `$ARCSIGHT_HOME\user\agent\fcg\windowsfg\windows_<version>\security.keymap.csv` with the appropriate keys for the specific security event and restart the connector.

How can I specify the keys for Security events in the security.keymap.csv file?

The format for specifying the keys is as follows:

```
<SecurityEventID>,<Event Name>,<Key[0]>,<Key[1]>,<Key[2]>,. . .  
.,Message:<Event Message>
```

Each token in the entry must be surrounded by quotation marks (" "). Specifying the event message is optional.

Example entries would be as follows:

```
"528","Successful Logon","User Name","Domain","Logon ID","Logon Type","Logon  
Process","Authentication Package","Workstation Name","Logon GUID","Caller  
User Name","Caller Domain","Caller Logon ID","Caller Process ID","Transited  
Services","Source Network Address","Source Port"
```

```
"528","Successful Logon","User Name","Domain","Logon ID","Logon Type","Logon  
Process","Authentication Package","Workstation Name","Logon GUID","Caller  
User Name","Caller Domain","Caller Logon ID","Caller Process ID","Transited  
Services","Source Network Address", "Source Port","Message:A logon attempt  
was successful"
```

I see the following message in agent.log; what can I do to resolve this message?

```
Found [<count>] keys to be missing for an event with Event ID = [<EventID>],  
Event Log Type = [<EventLogType>], Event Source = [<EventSource>], for  
Microsoft OS family = [<WindowsFamilyName>]. Please create or update the  
file [windowsfg\windows_<version>\security.keymap.csv] with the appropriate  
keys for the event.
```

This message means that the parsing of Security Event ID `<EventID>` is currently supported by the connector. However, the support is limited to fewer keys. The actual Windows event consists of an additional number of keys (the number shown in the `<count>` field) that the connector is missing in order to map the event values completely. In such cases, the connector will map the values to key names generated based upon the index of the value.

For example:

```
User=ABC&&Machine=10.0.0.1&&Key[2]=Interactive Log On
```

To fix this problem, create or update the file

```
$ARCSIGHT_HOME\user\agent\fc\windowsfg\windows_<version>\  
security.keymap.csv with the appropriate keys for the specific security event and restart the  
connector.
```

Cannot determine Microsoft OS version

The following message appears in `agent.log`; what should be done to fix this?

```
Cannot determine the family for Microsoft OS version [<HostWindowsVersion>]
for [<Host>]. Make sure that this Microsoft OS version is supported by the
ArcSight SmartConnector. If it is a supported version, add the property
[windowsfg.simplified.windows.version.<HostWindowsVersion>] to the
agent.properties file.
```

```
Select an appropriate value for this property from [Windows Vista, Windows
2008]. Example: [windowsfg.simplified.windows.version.Windows 2008
Server=Windows 2008]. This will map the detailed Microsoft OS version to its
simplified Microsoft OS version. (Note: Spaces in agent property names must
be prefixed by the '\ ' character.)
```

This message means that the connector cannot determine the Microsoft OS family for the host `<Host>` based upon its Windows version `<HostWindowsVersion>`. First make sure the connector can collect and process events from this Windows version. See the list of supported Microsoft OS versions.

If this Microsoft OS version is a supported version, create a property in the `agent.properties` file with the following name to fix this problem:

```
windowsfg.simplified.windows.version.<HostWindowsVersion>
```

Be sure to prefix each space in the `<HostWindowsVersion>` by the backslash (`\`) character. Now set a value for this property, to map it to a simplified OS version, by selecting from the following list:

- Windows Vista
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2

For example:

```
windowsfg.simplified.windows.version.Windows\ 2008\ Server=Windows 2008
```

Restart the connector.

Should a warning such as the following be displayed, provide the correct OS information for that host, either in `sourcehosts.csv` or in LDAP. Be sure there is no conflict between the two sources. The connector will default to Windows 2008 R2 in case of ambiguity.

```
[2013-08-30 12:25:09,220][INFO ][default.com.arcsight.agent.a
b][lookupSourceJHostInfo] Windows version info unavailable for TestHostWUC3.
Use the best guessed version, Windows Server 2008 R2.
```

If this Microsoft OS version is not a supported version, the recommendation is to remove the host `<Host>` from the connector configuration and restart the connector.

Connector unable to process events

When I change the path to the event logs from the default drive (C:\) to another drive due to lack of space, the connector no longer detects the event logs.

This may be an issue with the connector attempting to connect the event log process using %systemroot% as the default path. Create a symbolic link (symlink) on the default (C:\) drive pointing to the log file on the drive being used; the event logs will again be detected by the connector.

The following message appears in agent.log; what should be done to fix this?

```
Cannot load key value parser from file
[<NormalizedEventLogType>.<NormalizedEventSource>.sdkkeyvaluefilereader.prop
erties] to parse events of Event Log Type [<EventLogType>], Event Source
[<EventSource>], and Microsoft OS family [<WindowsFamilyName>]. Please
create or update the key value parser file
[windowsfg\windows_<version>\<NormalizedEventLogType>.<NormalizedEventSource
>.sdkkeyvaluefilereader.properties] to parse such events.
```

This message means that, although the connector can collect events from Event Log <EventLogType> and Microsoft OS versions < WindowsFamilyName>, it cannot parse the events completely; this is because it is expecting a parser file, namely [<NormalizedEventLogType>.<NormalizedEventSource>.sdkkeyvaluefilereader.properties], which is missing or is not correctly defined. In such cases, the connector will parse only the Windows event header, but not the event description.

To fix this to parse these events, create or update the parser file [windowsfg\windows_<version>\<NormalizedEventLogType>.<NormalizedEventSource>.sdkkeyvaluefilereader.properties] with the appropriate mappings.

Another option is to add a mapping to point to correct mappings; see [“Customize Event Source Mapping”](#) for more information.

Remote/local machine event collection

Why can't I retrieve events from a local machine? I have no problem collecting events from remote machines?

In our testing environment, this sometimes happens when we use a regular user account to log onto the SmartConnector machine. If you encounter the same problem, attempt to log in with a user account with adequate privilege to read the event logs.

What kind of services should we enable on remote Windows machines from which we want the SmartConnector to retrieve events?

Remote Windows machines should have the Remote Procedure Call (RPC) service running.

There is a personal firewall installed on some of the remote Windows machines from which I want to retrieve events. Which ports should be opened on those machines to let the SmartConnector collect events?

Enabling port 445 should be enough for the SmartConnector. If you cannot connect to and receive events from a host, contact Micro Focus SSO for assistance.

Forwarded Event Collection

With Forwarded Events Collection enabled, two new fields (`CollectionHost` and `CollectionEventLog`) are added to the connector Raw Event as shown in the following example:

```
EventlogType=Security&&ComputerName=N1H2.domain.com&&CollectionHost=N5H5WinC  
ollect&&CollectionEventLog=HardwareEvents
```