Micro Focus Security ArcSight ArcSight

Software Version: 8.3.0

Configuration Guide for for Microsoft Windows Event Log - Native SmartConnector

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

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

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

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

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

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

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

Support

Contact Information

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

Contents

Configuration Guide for SmartConnector for Microsoft Windows OS

ArcSight SmartConnectors intelligently collect a large amount of heterogeneous raw event data from security devices in an enterprise network, process the data into ArcSight security events, and transport data to destination devices.

To collect events from Microsoft Windows OS, use the ArcSight SmartConnector for Windows Event Log - Native, which supports event collection from log sources such as Sysmon, Powershell etc.,

This guide provides a high level overview of ArcSight SmartConnector for Windows Event Log - Native.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectorss to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

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

Contact Information

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

For specific product issues, contact Micro Focus Customer Care.

Product Overview

The SmartConnector for Microsoft Windows Event Log – Native can connect to local or remote machines, inside a single domain or from multiple domains, to retrieve events from all types of event logs. It can collect events from

ArcSightSmartConnectors provide easy, scalable, audit-quality collection of all logs from all event-generating sources across the enterprise for real-time and forensic analysis. The ArcSight is optimized for a large number of hosts.

The infrastructure provided with the SmartConnector for Microsoft Windows Event Log – Native has been improved to deliver critical features such as Operational Windows Event Logs and event collection and event filtering from IPv6 hosts. It leverages the native technology on the Microsoft platform and provides the best support for Windows event features and capabilities (including collection for all log types).

The Security events are not audited by default. You must specify the type of security events to be audited.

There are following types for default Windows event logs:

- Application log (tracks events that occur in a registered application)
- Security log (tracks security changes and possible breaches in security)
- System log (tracks system events)

The connector consists of the following major components:

- SmartConnector framework-based event processor
- The Windows API application, which collects events from Microsoft Windows Event Logs
- A Message Queue that facilitates communication between the previous two components

The Windows API event collection and the Message Queue are started by the connector at the time of connector setup and at the start of the connector process.

For SmartConnector security event mappings to ArcSight data fields, see *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings*.

SmartConnector Features

SmartConnector capabilities include real-time event collection and processing, as well as data enrichment (normalization, categorization, Common Event Format (CEF), aggregation, and filtering) and efficiency (caching, batching, compression, and bandwidth management). For more information about SmartConnector capabilities in general, see SmartConnector Features. Specific features of the Windows Event Log – Native connector are described n the following sections.

Custom Log Support

Supports event collection from non-administrative, operational, or custom logs.

Event Filtering

Supports filters that apply at the time of event collection from the event source to the connector. With this support, you can filter out events in which you have no interest, thus making better use of resources.

Globally Unique Identifier (GUID)

Supports translation and mapping of the GUID (also known as UUID) within a forest (A forest is a complete instance of Active Directory). The connector can perform GUID translation for GUIDs within a forest by querying the Global Catalog Server. The Active Directory parameters are used for Global Catalog Server. 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. Global Catalog and Active Directory must be on the same machine.

Host Browsing

Host browsing is used when hosts are added during installation using Active Directory. Notification is sent to a destination when a new host is added to Active Directory.

IPv6

Supports event collection from IPv6 hosts and parsing of IPv6 events.

Localization

The Windows Event Log – Native connector supports security event localization for the following languages:

Language	Locale	Encoding
French	fr_CA	UTF-8
Japanese	ja_JP	Shift_JIS
Chinese Simplified	zh_CN	GB2312
Chinese Traditional	zh_TW	Big5

The locale and encoding can be specified for the `event.name` field during SmartConnector installation. See Configuring Multiple Host Parameters . For localization of other languages, see Customizing Localization Support for the Native Connector.

Collect Forwarded Events

The connector has the ability to read events forwarded to a Windows Event Collector host. Windows Event Collection is a Microsoft capability that lets a Windows host collect events from multiple sources. Collecting forwarded events is different than the traditional event collection because the events are collected from multiple sources.

With Microsoft Windows Event Collector (WEC), you can subscribe to receive and store events on a local computer (event collector) that are forwarded from any number of remote computers (event sources). Before using this feature, refer to Microsoft Windows documentation, to know more about Windows Event Collector functionality. To configure the connector to collect forwarded events, see Collecting Forwarded Events.

Configuring Windows

You must enable the appropriate auditing policies on Windows servers from which the connector collects information and also setup standard user accounts. This section has the following information:

Enabling Microsoft Windows Event Log Audit Policies

Because event information generated by Windows servers is based on the auditing policies that are enabled, make sure that appropriate auditing policies are enabled on Windows servers from which the connector collect information. By default, none of the Windows auditing features are enabled.

Auditing events consumes system resources such as memory, processing power, and disk space. Auditing an excessive number of events can dramatically slow down your servers.

Note: You must be logged in 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 depending on whether the policy is being created on a member server, a domain controller, or a stand-alone server.

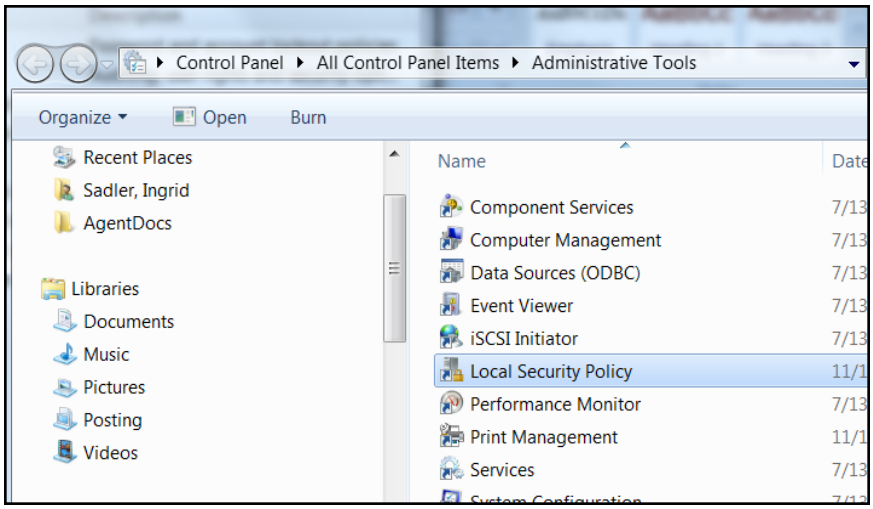
- To configure a domain controller, member server, or workstation, use **Active Directory Users and Computers**.
- To configure a system that does not participate in a domain, use **Local Security Settings**.

This section has the following information:

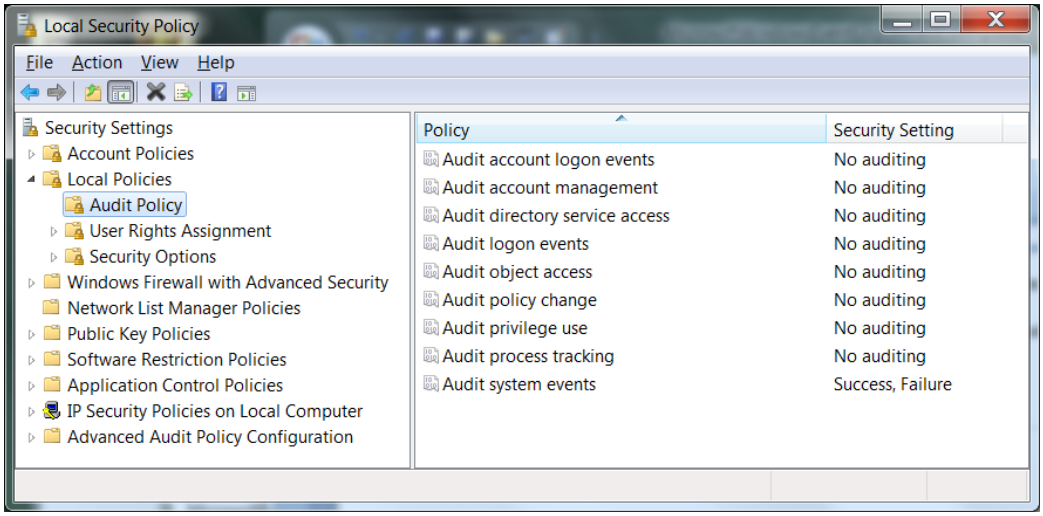
Enabling an Auditing Policy on a Local System

To establish an audit policy on a local system:

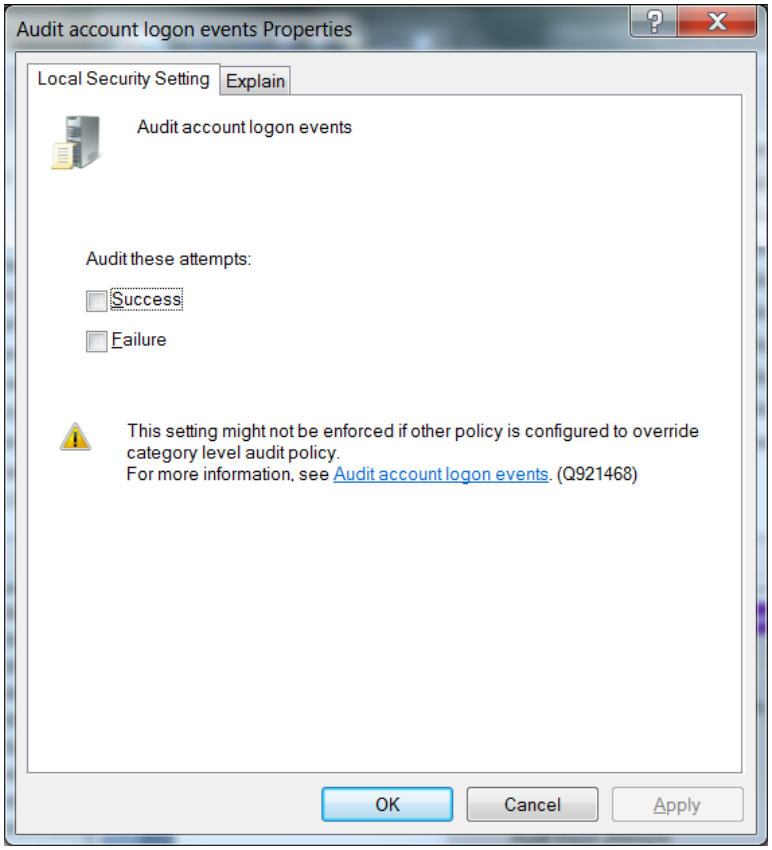
1. Select **Start > Control Panel > Administrative Tools > Local Security Policy**.



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 similar to the following is displayed, letting you choose to perform a **Success** or a **Failure** audit (or both) on that type of event.



Note: 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).

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

Setting Up an Audit Policy 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.

Setting 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.

Setting Up Standard User Accounts

The connector does not require domain administrator privileges to collect Security events from Windows hosts. Event Log Reader privilege is required for system and custom application event collection including Forwarded Events Collection.

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

These steps describe 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.

Note: 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**.

Standard Domain User Account from Windows Server Domain Controllers

On the Windows Server 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 the new Domain User `arcsight` to this security principal.
6. This Group Policy can take some time to take effect. To enable the policy immediately, run this command from the Windows Server Domain Controller and the Windows Domain Member command prompts:

   ```
   GPUpdate /Force
   ```

   This command will update any modifications you have made to any group policy, not just this one.

Standard Domain User Account from Domain Members

On the Windows Server 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 can take some time to take effect. To enable the policy immediately, run this command from the Windows Server Domain Controller and the Windows Domain Member command prompts:

   ```
   GPUpdate /Force
   ```

Note: This command will update modifications to any group policy you have made, not just this one

Standard Local User Account from Windows Workgroup Hosts

On the Windows 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**.

Add Security Certifications when Using SSL

If you choose to use SSL as the connection protocol, security certificates for both the Windows Domain Controller Service and for the Active Directory Server are required. 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 certificates will be imported to the connector's certificate store during the connector installation process. See **step 3** of the installation procedure for instructions.

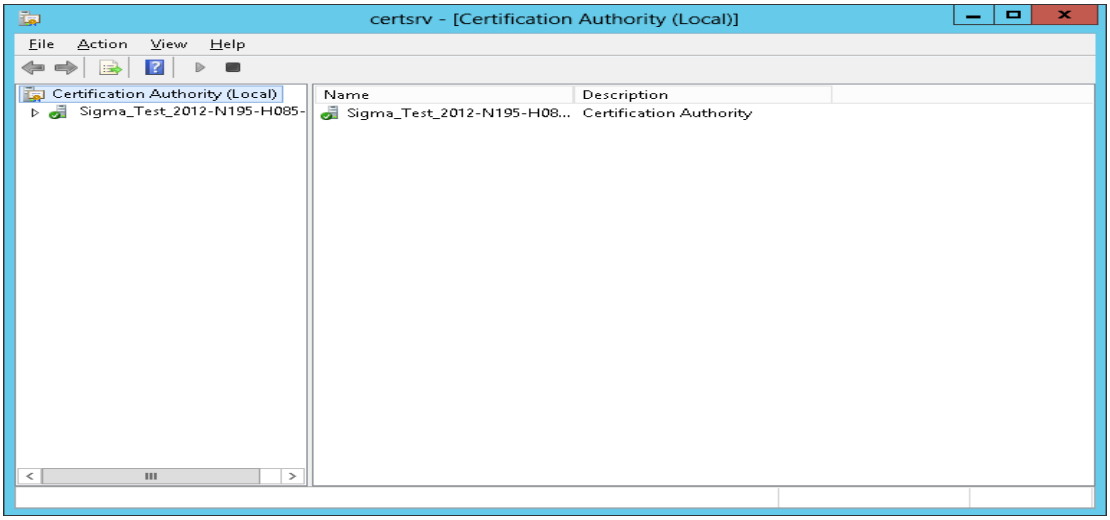
Procedures for Windows 2012 are shown; steps could vary with different Windows versions. For other Windows versions, see Microsoft's documentation for complete information.

Example: Windows Server 2012

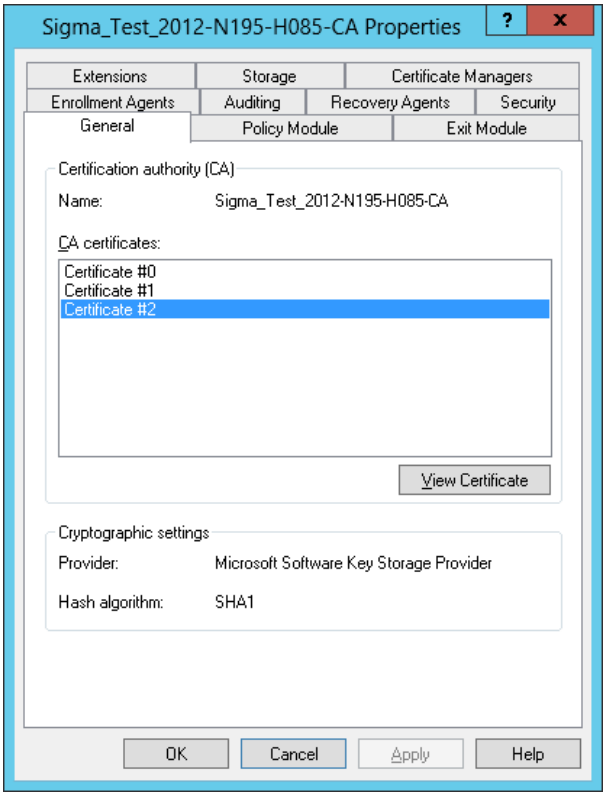
The following steps assume Windows Server 2012 as the operating system

To export the certificates:

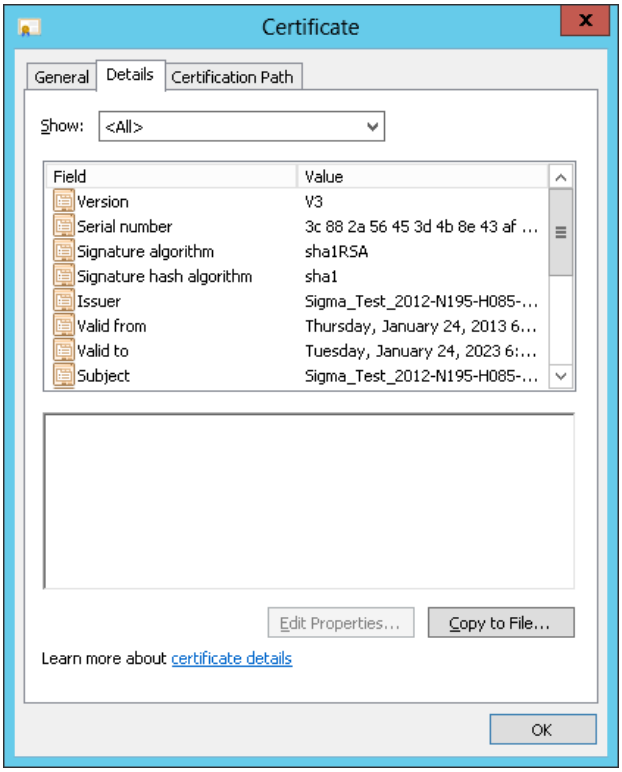
1. From the Windows **Start** menu, select **Administrative Tools**.
2. Select and double-click **Certification Authority**; one or more Domain Certificate Authority servers are shown.



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.

Installing the SmartConnector

This section has the following information:

Installation Prerequisites

Supported Operating Systems for Installation

System Requirements

This connecter can be installed on only one of the following supported Microsoft Windows 64-bit platforms:

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2 Standard
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (*)
- Microsoft Windows 10

.NET Requirements

- .NET 4.5.2, 4.6, 4.6.1 or 4.7.2.

Supported Operating Systems for Event Collection

ArcSight supports Windows Event Log Security, System, and Application event collection from hosts running the following Microsoft OS versions.

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (*)
- Microsoft Windows 10

It also supports events forwarded from source hosts to a Windows Event Collector (WEC).

Supported Log Parsers

The SmartConnector supports parsing for the following logs:

- Security
- System
- Application (event header)
- Forwarded Events (for forwarded security, system, and application (event Header) events

Supported Applications

Parser support for the following application events is provided:

- Microsoft Active Directory
- Microsoft Exchange Access Auditing
- Microsoft SQL Server Audit
- Microsoft Local Administrator Password Solution (LAPS)
- Microsoft Windows Powershell
- Microsoft Windows BITS Client
- Microsoft Windows ESENT
- Oracle Audit
- Symantec Mail Security for Exchange

Supported System Events

Parser support for the following system events is provided:

- Microsoft Network Policy Server
- Microsoft Remote Access
- Microsoft Service Control Manager
- Microsoft WINS Server
- Microsoft Windows WindowsUpdateClient

Supported Events

Windows Event Log supports parsing for:

Event Type	Event Header	Event Description
Security	yes	yes
Application	yes	no*

Event Type	Event Header	Event Description
System (Service Control Manager and WINS event sources)	yes	yes
Other System events (including Remote Access and NPS)	yes	no*

* Support is provided for a Flex-Connector-like framework that lets you create and deploy your own parsers to parse the event description for all system and application events. See "Create and Deploy Parsers for System and Application Events" for more information. See "Log Parser Support" for application and system events already supported.

Use of Active Directory Query for Hosts

An Active Directory query can be used to populate or update collection end points, or specify the Windows OS version of source hosts for forwarded events if collected from the Windows Event Collector. The connector discovers and retrieves information about the hosts registered in an Active Directory. The host information includes the DNS name along with its operating system version. Whe n new hosts are registered in an Active Directory while the connector is running, it sends an internal event notifying the user of the newly discovered host.

SmartConnector Setup Scenarios

The following examples describe some typical setup scenarios. For configuration details, see See "Configure the Connector"

- **Scenario 1 - Collect Application, Security, and System Logs for the Local Host:** You select local host logs on the first configuration window with no remote hosts, no custom logs or event filters, and no Windows Event Forwarding configuration. Locale and encoding of the local host are automatically detected and configured by the connector; therefore, configuration of these values for the local host is not necessary.
- **Scenario 2 - Collect Application, Security, and System Logs from Remote Hosts, from One Domain, and Enter the Hosts Manually:** In this scenario, you can collect logs from remote hosts and add the host entries manually. You can either add a table parameter in the entry window that is displayed or import a csv file containing host information. However, when importing, make sure your local host is in the csv file if you intend to collect events from the local host, as the content from the imported file replaces the existing host information.
- **Scenorio 3 - Collect Application, Security, and System logs from Hosts Recorded in Active Directory:** Collect logs from a host recorded in Active Directory. The table parameter entry window is then displayed, where you can make configuration selections for each host.
- **Scenario 4 - Collect Forwarded Events or Other WEC Logs from Local Or Remote Hosts:** With any of the previous scenarios, to collect Forwarded Events or other WEC logs from the local host (or remote hosts); a window is displayed where you can specify the name of a csv file containing the source hosts names and Windows OS versions for the hosts after making configuration selections for your hosts on the table parameter entry window.

Before you Begin

The following items are required when installing this SmartConnector :

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

Installation Notes

- Install this SmartConnector only on 64-bit Windows platforms. See "Operating Systems Support for Event Collection."
- If you use Forwarded Event Collection, the full computer name and OS version of source hosts must be available for use either through Active Directory or a source hosts file in csv format.

Enabling FIPS at the OS Level

1. From the Windows **Start** menu, select **Run**.
2. Enter `gpedit.msc`.
3. In the Group Policy Editor, navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.
4. In the right pane, locate and click the "System cryptography: Use FIPS compliant5 algorithms for encryption, hashing, and signing" setting.
5. Set to **Enabled** and click **OK**.
6. Restart the computer.

Installing and Configuring the SmartConnector

For additional information about installing the SmartConnectors, see the ArcSight SmartConnector Installation and User Guide.

To install and configure the Windows Event Log - Native SmartConnector:

1. Start the installation process.
2. Follow the instructions to add the required details to complete the installation of core software.
3. After the installation completes, to configure the connector, you can either click **Next** or run the `<ArcSightSmartConnectors_installDirectory>\current\bin\runagentsetup.bat` file.
4. Select the relevant Global Parameters, the click **Next**.
5. From the **Type** drop-down, select **Microsoft Windows Event Log - Native** as the type of connector, then click **Next**.
6. In the **Configure Parameters** window, specify the following information:
   a. Select logs for event collection:
      - The **Security log**, **System log**, and **Application log** options are selected by default. See "Log Parser Support" for a list of supported application and system events. For more information about the type of logs to select for different log sources, see Selecting the Type of Logs for Event Collection.
      - **Custom Log:** Select this option to collect custom logs. For more information, see Configuring Custom Logs and Filtering
      - **ForwardedEvents Log:** If you select this option, you can collect events forwarded from a source host to any log type on the collector machine to which the connector

has access.

Note: Security events cannot be forwarded to the Security event log on a collector machine, but can be forwarded to other log types.

b. If you selected the **ForwardedEvents Log** option, the Windows OS version of the event source host is not populated automatically in the normalized events. To populate this value, you must either provide the Windows OS version or configure the Active Directory. If both Active Directory and Windows OS version is available from the source host file , then value from Active Directory takes precedence. Select any of the following options to specify the Windows OS version for the hosts from which you want to collect events:

- **Use file for OS version:** Select this option to supply the name of the source hosts in a file. If you select this option, you will be prompted to specify the file details.
- **Use Active Directory for OS version**: Select this option, then the connector retrieves the host details from the configured Active Directory to identify the event source host Windows version information. Newly discovered hosts are added to the lookup automatically without having to reconfigure the connector itself.

  For the connector to be able to browse the Active Directory to retrieve source host Windows version information, it must be placed within the same forest as the Active Directory.

  If you select this option, you will be prompted to enter your domain credentials and Active Directory parameter information in the next screen.
- **Do not use any source for Windows OS version**: Select this option to not provide an Active Directory query or a CSV file to list all hosts involved in events forwarding along with their Windows OS version. If you select this option, no Windows OS version will be displayed in the event headers from the forwarding host.

c. Select one or many of the following parameters to add hosts for event collection:

- **Use Common Domain Credentials:** Select this option to specify common domain credentials.
- **Use Active Directory:** Select this option to use the host information (host name and version) from the configured Active Directory to identify the event source host Windows version information.
- **Enter Manually:** Select this option to manually specify all the host details.

7. Click **Next**.
8. One or more of the following screens will be displayed depending on your selections in the previous window:

a. **WEF Source Hosts File Name:** If you selected **ForwardedEvents log** or **Use file for OS version** options in the previous window, then you are prompted to enter the name of

the file that contains the source host information. This window is also displayed if you have selected **Is WEC** for any hosts in the table parameter window. For forwarded event collection, specify only the Event Collector hosts.

b. **Device Details Collection:** The first row displays selections from the initial parameter entry window for the local host. Click **Add** to manually add a host, or click **Import** to select a `.csv` file to import host information. Make sure that there is a carriage return (only one CR) at the last entry in the `.csv` file. Else the import fails.

   If you have added hosts for which you decide not to collect events, you can use the checkbox in the leftmost column to deselect rows in the table.

Parameter	Description
Host Name	Host name or IP address of the target Windows host.
Domain Name	Name of the domain to which the host belongs. If you are using a Domain User account for a target host or using Active Directory, fill in the Domain Name field. This must be a name, not an IP address, for the OS version to be resolved.
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**.
Windows Version	Select the Microsoft Operating System version this host is running.
Is WEC	If you selected **Indicates that this is a WEC server** on the initial configuration page, this selection is already checked for the local host.
Security	Select for security events to be collected from this host. This log is automatically selected for all hosts.
System	Select for system events to be collected from this host.
Application	Select for application events to be collected from the **Common Application Event Log** of this host.
ForwardedEvents	Select for events to be collected from the **ForwardedEvents** log of this host.
Custom Event Logs	Specify the custom application log names, separated by a comma (such as "`Exchange Auditing, Directory Service`"). For Windows Event Collector servers, use **HardwareEvents**. See "'Installing and Configuring the SmartConnector" on page 46" for more information.

Parameter	Description
Filter	This is a filter you can get from the Microsoft event viewer when you want to collect particular events. You can copy the filter text to this field. For more information, see "Configure a Filter."
Locale	Enter the value for your locale or accept the United States English default, **en_US**. Leave this field blank if you want the connector for the local host to automatically determine the correct Locale value. Values are: ■ French Canadian: `fr_CA` ■ Japanese: `ja_JP` ■ Simplified Chinese: `zh_CN` ■ Traditional Chinese: `zh_TW` ■ United States English (the default): `en_US` For localization of other languages, see "Customize Localization Support for the Native Connector" on page 39.
Encoding	Enter the encoding value for the language used to send localized log events, or accept the United States English default, en_US. This value cannot be determined automatically. Select from the following values: ■ French Canadian: `fr_CA` ■ Japanese: `Shift_JIS` ■ Simplified Chinese: `GB2312` ■ Traditional Chinese: `zh_TW` ■ United States English (the default): `UTF-8` For localization of other languages, see "Customize Localization Support for the Native Connector" on page 39.

c. **Domain Credentials:** If you selected **Use common domain credentials** option in the previous window, then you are prompted to specify the following details:

Note:

- A Domain User Name and Domain User Password is not required if you are performing local event collection.
- If the hosts Domain parameters are the same as Active Directory, then you do not have to enter both. The information will be taken from the Active Directory Domain and credentials.

Parameter	Description
Domain Name	Enter the name of the domain to which the host belongs. Work group hosts and stand-alone hosts can be added manually on the table parameters entry window.
Domain User Name	Enter the name of the user account with adequate privileges to collect Windows events from the target host. It is assumed that the AD server is located on the domain server and can be accessed with the domain user and password.
Domain User Password	Enter the password for the user specified in the **Domain User Name** field.

d. **Active Directory Parameters:** If you selected **Use common domain credentials** option in the previous window, then you are prompted to specify the following details:

Note:

- A Domain User Name and Domain User Password is not required if you are performing local event collection.
- If the hosts Domain parameters are the same as Active Directory, then you do not have to enter both. The information will be taken from the Active Directory Domain and credentials.
- If GUID translation is enabled, then the Active Directory Domain and credentials are used. You must provide the complete domain name, including any qualifiers, such as `.com`.

Parameter	Description
Active Directory Domain	Enter the name of the Active Directory domain to which the host belongs.
Active Directory User Name	Enter the name of the user account with adequate privileges to collect Windows events from the target host. It is assumed that the AD server is located on the domain server and can be accessed with the domain user and password.
Active Directory User Password	Enter the password for the user specified in the **Active Directory User Name** field.
Active Directory Server	Enter the Active Directory Host Name or IP address required for authentication to the Microsoft Active Directory for the host browsing feature.

Parameter	Description
Active Directory Filter	Enter the Active Directory Filter required for automatic host browsing to filter hosts by name, operating system, and creation time. The query can contain attributes for Common Names (cn), Operating System (`operatingsystem`) and Creation Time (`whencreated`) in 'YYMMDDHHmmSS' format, where `YY`=Last two digits of the year, `MM`=Month, `DD`=Date, `HH`=Hours, `mm`=Minutes, `SS`=Seconds in 24-hour format. The query can also contain wildcard characters (*) to match the attributes to different values. **Active Directory Filter examples** To create hosts after and inclusive of a particular time point, set filter to:`(&(cn=*)(operatingsystem=*)(whencreated>=YYMMDDHHmmSSZ))` To create hosts between and inclusive of two time points, set filter to: `(&(cn=*)(operatingsystem=*)(whencreated>=YYMMDDHHmmSS)(whencreated<=YYMMDDHHmmSS))`
Active Directory Protocol	Select whether the protocol to be used is **non_ssl** (the default value) or SSL. For SSL protocol, be sure to import the Active Directory security certificate to the connector before starting the connector.
Use Active Directory host results for	For WEF Only: If you selected "**Use Active Directory for OSVersion**" on the initial configuration window, the list of hosts retrieved from Active Directory is used to determine the Windows OS version for the WEF source hosts. When **For WEF Only** is selected, the result of the query will not populate the table of hosts on the table parameter entry window. For initial installation, **Merge Hosts and Replace Hosts** act the same because only the local host is present and preserved. If you selected **Use Active Directory** on the initial configuration screen under **Parameters to add hosts** for event collection, or you are modifying parameters to add hosts, the following applies. When **Merge Hosts** is selected, Active Directory is used to retrieve the hosts for collection (and can also be used for Windows Event Forwarding if WEC servers are present and **Use file for OS** is not selected on the initial configuration screen). The original host is not replaced and all other preconfigured hosts are preserved. Hosts are added from the list retrieved from Active Directory with Security events selected by default. If duplicates are found, the existing host entry is not overwritten. When **Replace Hosts** is chosen, Active Directory is used to retrieve the hosts for collection (and can also be used for Windows Event Forwarding when WEC servers are present and Use file for OS is not selected on the initial configuration screen). The local host is not replaced, but all other hosts preconfigured are replaced with those retrieved from Active Directory, with Security events selected by default.

9. Select a destination, then configure the destination parameters.
10. Specify a name for the connector.
11. Select whether you want to run the connector as a service or in the standalone mode.

12. Complete the installation process.

Using SSL for Connection (optional)

If you are using SSL for connector connection, follow these steps.

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

1. 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
2. Select `jre/lib/security/cacerts`, then select **import cert** to import your certificate. Verify that the correct certificate has been imported.
3. When prompted **Trust this certificate?**, click **Yes**.

   Repeat this process for the second certificate.
4. Save the keystore.
5. Verify the imported certificates by entering this command from `$ARCSIGHT_HOME\current\bin`:

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

   The new certificates are listed.
6. Return to the configuration wizard by entering the following command from `$ARCSIGHT_HOME\current\bin`:

   ```
   runagentsetup
   ```

Installing and Configuring Multiple Connector Instances

Follow these steps to install and run another instance of the connector on the source host.

1. Install the core connector software, then exit the wizard.
2. Go to the installation directory. For example:

   `$ARCSIGHT_HOME\ArcSightSmartConnectors\current\`
3. From the `$ARCSIGHT_HOME\current\user\agent` directory, edit the `agent.properties` file.
4. Select a valid TCP port value for the `mq.server.listener.port` property. The value cannot be used by another instance of the connector. Range can be a value from 1 to 65535; the default value is 61616.
5. Add the parameter and value for the `mq.server.listener.port` property.

6. In the `$ARCSIGHT_HOME\current\user\agent\winc` directory, create a `config.ini` file with the following contents:

```
mq.server.hostname=localhost
mq.protocol=tcp
mq.server.port=<valid tcp port>
```

   The `mq.server.port` value in this file should match the one configured in `agent.properties`.

7. Launch the setup wizard by running **runagentsetup** from the `$ARCSIGHT_HOME\current\bin` directory.

Notes:

- When running the configuration wizard, the following warning message might be logged as the event listener starts to send the heartbeat before it is assigned to `RemoteAgentId`:

```
[updateHeartbeat]RemoteAgentId unspecified. Ignoring the heartbeat.
```

- The connector *will not run* if the value of `mq.server.port` is not unique for each instance of the Native Windows Event Log installed on the same box. It will indicate that the port is already in use.
- Resource consumption increases as the number of connector instances increase, so this constraint may limit the number of instances you use in your enterprise.

Log sources and Event Mappings

This section provides information about the following supported log sources and Event Mappings to ArcSight fields:

Microsoft ADFS

Active Directory Federation Service (ADFS) is a software component in Windows Server 2012, Windows Server 2016, and Windows Server 2019. It contains Active Directory, Federation Server, Federation Server Proxy, and ADFS Web Server.

ADFS provides the following services:

- **Single Sign-On (SSO)**: ADFS provides SSO authorization to users who want to access applications in different networks or organizations. It provides SSO access to internet-facing applications or services.
- **Identity Federation (Identity Management)**: This provides the digital identity to the users and allows to centralize it. This helps to maintain security and rights across security and enterprise boundaries.

Supported Versions

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides main mappings for the Windows Event Log SmartConnectors. The field mappings listed in this document are specifically for Microsoft Remote Access.

Configuring Microsoft ADFS Logs

For information about configuring Microsoft ADFS events logs, seehttps://adfshelp.microsoft.com/AdfsEventViewer/GetAdfsEventList in the Microsoft TechNet Library.

Event Mappings for Microsoft ADFS

General

ArcSight Field	Vendor Field
Device Product	'ADFS Auditing'
Device Vendor	'Microsoft'

Event 299

ArcSight Field	Vendor Field
Destination DNS Domain	%3 (Relying Party)
Device Custom String 1	%2 (Activity ID)
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%1 (Instance ID)
Device Custom String 4 Label	"Instance ID"
Message	__concatenate("A token was successfully issued for the relying party ",%3)
Name	"A token was successfully issued for relying party"

Event 300

ArcSight Field	Vendor Field
Device Custom String 1	%1 (Activity ID)
Device Custom String 1 Label	"Activity ID"
Device Custom String 5	%2 (Request type)
Device Custom String 5 Label	"Request Type"
Device Custom String 6	%3 (Exception details)
Device Custom String 6 Label	"Exception details"
Message	"The Federation Service failed to issue a token as a result of an error during processing of the WS-Trust request"
Name	"Federation Service failed to issue a token as a result of an error"
Source Nt Domain	__extractNTDomain(%3)
Source User Name	__extractNTUser(%3)

Event 307

ArcSight Field	Vendor Field
Device Custom String 4	%1
Device Custom String 4 Label	"Instance ID"
Name	"Federation service configuration was changed"
Source Nt Domain	__extractNTDomain(%3)
Source User Name	__extractNTUser(%3)

Event 403

ArcSight Field	Vendor Field
Destination Address	%9 (Local IP)
Destination Dns Domain	%14
Destination Port	%8 (Local Port)
Device Custom Date 1	%3
Device Custom Date 1 Label	"Request Time"
Device Custom Number 1	%11
Device Custom Number 1 Label	"Content Length"
Device Custom String 1	%2
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%1
Device Custom String 4 Label	"Instance ID"
Device Custom String 6	%16
Device Custom String 6 Label	"Proxy DNS name"
End Time	%3
Name	"An HTTP request was received"
Old File Hash	__concatenate("Through Proxy:",%15)
Old File Id	__concatenate("Caller Identity:",%12)
Old File Type	__concatenate("Certificate Identity:",%13)
Request Client Application	%10 (User Agent)
Request Method	%5 (HTTP Method)

Request Url File Name	%6 (Url Absolute Path)
Request Url Query	%7 (Query string)
Source Address	%4
Start Time	%3

Event 404

ArcSight Field	Vendor Field
Device Custom Date 1	%3
Device Custom Date 1 Label	"Response Time"
Device Custom String 1	%2
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%1
Device Custom String 4 Label	"Instance ID"
Device Custom String 5	%5
Device Custom String 5 Label	"Status Description"
End Time	%3
Event Outcome	%4
Name	"An HTTP response was dispatched"

Event 405

ArcSight Field	Vendor Field
Destination Host Name	%3
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Message	__concatenate("Password change succeeded for following user:",%2)
Name	"Password change succeeded"
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 406 - Windows Server 2016

ArcSight Field	Vendor Field
Destination Host Name	%3
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Message	__concatenate("Password change failed for following user:",%2)
Name	"Password change failed"
Reason	%4
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 406 - Windows Server 2019

ArcSight Field	Vendor Field
Destination Host Name	%4
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%3
Device Custom String 4 Label	"Device Certificate"
Message	__concatenate("Password change failed for following user:",%2)
Name	"Password change failed"
Reason	%5
Source Address	%6
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 410

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"

ArcSight Field	Vendor Field
Device Custom String 4	%3
Device Custom String 4 Label	"Client Application"
Device Custom String 5	%13
Device Custom String 5 Label	"Proxy"
Device Custom String 6	%11
Device Custom String 6 Label	"Forwarded Client IP"
Name	"Following request context headers present"
Old File Id	__concatenate(%6,":",%7)
Request Client Application	%5
Request Url File Name	%9
Source Address	%15
Source Translated Address	__regexToken(%11)

Event 411

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%2
Device Custom String 4 Label	"Token Type"
Device Custom String 5	%3
Device Custom String 5 Label	"Error message"
Device Custom String 6	%4
Device Custom String 6 Label	"Exception details"
Name	"Token validation failed"
Reason	__regexToken(%3)
Request Url	%2
Source Address	%5
Source User Name	__regexToken(%3)

Event 412

ArcSight Field	Vendor Field
Destination Dns Domain	%4
Device Custom String 1	%2
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%1
Device Custom String 4 Label	"Instance ID"
Device Custom String 6	%3
Device Custom String 6 Label	"Token type"
Message	__concatenate("A token of type ",%3," for relying party ",%4," was successfully authenticated")
Name	"A token for relying party was successfully authenticated"

Event 413

ArcSight Field	Vendor Field
Destination Dns Domain	%5
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Name	"An error occurred during processing of a token request"
Old File Hash	__concatenate("Caller:",%2)
Old File Id	__concatenate("Device identity:",%6)
Old File Name	__concatenate("Act as User:",%4)
Source Address	%7
Source User Name	__extractNTUser(%3)

Event 418

ArcSight Field	Vendor Field
File Hash	%4
File Name	%2

ArcSight Field	Vendor Field
Name	"Trust between federation server proxy and service was successfully renewed"
Old File Hash	%3
Source Address	%1

Event 420

ArcSight Field	Vendor Field
File Hash	%4
File Name	%3
Name	"Trust between federation server proxy and service was successfully established"
Source Address	%2
Source User Name	__extractNTUser(%1)
Surce Nt Domain	__extractNTDomain(%1)

Event 424

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 6	%5
Device Custom String 6 Label	"Inner exception"
File Hash	%2
File Name	%3
Name	"The federation server proxy was not able to authenticate the client certificate presented in the request"
Source Address	%4

Event 431

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"

ArcSight Field	Vendor Field
Device Custom String 4	%5
Device Custom String 4 Label	"Token Type"
Device Custom String 5	%4
Device Custom String 5 Label	"Request Type"
Device Custom String 6	%6
Device Custom String 6 Label	"Signature Algorithm"
File Size	%2
File Type	%3
Name	"An active request was received at STS with RST"

Event 512

ArcSight Field	Vendor Field
Device Custom Date 1	__concatenate(%5," ",%6)
Device Custom Date 1 Label	"Last Bad Password Attempt"
Device Custom Number 1	%4
Device Custom Number 1 Label	"Bad Password Count"
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Message	__concatenate("The account for the following user ",%2," is locked out. A login attempt is being allowed due to the system configuration")
Name	"The account for the following user is locked out"
Source Address	%3
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 513

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 6	%4

ArcSight Field	Vendor Field
Device Custom String 6 Label	"Exception details"
Name	"The Artifact REST service failed to return an artifact as a result of an error during processing"
Request Url	%3
Source Address	%2

Event 515

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Event Outcome	"This account may be compromised"
Message	__concatenate("The following user ",%2," account was in a locked out state and the correct password was just provided. This account may be compromised")
Name	"The following user account was in a locked out state and the correct password was just provided"
Source Address	%3
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 516

ArcSight Field	Vendor Field
Device Custom Date 1	__concatenate(%5," ",%6)
Device Custom Date 1 Label	"Last Bad Password Attempt"
Device Custom Number 1	%4
Device Custom Number 1 Label	"Bad Password Count"
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Name	"The following user account has been locked out due to too many bad password attempts"
Source Address	%3
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 1102

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 5	%4
Device Custom String 5 Label	"Additional details"
Name	"The Federation Service authorized a request to one of the REST endpoints"
Request Url	%3
Source Address	%2

Event 1200

ArcSight Field	Vendor Field
Name	"The Federation Service issued a valid token"

Event 1201

ArcSight Field	Vendor Field
Name	"The Federation Service failed to issue a valid token"

Event 1202

ArcSight Field	Vendor Field
Name	"The Federation Service validated a new credential"

Event 1203

ArcSight Field	Vendor Field
Name	"The Federation Service failed to validate a new credential"

Event 1204

ArcSight Field	Vendor Field
Name	"A password was changed"

Event 1205

ArcSight Field	Vendor Field
Name	"A password change was attempted, but failed"

Event 1206

ArcSight Field	Vendor Field
Name	"A Sign Out request was successfully processed"

Event 1210

ArcSight Field	Vendor Field
Name	"An extranet lockout event has occurred"

Common Mappings for Events - 1200, 1201, 1202, 1203, 1204, 1205, 1206, and 1210

ArcSight Field	Vendor Field
Application Protocol	AuthProtocol
Destination Dns Domain	RelyingParty
Destination Host Name	__regexToken(Server)
Destination Service Name	__regexToken(Server)
Device Custom Date 1	LastBadAttempt
Device Custom Date 1 Label	"Last Bad Attempt"
Device Custom Number 1	__oneOfLong(CurrentBadPasswordCount)
Device Custom Number 1 Label	"Current Bad Password Count"
Device Custom Number 2	__oneOfLong(ConfigBadPasswordCount)
Device Custom Number 2 Label	"Config Bad Password Count"
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 5	ForwardedIpAddress
Device Custom String 5 Label	"Forwarded Ip Address"

ArcSight Field	Vendor Field
Device Custom String 6	AuditType
Device Custom String 6 Label	"Audit Type"
Device Domain	NetworkLocation
Device External Id	DeviceId
Device Process Name	ClaimsProvider
Event Outcome	AuditResult
Old File Hash	__concatenate("SSO Binding Validation Level:",SSOBindingValidationLevel)
Old File Name	__concatenate("Device Auth:",DeviceAuth)
Old File Path	__concatenate("Primary Auth:",PrimaryAuth)
Old File Type	__concatenate("Failure Type:",FailureType)
Reason	ErrorCode
Request Client Application	UserAgentString
Source Address	IpAddress
Source Nt Domain	__extractNTDomain(UserId)
Source Translated Address	__regexToken(ForwardedIpAddress)
Source User Name	__extractNTUser(UserId)

Active Directory

Active Directory, an essential component of the Windows architecture, presents organizations with a directory service designed for distributed computing environments. Active Directory lets organizations centrally manage and share information on network resources and users while acting as the central authority for network security.

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this section are specifically for the SmartConnector for Microsoft Active Directory Windows Event Log – Native: Active Directory.

Audit Active Directory Objects in Windows

When you use Windows auditing, you can track both user activities and Windows activities. When you use auditing, you can specify which events are written to the Security log. For example, the Security log can maintain a record of both valid and invalid logon attempts and events that relate to creating, opening, or deleting files or other objects.

When you audit Active Directory events, Windows writes an event to the Security log on the domain controller. For example, if a user attempts to log on to the domain using a domain user account and the logon attempt is unsuccessful, the event is recorded on the domain controller and not on the computer on which the logon attempt was made. This is because it is the domain controller that attempted to authenticate the logon attempt but could not do so.

To enable auditing of Active Directory objects:

1. Configure an audit policy setting for a domain controller. (When you configure an audit policy setting, you can audit objects, but you cannot specify which object you want to audit.)
2. Configure auditing for specific Active Directory Objects. After you specify the events to audit for files, folders, printers, and Active Directory Objects, Windows tracks and logs these events.

Configure an Audit Policy Setting for a Domain Controller

Auditing is turned off by default. For domain controllers, an audit policy setting is configured for all domain controllers in the domain. To audit events that occur on domain controllers, configure an audit policy setting that applies to all domain controllers in a non-Local Group Policy object (GPO) for the domain. You can access this policy setting through the Domain Controller's organizational unit. To audit user access to Active Directory objects, configure the Audit Directory Service Access event category in the audit policy setting.

The computer on which you want to configure an audit policy setting must be granted the Manage Auditing and Security Log user right. By default, Windows grants these rights to the Administrators group.

Note: The files and folders you want to audit must be on Microsoft Windows NT file system (NTFS) volumes.

To configure an audit policy setting for a domain controller (steps may vary for differing Windows operating systems):

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. From the **View** menu, click **Advanced Features**.
3. Right-click **Domain Controllers**; then click **Properties**.
4. Click the **Group Policy** tab, click **Default Domain Controller Policy**, and then click **Edit**.
5. Click **Computer Configuration**, double-click **Windows Settings**, double-click **Security Settings**, double-click **Local Policies**, and then double-click **Audit Policy**.
6. In the right pane, right-click **Audit Directory Services Access**, and then click **Security**.
7. Click **Define These Policy Settings**, then click to select one or both of the following check boxes:

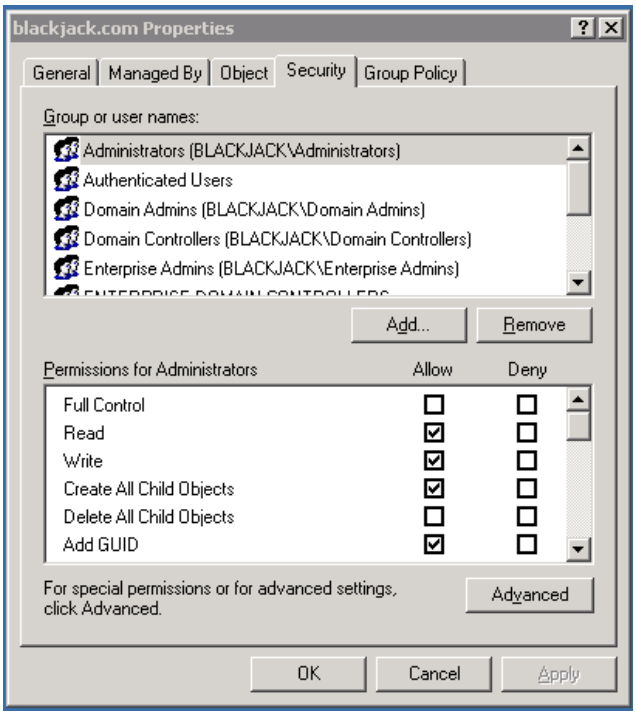
   Success: Click to audit successful attempts for the event category
   Failure: Click to audit failed attempts for the event category
8. Right-click any other event category that you want to audit; then click **Security**.
9. Click **OK**.
10. Because the changes you make to your computer's audit policy setting takes affect only when the policy setting is propagated (or applied) to your computer, to initiate policy propagation, either enter `secedit/refreshpolicy machine_policy` at the command prompt and then restart the computer or wait for automatic policy propagation, which occurs at regular intervals you can configure. By default policy propagation occurs every eight hours.

Configure Auditing for Specific Active Directory Objects

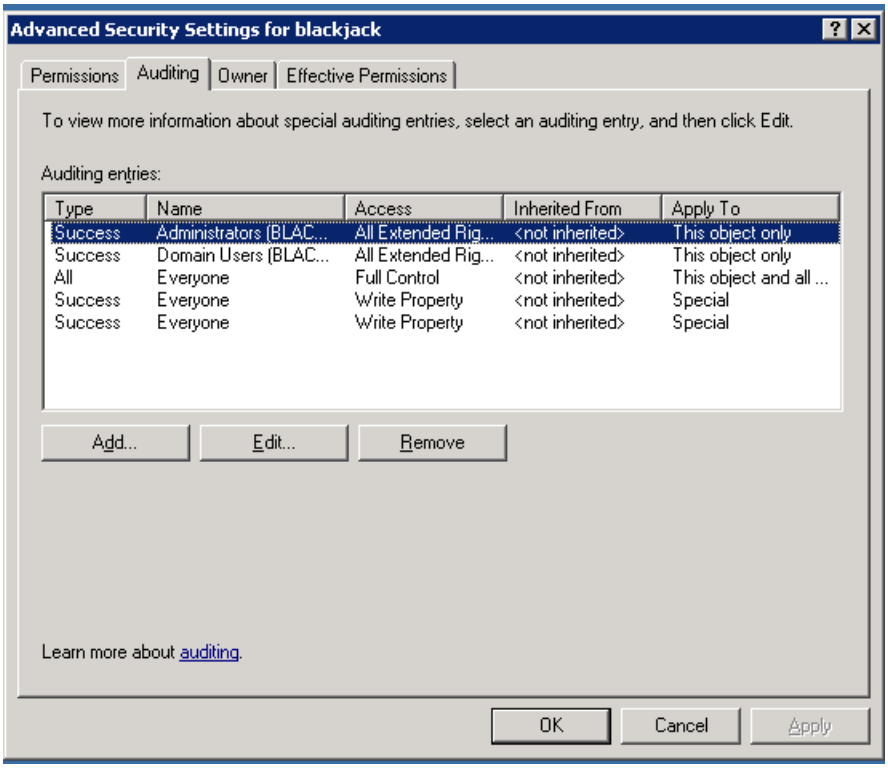
After you configure an audit policy setting, you can configure auditing for specific objects, such as users, computers, organizational units, or groups, by specifying both the types of access and the users whose access you want to audit.

To configure auditing for specific Active Directory objects (steps may vary for differing Windows operating systems):

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Verify that **Advanced Features** is selected on the **View** menu (the command has a checkmark beside it).
3. Right-click on the Active Directory object you want to audit (`blackjack.com` in the example) and select **Properties**.



4. Click the **Security** tab, then click the **Advanced** button; **Advanced Security Settings** for the object is displayed. Click the **Auditing** tab.



5. To add an object, click **Add**.
6. Either enter the name of either the user or the group whose access you want to audit in the **Enter the object name to select** box, then click **OK**, or browse the list of names and then double-click either the user or the group whose access you want to audit.
7. Click to select either the **Successful** checkbox or the **Failed** checkbox for the actions you want to audit, then click **OK**. Click **OK** on the next two windows to exit.

Active Directory Event Mappings

General Mappings

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

NTDS Database Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Microsoft Active Directory Domain services version)

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared. New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1404

ArcSight Field	Vendor Field
Name	'This directory service is now the intersite topology generator and has assumed responsibility for generating and maintaining intersite replication topologies for this site'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory has detected that the quota-tracking table is either missing or not completely built'
Message	'Active Directory has detected that the quota-tracking table is either missing or not completely built. The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2065

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has completed rebuilding the quota-tracking table. Quota enforcement is now in effect'

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

Windows 2008 NTDS Database Mappings

General

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	Microsoft Active Directory Domain services version

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Microsoft Active Directory Domain services version)

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared. New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1404

ArcSight Field	Vendor Field
Name	'This directory service is now the intersite topology generator and has assumed responsibility for generating and maintaining intersite replication topologies for this site'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory has detected that the quota-tracking table is either missing or not completely built'
Message	'Active Directory has detected that the quota-tracking table is either missing or not completely built. The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2065

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has completed rebuilding the quota-tracking table. Quota enforcement is now in effect'

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

General NTDS Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory startup complete'
Device Version	%1 (Microsoft Active Directory Domain Services version)

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	%2 (Destination network address)
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service
Source User Name	User

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory was unable to establish a connection with the global catalog'
Message	'Make sure a global catalog is available in the forest, and is reachable from this domain controller. You may use the nltest utility to diagnose this problem'
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)

ArcSight Field	Vendor Field
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Directory service

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1463

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected and deleted some possibly corrupted indices as part of initialization'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID
Destination Host name	%5 (source directory service address)

Event 1863

ArcSight Field	Vendor Field
Name	'This directory server has not received replication information from a number of directory servers within the configured latency interval'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of directory servers in all sites
Device Custom Number 2	Number of directory servers in this site
Device Custom Number 3	Latency Interval (Hours)
File Type	Registry Key
File Name	%5 (Registry Key)

Event 1864

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'Directory servers that do not replicate in a timely manner may encounter errors. They may miss password changes and be unable to authenticate. A DC that has not replicated in a tombstone lifetime may have missed the deletion of some objects, and may be automatically blocked from future replication until it is reconciled'
Device Custom String 1	Directory partition
Device Custom Number 1	More than 24 hours
Device Custom Number 2	More than a week
Device Custom Number 3	More than one month

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory has located a global catalog'
Device Custom String 5	Site
Destination Host Name	%1 (Global catalog)

Event 1898

ArcSight Field	Vendor Field
Name	'Internal event: Schema object was modified'
Device Custom String 5	Schema object
File Name	%1 (Schema object name)
File Type	'Schema object'

Event 1925

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link for writable directory partition failed'
Message	'This directory service will be unable to replicate with the source directory service until this problem is corrected'
Destination Host Name	%2 (Source directory service address)
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source directory service
Source User Name	User

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	%2 (Source domain controller address)
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
Source User Name	User

Event 2013

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services is rebuilding indices as part of the initialization process'
Device Custom Number 3	Indices

Event 2014

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services successfully completed rebuilding indice'
Device Custom Number 3	Indices

Event 2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'
Device Custom String 1	Event Code
Device Custom Number 3	Number of duplicate entries

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected that the quota-tracking table is either missing or not completely built'
Message	'The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Destination Host Name	%2 (Failing DNS host name)

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Destination Host Name	%2 (Failing DNS host name)

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	%4 (FSMO Role)

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

Windows 2008 General NTDS Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory startup complete'
Device Version	%1 (Microsoft Active Directory Domain Services version)

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	%2 (Destination network address)
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service
Source User Name	User

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory was unable to establish a connection with the global catalog'
Message	'Make sure a global catalog is available in the forest, and is reachable from this domain controller. You may use the nltest utility to diagnose this problem'

ArcSight Field	Vendor Field
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Directory service

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1463

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected and deleted some possibly corrupted indices as part of initialization'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID
Destination Host name	%5 (source directory service address)

Event 1863

ArcSight Field	Vendor Field
Name	'This directory server has not received replication information from a number of directory servers within the configured latency interval'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of directory servers in all sites
Device Custom Number 2	Number of directory servers in this site
Device Custom Number 3	Latency Interval (Hours)
File Type	Registry Key
File Name	%5 (Registry Key)

Event 1864

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'Directory servers that do not replicate in a timely manner may encounter errors. They may miss password changes and be unable to authenticate. A DC that has not replicated in a tombstone lifetime may have missed the deletion of some objects, and may be automatically blocked from future replication until it is reconciled'
Device Custom String 1	Directory partition

ArcSight Field	Vendor Field
Device Custom Number 1	More than 24 hours
Device Custom Number 2	More than a week
Device Custom Number 3	More than one month

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory has located a global catalog'
Device Custom String 5	Site
Destination Host Name	%1 (Global catalog)

Event 1898

ArcSight Field	Vendor Field
Name	'Internal event: Schema object was modified'
Device Custom String 5	Schema object
File Name	%1 (Schema object name)
File Type	'Schema object'

Event 1925

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link for writable directory partition failed'
Message	'This directory service will be unable to replicate with the source directory service until this problem is corrected'
Destination Host Name	%2 (Source directory service address)
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source directory service
Source User Name	User

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	%2 (Source domain controller address)
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
Source User Name	User

Event 2013

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services is rebuilding indices as part of the initialization process'
Device Custom Number 3	Indices

Event 2014

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services successfully completed rebuilding indice'
Device Custom Number 3	Indices

Event 2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'

ArcSight Field	Vendor Field
Device Custom String 1	Event Code
Device Custom Number 3	Number of duplicate entries

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected that the quota-tracking table is either missing or not completely built'
Message	'The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Destination Host Name	%2 (Failing DNS host name)

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Destination Host Name	%2 (Failing DNS host name)

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	%4 (FSMO Role)

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

NTDS ISAM Mappings

Event 102

ArcSight Field	Vendor Field
Name	'The database engine started a new instance'
Device Version	All of (%5,'.',%6,'.',%7,'.',%8)
Device Custom String 5	Instance ID

Event 103

ArcSight Field	Vendor Field
Name	'The database engine stopped the instance'
Device Custom String 5	Instance ID

Event 300

ArcSight Field	Vendor Field
Name	'The database engine is initiating recovery steps'

Event 301

ArcSight Field	Vendor Field
Name	'The database engine has begun replaying logfile'
File Name	%4 (logfile)
Device Custom Number 1	%7 (Time Seen)
Device Custom String 4	%5 (Processing Stats)
Device Custom String 5	%6 (Most Frequent Record Type)

Event 302

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed recovery steps'

Event 609

ArcSight Field	Vendor Field
Name	'The database engine is initiating index cleanup of database as a result of a Windows version upgrade'
Message	'This message is informational and does not indicate a problem in the database'
File Name	%4 (database)
Device Version	All of (%5,'.',%6,'.',%7,'.',%8)
Device Custom String 5	old device version

Event 611

ArcSight Field	Vendor Field
Name	'The secondary index of table will be rebuilt as a precautionary measure after the Windows version upgrade of this system'
File Name	%4 (database)
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 612

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed index cleanup on database'
File Name	%4 (database)

Event 614

ArcSight Field	Vendor Field
Name	'The secondary index of table may be corrupt'
Message	'If there is no later event showing the index being rebuilt, then please defragment the database to rebuild the index'
File Name	%4 (database)
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 626

ArcSight Field	Vendor Field
Name	'The database engine updated index entries in database because of a change in the NLS version'
Message	'This message is informational and does not indicate a problem in the database'

ArcSight Field	Vendor Field
Device Custom Number 3	Index entries
File Name	%5 (database)

Event 700

ArcSight Field	Vendor Field
Name	'Online defragmentation is beginning a full pass on database'
File Name	%4 (database)

Event 701

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed a full pass on database'
File Name	%4 (database)

Event 702

ArcSight Field	Vendor Field
Name	'Online defragmentation is resuming its pass on database'
File Name	%4 (database)

Event 703

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed the resumed pass on database'
File Name	%4 (database)

Event 704

ArcSight Field	Vendor Field
Name	'Online defragmentation of database was interrupted and terminated'
Message	'The next time online defragmentation is started on this database, it will resume from the point of interruption'
File Name	%4 (database)

Windows 2008 NTDS ISAM Mappings

Event 102

ArcSight Field	Vendor Field
Name	'The database engine started a new instance'
Device Version	All of (%5,'.',%6,'.',%7,'.',%8)
Device Custom String 5	Instance ID

Event 103

ArcSight Field	Vendor Field
Name	'The database engine stopped the instance'
Device Custom String 5	Instance ID

Event 300

ArcSight Field	Vendor Field
Name	'The database engine is initiating recovery steps'

Event 301

ArcSight Field	Vendor Field
Name	'The database engine has begun replaying logfile'
File Name	%4 (logfile)
Device Custom Number 1	%7
Device Custom String 4	%5
Device Custom String 5	%6

Event 302

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed recovery steps'

Event 609

ArcSight Field	Vendor Field
Name	'The database engine is initiating index cleanup of database as a result of a Windows version upgrade'
Message	'This message is informational and does not indicate a problem in the database'
File Name	%4 (database)
Device Version	All of (%5,'.',%6,'.',%7,'.',%8)
Device Custom String 5	old device version

Event 611

ArcSight Field	Vendor Field
Name	'The secondary index of table will be rebuilt as a precautionary measure after the Windows version upgrade of this system'
File Name	%4 (database)

ArcSight Field	Vendor Field
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 612

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed index cleanup on database'
File Name	%4 (database)

Event 614

ArcSight Field	Vendor Field
Name	'The secondary index of table may be corrupt'
Message	'If there is no later event showing the index being rebuilt, then please defragment the database to rebuild the index'
File Name	%4 (database)
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 626

ArcSight Field	Vendor Field
Name	'The database engine updated index entries in database because of a change in the NLS version'
Message	'This message is informational and does not indicate a problem in the database'
Device Custom Number 3	Index entries
File Name	%5 (database)

Event 700

ArcSight Field	Vendor Field
Name	'Online defragmentation is beginning a full pass on database'
File Name	%4 (database)

Event 701

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed a full pass on database'
File Name	%4 (database)

Event 702

ArcSight Field	Vendor Field
Name	'Online defragmentation is resuming its pass on database'
File Name	%4 (database)

Event 703

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed the resumed pass on database'
File Name	%4 (database)

Event 704

ArcSight Field	Vendor Field
Name	'Online defragmentation of database was interrupted and terminated'
Message	'The next time online defragmentation is started on this database, it will resume from the point of interruption'
File Name	%4 (database)

NTDS KCC Mappings

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	%2 (Destination network address)
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service

Event 1128

ArcSight Field	Vendor Field
Name	'A replication connection was created from source directory service to the local directory service'
Device Custom String 1	Creation Point Internal ID
Device Custom String 4	Reason or Error Code
Device Custom String 5	Local directory service
Device Custom String 6	Source directory service

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'

ArcSight Field	Vendor Field
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Domain service

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	%2 (Source domain controller address)
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller

Windows 2008 NTDS KCC Mappings

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	%2 (Destination network address)
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service

Event 1128

ArcSight Field	Vendor Field
Name	'A replication connection was created from source directory service to the local directory service'
Device Custom String 1	Creation Point Internal ID
Device Custom String 4	Reason or Error Code
Device Custom String 5	Local directory service
Device Custom String 6	Source directory service

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Domain service

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	%2 (Source domain controller address)
Destination User Name	User

ArcSight Field	Vendor Field
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller

Windows 2008 NTDS LDAP Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Version)

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was unable to establish a connection with the global catalog'
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID

Event 1220

ArcSight Field	Vendor Field
Name	'LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate'
Device Custom String 4	Reason or Error Code

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Directory service

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has located a global catalog'
Device Custom String 5	Site
Destination Host Name	%1 (Global catalog)

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Source Host Name	%2 (Failing DNS host name)

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Source Host Name	%2 (Failing DNS host name)

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923. Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher'
Device Custom Number 1	Number of simple binds performed without SSL/TLS
Device Custom Number 2	Number of Negotiate/Kerberos/NTLM/Digest binds performed without signing

NTDS Replication Mappings

Event 1188

ArcSight Field	Vendor Field
Name	'A thread in Active Directory Domain Services is waiting for the completion of a RPC made to directory service'
Message	'Active Directory Domain Services has attempted to cancel the call and recover this thread. If this condition continues, restart the directory service'
Device Custom String 1	Thread ID
Device Custom String 5	Operation
Device Custom String 6	Directory service
Device Custom Number 2	Timeout period (minutes)

Event 1232

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to perform a remote procedure call (RPC) to server. The call timed out and was cancelled'
Destination Host Name	%2 (Destination Host Name)
Device Custom Number 2	Call Timeout (Mins)
Device Custom String 1	Thread ID
Device Custom String 5	Internal ID
Source User Name	User

Event 1863

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'This directory server has not received replication information from a number of directory servers within the configured latency interval. To identify the directory servers by name, use the dcdiag.exe tool. You can also use the support tool repadmin.exe to display the replication latencies of the directory servers. The command is \"repadmin /showvector /latency <partition-dn>\"'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of domain controllers in all sites
Device Custom Number 3	Number of domain controllers in this site
Device Custom Number 2	Latency Interval (Hours)
File Type	Registry Key
File Name	Both (%5,'\\Replicator latency error interval(hours)')

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address. This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Source Host Name	%2 (Failing DNS host name)
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	FSMO Role

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923. Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher'
Device Custom Number 1	Number of simple binds performed without SSL/TLS
Device Custom Number 2	Number of Negotiate/Kerberos/NTLM/Digest binds performed without signing

Windows 2008 NTDS Replication Mappings

Event 1188

ArcSight Field	Vendor Field
Name	'A thread in Active Directory Domain Services is waiting for the completion of a RPC made to directory service'
Message	'Active Directory Domain Services has attempted to cancel the call and recover this thread. If this condition continues, restart the directory service'
Device Custom String 1	Thread ID
Device Custom String 5	Operation
Device Custom String 6	Directory service
Device Custom Number 2	Timeout period (minutes)

Event 1232

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to perform a remote procedure call (RPC) to server. The call timed out and was cancelled'
Destination Host Name	%2 (Destination Host Name)
Device Custom Number 2	Call Timeout (Mins)
Device Custom String 1	Thread ID
Device Custom String 5	Internal ID
Source User Name	User

Event 1863

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'This directory server has not received replication information from a number of directory servers within the configured latency interval. To identify the directory servers by name, use the dcdiag.exe tool. You can also use the support tool repadmin.exe to display the replication latencies of the directory servers. The command is \"repadmin /showvector /latency <partition-dn>\"'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of domain controllers in all sites
Device Custom Number 3	Number of domain controllers in this site
Device Custom Number 2	Latency Interval (Hours)
File Type	Registry Key
File Name	Both (%5,'\\Replicator latency error interval(hours)')

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address. This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Source Host Name	%2 (Failing DNS host name)
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	FSMO Role

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923. Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher'
Device Custom Number 1	Number of simple binds performed without SSL/TLS
Device Custom Number 2	Number of Negotiate/Kerberos/NTLM/Digest binds performed without signing

NTDS LDAP Mappings

1000

ArcSight Field	Vendor Field
Name	‘Microsoft Active Directory Domain Services startup complete’
Device Version	%1 (Version)

1004

ArcSight Field	Vendor Field
Name	‘Active Directory Domain Services was shut down successfully’

1126

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was unable to establish a connection with the global catalog'
Device Custom String 5	Internal ID
Device Custom String 4	Reason or Error Code
Reason	%3 (Reason or Error Code)

1138

ArcSight Field	Vendor Field
Name	'Function entered'
Message	Both ('Internal event:Function', %1,' entered')

1139

ArcSight Field	Vendor Field
Name	'Function exited'
Message	Both ('Internal event:Function',%1,' exited')

1213

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because it was disconnected on the client side'
Device Custom String 5	Internal ID

1215

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because the client closed the connection'
Device Custom String 5	Internal ID

1216

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because of an error'
Source Address	%1 (Source address)
Reason	%3 (Reason or Error Code)
Device Custom String 5	Internal ID

1220

ArcSight Field	Vendor Field
Name	'LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate'
Device Custom String 4	Reason or Error Code

1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed.'
Device Custom Number 3	Attempts

ArcSight Field	Vendor Field
Device Custom String 6	Directory service
Device Custom Number 2	Period of time (minutes)
Device Custom String 4	Reason or Error Code

1317

ArcSight Field	Vendor Field
Name	'The directory service has disconnected the LDAP connection'
Message	'The directory service has disconnected the LDAP connection from the following network address due to a time-out'
Source Address	%1 (Source address)

1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted.'

1535

ArcSight Field	Vendor Field
Name	'The LDAP server returned an error'
Message	Both ('The LDAP server returned an error value:',%1)
Reason	%1 (Reason or Error Code)

1655

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to communicate with the following global catalog and the attempts were unsuccessful'
Device Host Name	%1 (Host name)
Reason	%2 (Reason or Error Code)

1869

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has located a global catalog'
Destination Host Name	%1 (Host name)
Device Custom String 5	Site

2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'
Device Custom Number 3	Number of duplicate entries

2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions, and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources.'
Device Custom String 6	Source domain controller
Source Host Name	%2 (Host name)
Device Custom String 4	Reason or Error Code
File Type	'Registry Key'
File Name	All of (%5,'\\',%6)

2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers, or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 6	Alternate server name
Source Host Name	%2 (Host name)
Device Custom String 4	Reason or Error Code
File Type	'Registry Key'
File Name	All of (%5,'\\',%6)

2089

ArcSight Field	Vendor Field
Name	‘This directory partition has not been backed up’
Message	‘This directory partition has not been backed up since at least the following number of days’
Device Custom String 1	Directory partition
Device Custom Number 2	Latency interval (hours)
File Type	‘Registry Key’
File Name	All of (%3,’\\’,%4)

2886

ArcSight Field	Vendor Field
Name	‘The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a clear text (non-SSL/TLS-encrypted) connection.'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher.'

2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923. Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher.'
Device Custom Number 1	number of simple binds performed without SSL/TLS
Device Custom Number 2	number of negotiate/Kerberos/NTLM/Digest binds performed without signing

2889

ArcSight Field	Vendor Field
Name	‘LDAP bind without requesting signing or performed a simple bind’
Message	‘The following client performed a SASL (Negotiate/Kerberos/NTLM/Digest) LDAP bind without requesting signing (integrity verification), or performed a simple bind over a cleartext (non-SSL/TLS-encrypted) LDAP connection’
Source User Name	%2 (User name)
Source Address	%1 (Source address)

Windows 2012/Windows 8 NTDS LDAP Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Version)

1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

1126

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was unable to establish a connection with the global catalog'
Device Custom String 5	Internal ID
Device Custom String 4	Reason or Error Code
Reason	%3 (Reason or Error Code)

1138

ArcSight Field	Vendor Field
Name	'Function entered'
Message	Both ('Internal event:Function', %1,' entered')

1139

ArcSight Field	Vendor Field
Name	'Function exited'
Message	Both ('Internal event:Function',%1,' exited')

1213

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because it was disconnected on the client side'
Device Custom String 5	Internal ID

1215

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because the client closed the connection'
Device Custom String 5	Internal ID

1216

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because of an error'
Source Address	%1 (Source address)

ArcSight Field	Vendor Field
Reason	%3 (Reason or Error Code)
Device Custom String 5	Internal ID

1220

ArcSight Field	Vendor Field
Name	'LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate'
Device Custom String 4	Reason or Error Code

1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed.'
Device Custom Number 3	Attempts
Device Custom String 6	Directory service
Device Custom Number 2	Period of time (minutes)
Device Custom String 4	Reason or Error Code

1317

ArcSight Field	Vendor Field
Name	'The directory service has disconnected the LDAP connection'
Message	'The directory service has disconnected the LDAP connection from the following network address due to a time-out'
Source Address	%1 (Source address)

1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted.'

1535

ArcSight Field	Vendor Field
Name	'The LDAP server returned an error'
Message	Both ('The LDAP server returned an error value:',%1)
Reason	%1 (Reason or Error Code)

1655

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to communicate with the following global catalog and the attempts were unsuccessful'
Device Host Name	%1 (Host name)
Reason	%2 (Reason or Error Code)

1869

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has located a global catalog'
Destination Host Name	%1 (Host name)
Device Custom String 5	Site

2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'
Device Custom Number 3	Number of duplicate entries

2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions, and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources.'
Device Custom String 6	Source domain controller
Source Host Name	%2 (Host name)
Device Custom String 4	Reason or Error Code
File Type	'Registry Key'
File Name	All of (%5,'\\',%6)

2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers, or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 6	Alternate server name
Source Host Name	%2 (Host name)
Device Custom String 4	Reason or Error Code
File Type	'Registry Key'
File Name	All of (%5,'\\',%6)

2089

ArcSight Field	Vendor Field
Name	'This directory partition has not been backed up'
Message	'This directory partition has not been backed up since at least the following number of days'
Device Custom String 1	Directory partition
Device Custom Number 2	Latency interval (hours)
File Type	'Registry Key'
File Name	All of (%3,'\\',%4)

2886

ArcSight Field	Vendor Field
Name	‘The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a clear text (non-SSL/TLS-encrypted) connection.'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher.'

2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923. Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher.'

ArcSight Field	Vendor Field
Device Custom Number 1	number of simple binds performed without SSL/TLS
Device Custom Number 2	number of negotiate/Kerberos/NTLM/Digest binds performed without signing

2889

ArcSight Field	Vendor Field
Name	‘LDAP bind without requesting signing or performed a simple bind’
Message	‘The following client performed a SASL (Negotiate/Kerberos/NTLM/Digest) LDAP bind without requesting signing (integrity verification), or performed a simple bind over a cleartext (non-SSL/TLS-encrypted) LDAP connection’
Source User Name	%2 (User name)
Source Address	%1 (Source address)

Local Administrator Password Solution

MS Local Administrator Password Solution is a network service in Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, and Windows Server 2016 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Local Administrator Password Solution

Configuring MS Local Administrator Password Solution

For complete information about Microsoft's Reporting and MS Local Administrator Password Solution, see "Remote Access (DirectAccess, Routing and Remote Access)" topic in the TechNet Library for Windows Server: http://technet.microsoft.com/en-us/library/hh831416

Mappings for Microsoft Local Administrator Password Solution

Event 5

ArcSight Field	Vendor Field
Name	__ifThenElse(%1,,"Validation passed for new local admin password","Validation failed for new local admin password against local password policy")
Message	__ifThenElse(%1,,"Validation passed for new local admin password","Validation failed for new local admin password against local password policy")
Reason	%1

Event 10

ArcSight Field	Vendor Field
Name	__stringConstant("Password expiration too long for computer")
Message	__stringConstant("Password expiration too long for computer")
Device Action	__stringConstant("Resetting password now")
Device Custom Number 1	__safeToLong(%1)
Device Custom String1 Label	Excessive Days
Device Custom String2 Label	Days to change password

Event 11

ArcSight Field	Vendor Field
Name	__stringConstant("It is not necessary to change password yet")
Message	__stringConstant("It is not necessary to change password yet")
Device Custom Number 2	__safeToLong(%1)

Event 12

ArcSight Field	Vendor Field
Name	__stringConstant("Local Administrator password has been changed")
Message	__stringConstant("Local Administrator password has been changed")

Event 13

ArcSight Field	Vendor Field
Name	__stringConstant("Local Administrator password has been reported to AD")
Message	__stringConstant("Local Administrator password has been reported to AD")

Event 14

ArcSight Field	Vendor Field
Name	__stringConstant("Finished Successfully")
Message	__stringConstant("Finished Successfully")

Event 15

ArcSight Field	Vendor Field
Name	__stringConstant("Beginning Processing")
Message	__stringConstant("Beginning Processing")

Event 16

ArcSight Field	Vendor Field
Name	__stringConstant("Admin account management not enabled")
Message	__stringConstant("Admin account management not enabled")
Device Action	__stringConstant("Exiting")

Microsoft Antimalware Logs

Microsoft Antimalware is a network service in Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016.

Microsoft Antimalware is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your system.

The antimalware events are collected from the Windows Event system logs to your storage account. You can configure the storage account for your virtual machine to collect the antimalware events by selecting the appropriate storage account.

This section provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft antimalware and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this sectionare specifically for Microsoft Antimalware.

Mappings for Antimalware

Event 1000

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameters
Source Nt Domain	Domain

ArcSight Field	Vendor Field
Source User Name	User
Sid	SID
File Path	Scan resources

Event 1001

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Device Custom Number 1	Scan Time Hours
Device Custom Number 2	Scan Time Minutes
Device Custom Number 3	Scan Time Seconds

Event 1002

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Sid	SID

Event 1005

ArcSight Field	Vendor Field
Device Custom String 1 Label	Scan ID
Device Custom String 1	Scan ID
Device Custom String 5	Error Code
Device Custom String 5 Label	Error Code
Device Event Category	Scan Type
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Reason	Error Code

Event 1011

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Device Custom String 1	Threat Name
Device Custom Number 1	Threat ID
Device Custom Number 2	Severity ID
Device Custom Number 3	Category ID
FWLink	FWLink
File Path	Path
Device Severity	Severity Name
Device Custom String 4	Category Name
Device Custom String2	Signature Version
(Concatenating both the fields)	Engine Version

Event 1013

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom Date1	Timestamp
Source Nt Domain	Domain
Source User Name	User
Sid	SID

Event 1116

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 5	Detection ID
Device Custom Date 1	Detection Time
Device Custom Number 1	Threat ID
Device Custom String 1	Threat Name
Device Custom Number 2	Severity ID
Device Custom String 3	Severity Name
Device Custom Number 3	Category ID
Device Custom String 4	Category Name
FWLink	FWLink
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
Source Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
File Path	Path
Origin ID	Origin ID
Origin Name	Origin Name

ArcSight Field	Vendor Field
Execution ID	Execution ID
Execution Name	Execution Name
Type ID	Type ID
Old File Type	Type Name
Pre Execution Status	Pre Execution Status
Action ID	Action ID
Device Action	Action Name
Error Code	Error Code
Reason	Error Description
Post Clean Status	Post Clean Status
Additional Action ID	Additional Action ID
Additional Action String	Additional Action String
Remediation User	Remediation User
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Signature Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Engine Version

Event 1117

ArcSight Field	Vendor Field
Product Version	Device Version
Detection ID	Device Custom String 5
Detection Time	Device Custom Date 1
Threat ID	Device Custom Number 1
Threat Name	Device Custom String 1
Severity ID	Device Custom Number 2
Severity Name	Device Custom String 3
Category ID	Device Custom Number 3
Category Name	Device Custom String 4
FWLink	FWLink

ArcSight Field	Vendor Field
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
Source Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
File Path	Path
Origin ID	Origin ID
Origin Name	Origin Name
Execution ID	Execution ID
Execution Name	Execution Name
Type ID	Type ID
Old File Type	Type Name
Pre Execution Status	Pre Execution Status
Action ID	Action ID
Device Action Name	Action Name
Error Code	Error Code
Reason	Error Description
Post Clean Status	Post Clean Status
Additional Action ID	Additional Action ID
Additional Action String	Additional Action String
Remediation User	Remediation User
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Signature Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Engine Version

Event 1150

ArcSight Field	Vendor Field
Device Version	Product Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Signature Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Engine Version

Event 2000

ArcSight Field	Vendor Field
Device Venison	Product Version
File Id	Current Signature Version
Old File Id	Previous Signature Version
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Update Type Index	Update Type Index
Device Custom String 6	Update Type
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Current Engine Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Previous Engine Version

Event 2001

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain

ArcSight Field	Vendor Field
Source User Name	User
Sid	SID
Device Custom String 5	Error Code
Reason	Error Description
File Path	FWLink

Event 2002

ArcSight Field	Vendor Field
Product Verison	Device Version
(Concatenating both Previous Engine Version and Current Version in Device Custom String 2	Previous Engine Version
(Concatenating both Previous Engine Version and Current Version in Device Custom String 2	Current Engine Version
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Feature Index	Feature Index
Feature Name	Feature Index Name

Event 2010

ArcSight Field	Vendor Field
Device Version	Product Version
File Id	Current Signature Version
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String 2	Current Engine Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type

ArcSight Field	Vendor Field
File Path	Persistence Path
Dynamic Signature Version	Dynamic Signature Version
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type
Persistence Limit Value	Persistence Limit Value

Event 2011

ArcSight Field	Vendor Field
Device Version	Product Version
File Id	Current Signature Version
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String 2	Current Engine Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path
Dynamic Signature Version	Dynamic Signature Version
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type
Persistence Limit Value	Persistence Limit Value
Removal Reason Index	Removal Reason Index
Reason	Removal Reason Value

Event 3002

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 5	Error Code
Reason	Error Description

Event 5000

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5001

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5004

ArcSight Field	Vendor Field
Device Version	Product Version
File Hash	Feature Name
File Id	Feature ID
Device Custom Number 1	Configuration
Device Custom Number 1 Label	Configuration

Event 5007

ArcSight Field	Vendor Field
Device Version	Product Version
Old File Name	Old Value
File Name	New Value

Event 5010

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5012

ArcSight Field	Vendor Field
Device Version	Product Version

Microsoft Windows Defender AntiVirus

Microsoft Windows Defender AntiVirus is a network service in Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, and Windows Server 2016 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

This section provides information about configuring Microsoft Windows Defender AntiVirus as a log source and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Microsoft Windows Defender AntiVirus

For complete information about Microsoft's Reporting and Microsoft Windows Defender AntiVirus, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)": http://technet.microsoft.com/en-us/library/hh831416

Mappings for Microsoft Windows Defender AntiVirus

Event 1000

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String1 Label	"Scan ID"
Device Custom String1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameter
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
File Path	Scan Resources

Event 1001

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String1 Label	"Scan ID"
Device Custom String1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameter
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom Number1 Label	"Hours"
Device Custom Number1	Scan Time Hours

ArcSight Field	Vendor Field
Device Custom Number2 Label	"Minutes"
Device Custom Number2	Scan Time Minutes
Device Custom Number3 Label	"Seconds"
Device Custom Number3	Scan Time Seconds

Event 1002

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String1 Label	"Scan ID"
Device Custom String1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameter
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID

Event 1009

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID

ArcSight Field	Vendor Field
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
FWLink	FWLink
File Path	Path
Old File ID	Severity Name
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
Device Custom String2Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version

Event 1011

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
FWLink	FWLink
File Path	Path
Old File ID	Severity Name
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
Device Custom String2Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version

Event 1013

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom Date1 Label	"Action Time"
Device Custom Date1	Timestamp
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID

Event 1015

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
Device Custom String6 Label	"Detection ID"
Device Custom String6	Detection ID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
FWLink	FWLink

ArcSight Field	Vendor Field
Source Process Name	Process Name
File Path	Path Found
Request Context	Detection Origin
Old File Type	Detection Type
Source Service Name	Detection Source

Event 1116

ArcSight Field	Vendor Field
Device Version	Product Version
Start Time	Detection Time
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
Device Custom String6 Label	"Detection ID"
Device Custom String6	Detection ID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
Old File ID	Severity Name
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
FWLink	FWLink

ArcSight Field	Vendor Field
File Path	Path
Request context	Detection Origin
Source Service Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
Origin ID	Origin ID
Request Context	Origin Name
Execution ID	Execution ID
Execution Name	Execution Name
Type ID	Type ID
Old File Type	Type Name
Pre Execution Status	Pre Execution Status
Action ID	Action ID
Device Action	Action Name
Reason	Error Code
Device Custom String5 Label	"Error Description"
Device Custom String5	Error Description
Post Clean Status	Post Clean Status
Additional Actions ID	Additional Actions ID
Remediation User	Remediation User

Event 1117

ArcSight Field	Vendor Field
Device Version	Product Version
Start Time	Detection Time
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"

ArcSight Field	Vendor Field
Device Custom Number3	Category ID
Device Custom String6 Label	"Detection ID"
Device Custom String6	Detection ID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
Old File ID	Severity Name
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
FWLink	FWLink
File Path	Path
Request context	Detection Origin
Source Service Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
Origin ID	Origin ID
Request Context	Origin Name
Execution ID	Execution ID
Execution Name	Execution Name
Type ID	Type ID
Old File Type	Type Name
Pre Execution Status	Pre Execution Status
Action ID	Action ID
Device Action	Action Name
Reason	Error Code
Device Custom String5 Label	"Error Description"

ArcSight Field	Vendor Field
Device Custom String5	Error Description
Post Clean Status	Post Clean Status
Additional Actions ID	Additional Actions ID
Remediation User	Remediation User

Event 1150

ArcSight Field	Vendor Field
Device Version	Platform Version
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version

Event 1151

ArcSight Field	Vendor Field
Device Version	Platform Version
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version
Device Custom String1 Label	"RTP State/ OA State/ IOAV State/ BM State"
Device Custom String 1	RTP State/ OA State/ IOAV State/ BM State
Device Custom Number1	safeToLong(updateRevisionNumber)
Device Custom Number1 Label	"Last AV Signature Age"
Device Custom Number1	AV signature age
Device Custom Number2 Label	"Last AS Signature Age"
Device Custom Number2	AS signature age
Device Custom Number3 Label	"Last quick scan age"
Device Custom Number3	Last quick scan age
Device Floating Point1 Label	"Last full scan age"
Device Floating Point1	Last full scan age
File Create Time	AV signature creation time
Old File Create Time	AS signature creation time
Start Time	Last quick scan start time

ArcSight Field	Vendor Field
End Time	Last quick scan end time
Device Custom String4 Label	"Last Quick Scan Source"
Device Custom String4	Last quick scan source
Device Custom Date1 Label	"Last full scan start time"
Device Custom Date1	Last full scan start time
Device Custom Date2 Label	"Last full scan end time"
Device Custom Date2	Last full scan end time
Device Custom String6 Label	"Last full scan source"
Device Custom String6	Last full scan source
Product status	Product status

Event 2000

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Update Type Index	Update Type Index
Device Custom String6 Label	"Update Type"
Device Custom String6	Update Type
Device Custom String2 Label	"Current Engine Version/Previous Engine Version/Current Signature Version/Previous Signature Version"
Device Custom String2	Current Engine Version,Previous Engine Version,Current Signature Version,Previous Signature Version

Event 2001

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain

ArcSight Field	Vendor Field
Source User Name	User
Source User ID	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Update Type Index	Update Type Index
Device Custom String6 Label	"Update Type"
Device Custom String6	Update Type
Device Custom String2 Label	"Current Engine Version/Previous Engine Version/Current Signature Version/Previous Signature Version"
Device Custom String2	Current Engine Version,Previous Engine Version,Current Signature Version,Previous Signature Version
Reason	Error Code
Device Custom String5 Label	"Error Description"
Device Custom String5	Error Description
File Path	Source Path

Event 2002

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom String2 Label	"Current/ Previous Engine Version"
Device Custom String2	Current Engine Version, Previous Engine Version
Feature Index	Feature Index
Device Event Category	Feature Name

Event 2010

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain

ArcSight Field	Vendor Field
Source User Name	User
Source User ID	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String2 Label	"Current Engine Version/Current Signature Version"
Device Custom String2	Current Engine Version,Current Signature Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path
Device Custom String1 Label	"Dynamic Signature Version"
Device Custom String1	Dynamic Signature Version
Device Custom Date1 Label	"Dynamic Signature Compilation Timestamp"
Device Custom Date1	Dynamic Signature Compilation Timestamp
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type
Persistence Limit Value	Persistence Limit Value

Event 2011

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String2 Label	"Current Engine Version/Current Signature Version"
Device Custom String2	Current Engine Version,Current Signature Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path

ArcSight Field	Vendor Field
Device Custom String1 Label	"Dynamic Signature Version"
Device Custom String1	Dynamic Signature Version
Device Custom Date1 Label	"Dynamic Signature Compilation Timestamp"
Device Custom Date1	Dynamic Signature Compilation Timestamp
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type
Persistence Limit Value	Persistence Limit Value
Removal Reason Index	Removal Reason Index
Reason	Removal Reason Value

Event 2030

ArcSight Field	Vendor Field
Device Version	Product Version

Event 3002

ArcSight Field	Vendor Field
Device Version	Product Version
File ID	Feature ID
File Hash	Feature Name
Reason	Error Code
Device Custom String5 Label	"Error Description"
Device Custom String5	Error Description

Event 5000

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5001

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5004

ArcSight Field	Vendor Field
Device Version	Product Version
File Hash	Feature Name
Device Custom Number	"Configuration"
Device Custom Number1 Label	Configuration
File ID	Feature ID

Event 5007

ArcSight Field	Vendor Field
Device Version	Product Version
Old File Name	Old Value
File Name	"New Value"

Event 5010

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5012

ArcSight Field	Vendor Field
Device Version	Product Version

Microsoft DNS Server Analytics

Microsoft DNS Server Analytic Logs is a Windows system service and device driver that enables the Microsoft Windows Event Log – Native (WiNC) SmartConnector to monitor and collect the analytic events / logs from the DNS Server.

It provides information about operational events such as dynamic updates, zone transfers, and DNSSEC zone signing and unsigning.

This section provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft DNS Server Analytic Logs and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Configuring Microsoft DNS Server Analytic Logs

For information about configuring Microsoft DNS Logging and Microsoft DNS analytic events logs, see Microsofts DNS Logging and Diagnostics.

Mappings for Microsoft DNS Server Analytic Logs

General

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'DNS Server Analytic'
Device Version	'Unknown'

Event ID 256

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP

ArcSight Field	Vendor Field
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"QUERY_RECEIVED"
Old File Id	RD

Event ID 257

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 2	DNSSEC
Device Custom Number 2 Label	"DNSSEC"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"

ArcSight Field	Vendor Field
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"RESPONSE_SUCCESS"
Old File Id	AA,AD
Request Context	Zone
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event ID 258

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"RESPONSE_FAILURE"

ArcSight Field	Vendor Field
Reason	Reason
Request Context	Zone
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event ID 259

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Direction	Inbound/Outbound
File Hash	AdditionalInfo
Name	"IGNORED_QUERY"
Reason	Reason
Request Context	Zone
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event ID 260

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"RECURSE_QUERY_OUT"
Old File Id	RD
Old File Hash	RecursionScope,CacheScope
Request Cookies	"Recursive query"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event ID 261

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags

ArcSight Field	Vendor Field
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"RECURSE_RESPONSE_IN"
Old File Id	AA,AD
Old File Hash	RecursionScope,CacheScope
Request Cookies	"Recursive query"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event ID 262

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Hash	AdditionalInfo
Name	"RECURSE_QUERY_TIMEOUT"

ArcSight Field	Vendor Field
Old File Hash	RecursionScope,CacheScope
Request Cookies	"Recursive query"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event ID 263

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 2	Secure
Device Custom Number 2 Label	"SECURE"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"DYN_UPDATE_RECV"
Request Cookies	"Dynamic update"
Request Url	QNAME
Source Port	Port
Source Address	Source

Event ID 264

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"

ArcSight Field	Vendor Field
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"DYN_UPDATE_RESPONSE"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Dynamic update"
Request Url	QNAME
Source Address	InterfaceIP

Event ID 265

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"IXFR_REQ_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event ID 266

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"IXFR_REQ_RECV"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event ID 267

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"IXFR_RESP_OUT"
Old File Hash	ZoneScope
Request Context	Zone

ArcSight Field	Vendor Field
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	InterfaceIP

Event ID 268

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"IXFR_RESP_RECV"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	InterfaceIP

Event ID 269

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound

ArcSight Field	Vendor Field
File Size	BufferSize
Name	"AXFR_REQ_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event ID 270

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"AXFR_REQ_RECV"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event ID 271

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID

ArcSight Field	Vendor Field
Device Custom String 4 Label	"XID"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
Name	"AXFR_RESP_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	InterfaceIP

Event ID 272

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
Name	"AXFR_RESP_RECV"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	InterfaceIP

Event ID 273

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"XFR_NOTIFY_RECV"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event ID 274

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"XFR_NOTIFY_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event ID 275

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"XFR_NOTIFY_ACK_IN"

ArcSight Field	Vendor Field
Old File Hash	ZoneScope
Request Cookies	"Zone XFR"
Source Address	Source

Event ID 276

ArcSight Field	Vendor Field
Destination Address	Destination
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"XFR_NOTIFY_ACK_OUT"
Request Context	Zone
Request Cookies	"Zone XFR"
Source Address	InterfaceIP

Event ID 277

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
Name	"DYN_UPDATE_FORWARD"
Request Context	Zone
Request Cookies	"Dynamic update"
Source Address	ForwardInterfaceIP

Event ID 278

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom String 4	XID
Device Custom String 4 Label	"XID"

ArcSight Field	Vendor Field
Device Direction	Inbound/Outbound
Name	"DYN_UPDATE_RESPONSE_IN"
Request Context	Zone
Request Cookies	"Dynamic update"
Request Url	QNAME
Source Address	Source

Event ID 279

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"INTERNAL_LOOKUP_CNAME"
Old File Id	RD
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	Source

Event ID 280

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"INTERNAL_LOOKUP_ADDITIONAL"
Old File Id	RD
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	Source

Microsoft Exchange Mailbox Access Auditing

Microsoft Exchange Server is the server side of a client-server, collaborative application product developed by Microsoft. It is part of Microsoft's line of server products, used by enterprises using Microsoft infrastructure solutions. Microsoft Exchange 2007 Service Pack 2 is supported by this SmartConnector.

This section provides information about the SmartConnector for Microsoft Exchange Access Auditing Windows Event Log Native and its event mappings to ArcSight data fields. This connector supports Microsoft Exchange Server 2007 and 2007 SP3 audit application events for Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 versions.

With Exchange Server 2010, Microsoft has added new native audit capabilities, such that the audit logs are maintained in the mailboxes themselves. Being able to get those audit logs is

very difficult due to the potential number of mailboxes and the vast amount of data they may contain, and Windows Event Log integration for this will not work.

Therefore, for Microsoft Exchange 2010 and later versions, use the SmartConnector for Microsoft Exchange PowerShell, which retrieves Microsoft Exchange Server 2010 SP2 and 2013 Mailbox Audit logs remotely, and lets you specify the mailboxes to be audited.

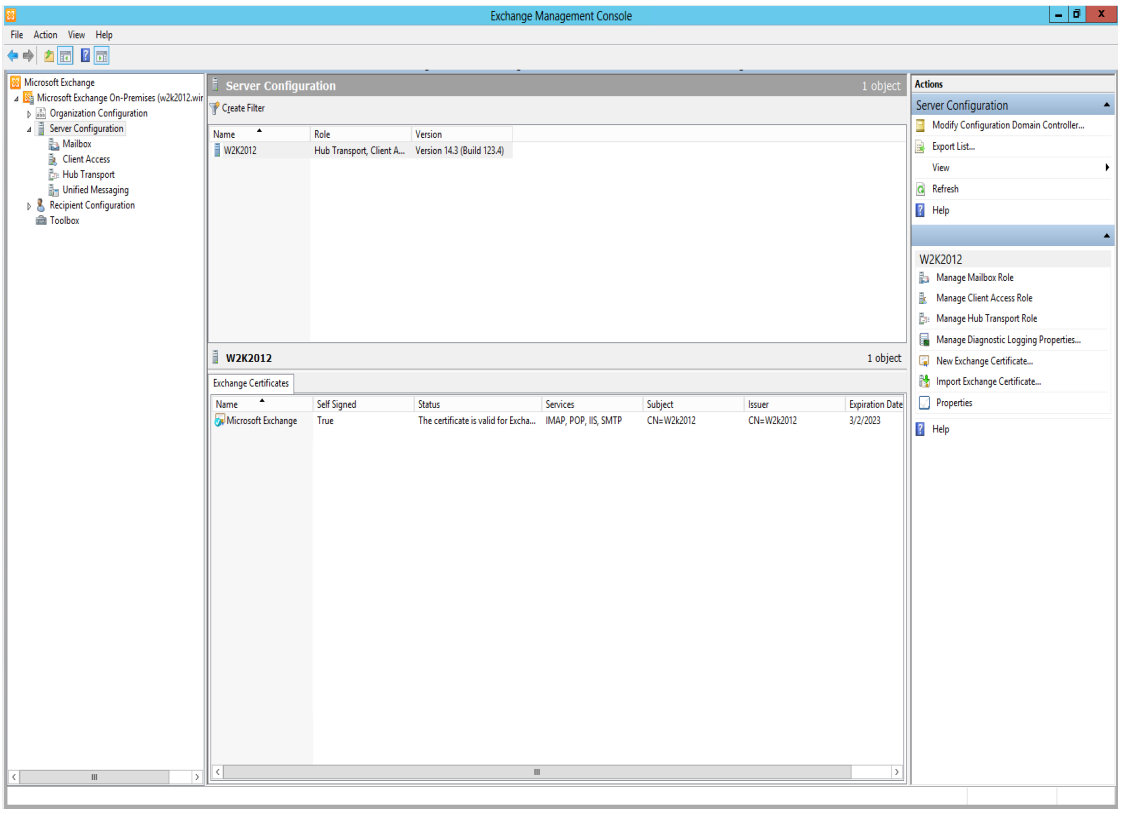
The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft Exchange Audit.

Configuring Mailbox Access Auditing

Use the Exchange Management Console to access the configuration area for mailbox access auditing.

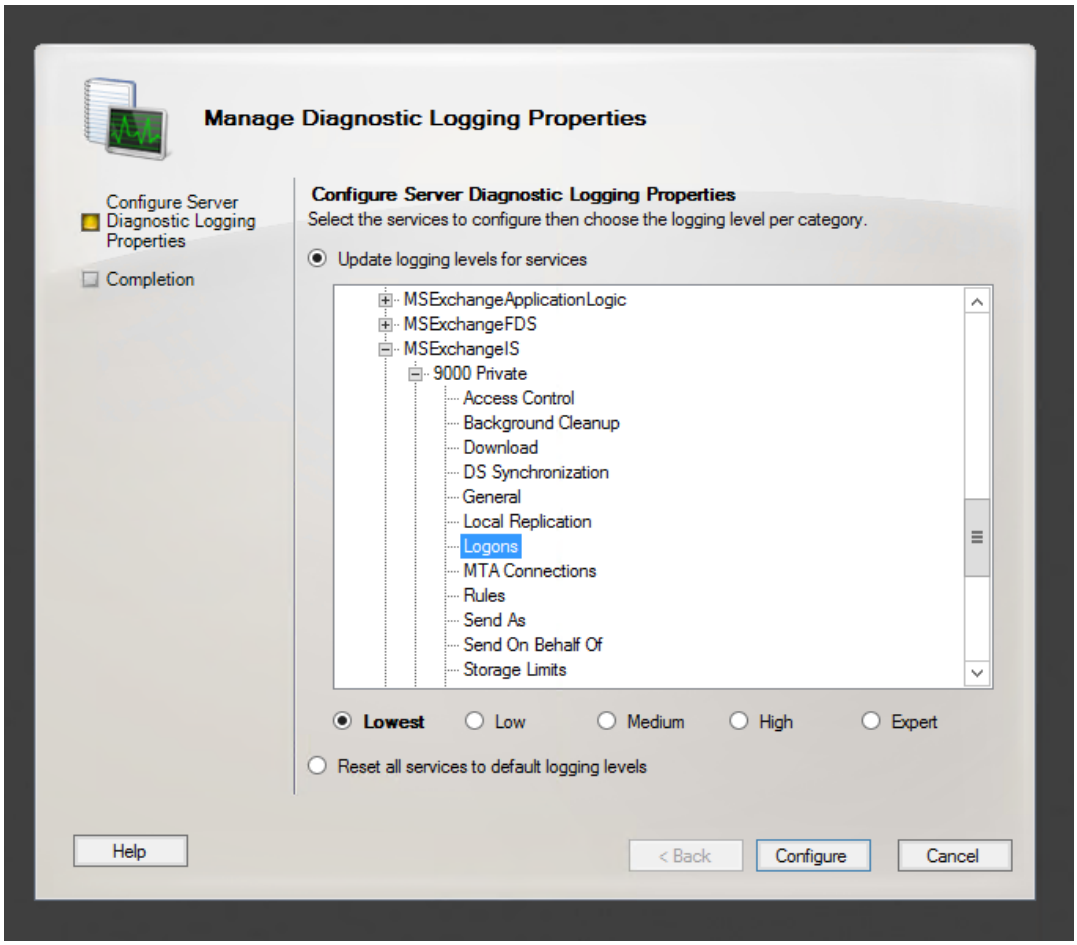
Enabling Mailbox Access Auditing

The following figure shows the new **Manage Diagnostic Logging Properties** menu option.



To configure mailbox access auditing on a particular mailbox server:

1. Select that server in the Exchange Management Console and then select the **Manage Diagnostics Logging Properties** menu option from the action pane; the **Manage Diagnostics Logging Properties** window is displayed.



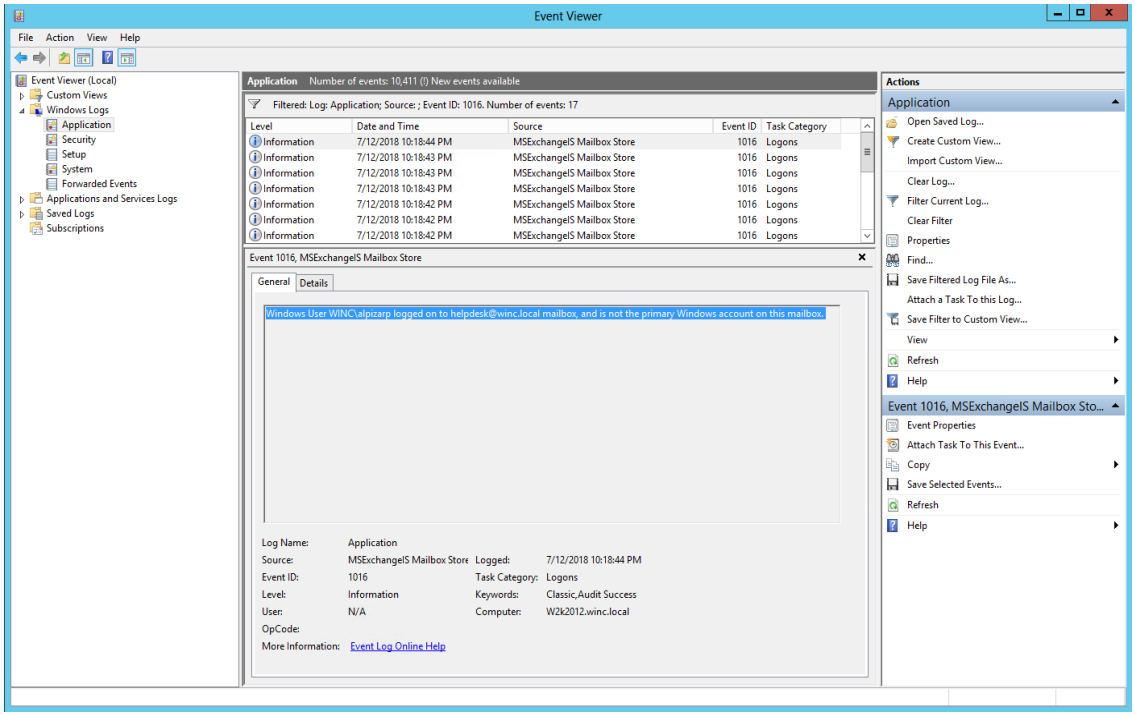
2. Expand the **MSExchangeIS** category and then expand the **9000 Private** category.
3. Under the **MSExchangeIS\9000 Private** category, configure auditing for any or all of the four possible actions:
   - Folder Access, to log events that correspond to opening folders, such as the Inbox, Outbox, or Sent Items folders
   - Message Access, to log events that correspond to explicitly opening messages
   - Extended Send As, to log events that correspond to sending a message as a mailbox-enabled user
   - Extended Send On Behalf Of, to log events that correspond to sending a message on behalf of a mailbox-enabled user.
4. When you complete the auditing level configuration, click **Configure**.

For more information about Exchange mailbox access auditing, see http://www.msexchange.org/articles_tutorials/exchange-server-2007/compliance-policies-archiving/exchange-2007-mailbox-access-auditing-part1.html

For examples of configuring Exchange mailbox access auditing, see http://www.howexchangeworks.com/2009/09/mailbox-access-auditing-in-exchange.html

Accessing the Audited Information

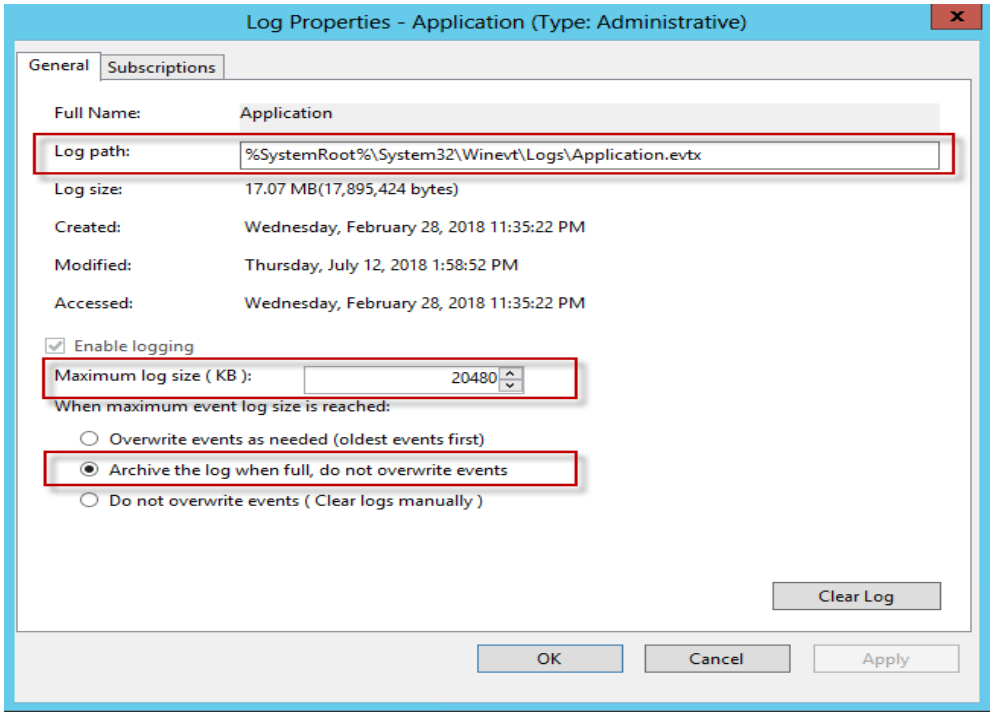
To view the information logged, navigate to **Event Viewer** > **Applications & Services Log** > **Exchange Auditing**.



Changing Default Log Storage location

By default, the logs are stored in the Exchange Server installation directory (`Drive\Program Files\Microsoft\Exchange Server\Logging\AuditLogs`). The logs are archived by default when the location gets full. Therefore, make sure that the location of the logs is changed to a drive that has enough free space.

To modify the log storage location, select the properties for the Exchange Auditing log and change the options.



Excluding Service Accounts

Service accounts that have full access to the mailboxes might fill up your mailbox access log with events. To exclude service accounts from being audited, run the following command:

```
Get-MailboxDatabase -identity "server\sg\dbname" | Add-ADPermission -User "service account" -ExtendedRights ms-Exch-Store-Bypass-Access-Auditing -InheritanceType All
```

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Exchange Events 10100, 10101 Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom String 4	Mailbox Name
Device Custom String 5	Relatively Unique Identifier
File Name	%2 (Message ID or Folder name depending upon event)
File Path	%1 (Folder path)

ArcSight ESM Field	Device-Specific Field
Name	A folder in mailbox was opened by user.
Source Host Name	%9 (Account Name)
Source Process Name	%11 (Process Name)
Source Service Name	%13 (Application ID)
Target Address	Address
Destination User ID	%5 (Accessing User (full Exchange ID))
Destination User Name	%4 (Account Name)
Destination User Privileges	One of (‘Administrative rights were used’, ‘ ‘)

Exchange Event 10102 Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom Number 3	Administrative Rights
Device Custom String 4	Mailbox Name
Device Custom String 5	Identifier
Device Custom String 6	Administrative Rights
File Name	Message ID or Folder name, depending upon event
File Path	Folder path (when relevant)
Name	A message in mailbox was opened by user.
Source Host Name	Machine Name
Source Process Name	Process Name
Source Service Name	Application ID
Source User ID	Accessing User (full Exchange ID)
Source User Name	Account Name
Target Address	Address

Exchange Events 10104, 10106 Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom String 4	Mailbox Name
Device Custom String 5	Relatively Unique Identifier
Device Custom String 6	Sent as user
File Name	%3 (Message ID or Folder name, depending upon event)
Name	User sent a message on behalf of another user.
Source Host Name	10% (Machine Name)
Source Process Name	12% (Process Name)
Source Service Name	14% (Application ID)
Destination User ID	%6 (Accessing User (full Exchange ID))
Destination User Name	%5 (Account Name)
Destination User Privileges	One of (‘Administrative rights were used’, ‘ ‘)
Destination Host Name	%11 (Address)
Destination Address	%11 (Address)

Exchange Online Message Tracking

Message tracking, or message tracing, as it is called in Office 365, is one of the most basic tools used by administrators to monitor the email flow. As emails travel through Office 365, some information about them gets stored in logs and is available for administrative purposes. No matter if users delete or purge messages, the administrator is able to view basic information about sent and received emails.

This section provides information about configuring Exchange Online Message Tracking and event mappings.

Message tracing does not allow you to peek into a message's contents. Still, it can provide quite a lot of important data about emails:

- Sender and Recipient
- Send and receive dates
- Subject and size
- Status and details of events. There are seven possible values in the delivery status field: delivered, failed, pending, expanded, quarantined, filtered as spam and unknown.
- IP address used to send the message
- Message ID a unique number identifying a message. If a message is sent to more than one recipient, it will display once for every recipient in the message trace search, but all those entries will have the same Message-ID and different Message Trace ID

Device Event Mapping to ArcSight Fields

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

ArcSight ESM Field	Device-Specific Field
Device Vendor	'Microsoft'
Device Product	'Exchange Online'
Name	Both('Message ',Status)
External Id	MessageTraceId
Device Receipt Time	Received
Device Event Class Id	Both('Message ',Status)
Device Custom String 3	Subject
Device Custom String 6	Organization

ArcSight ESM Field	Device-Specific Field
Source Address	FromIP
Source User Name	SenderAddress
Destination Address	ToIP
Destination User Name	RecipientAddress
File Size	Size
File Id	MessageId

Microsoft Exchange Mailbox Store

Microsoft Exchange Server is the server side of a client-server, collaborative application product developed by Microsoft. It is part of Microsoft's line of server products, used by enterprises using Microsoft infrastructure solutions. Microsoft Exchange 2010 Service Pack 1 is supported by this SmartConnector.

This section provides information about configuring Microsoft Exchange Mailbox Store and understanding its event mappings to ArcSight data fields. This connector supports , Windows Server 2008 R2.

With Exchange Server 2010, Microsoft has added new native audit capabilities, such that the audit logs are maintained in the mailboxes themselves. Being able to get those audit logs is very difficult due to the potential number of mailboxes and the vast amount of data they may contain, and Windows Event Log integration for this will not work.

Therefore, for Microsoft Exchange 2010 and later versions, use the SmartConnector for Microsoft Exchange PowerShell, which retrieves Microsoft Exchange Server 2010 SP1 and 2013 Mailbox Audit logs remotely, and lets you specify the mailboxes to be audited.

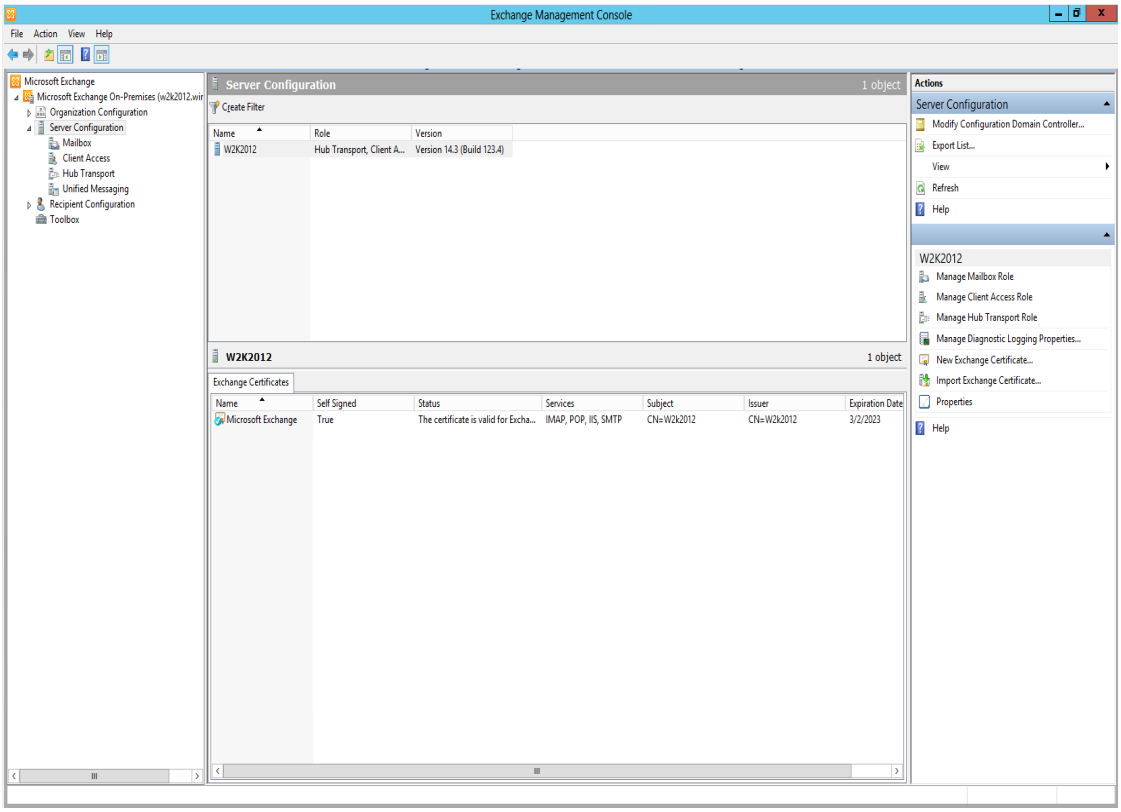
The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Microsoft Exchange Mailbox Store Windows Event Log Native.

Configuring Mailbox Store Auditing

Use the Exchange Management Console to access the configuration area for mailbox store auditing.

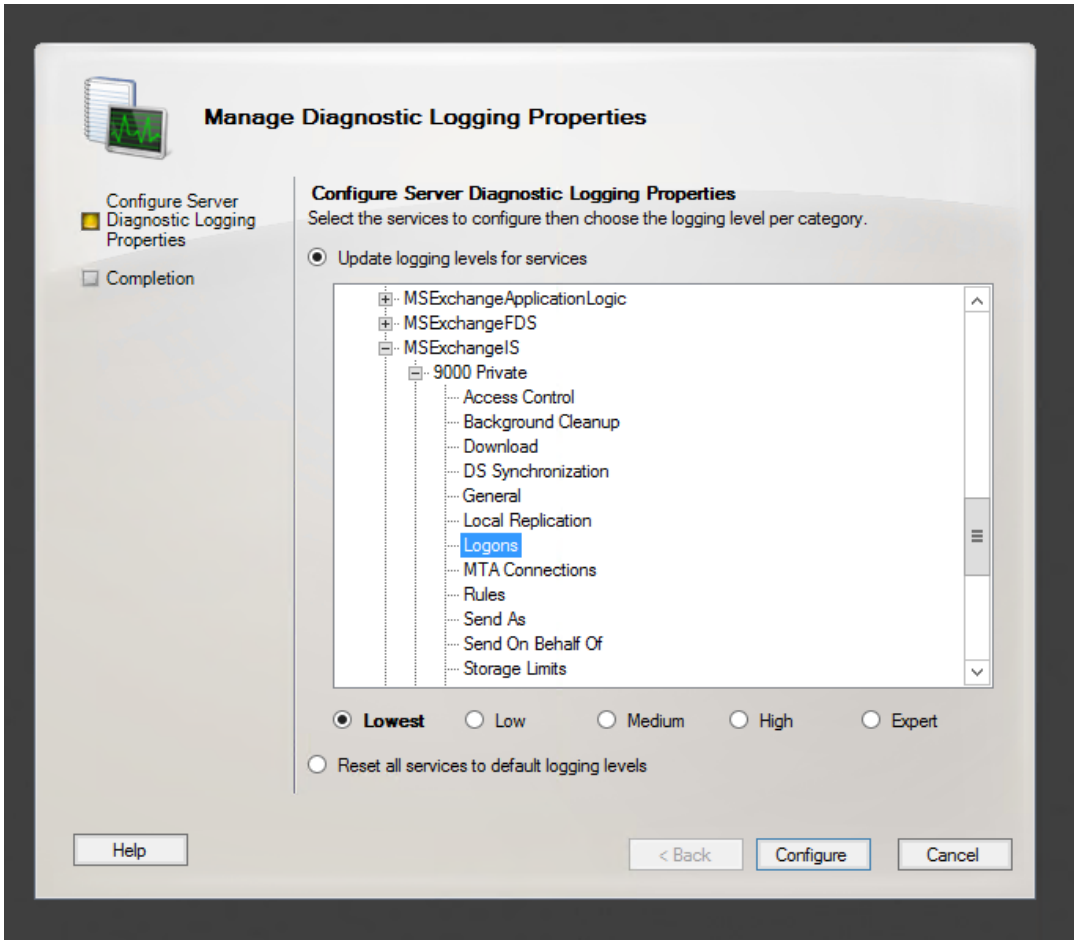
Enabling Mailbox Store

To access the configuration area for mailbox store auditing, use the Exchange Management Console. The following figure shows the new **Manage Diagnostic Logging Properties** menu option.



To configure mailbox store auditing on a particular mailbox server:

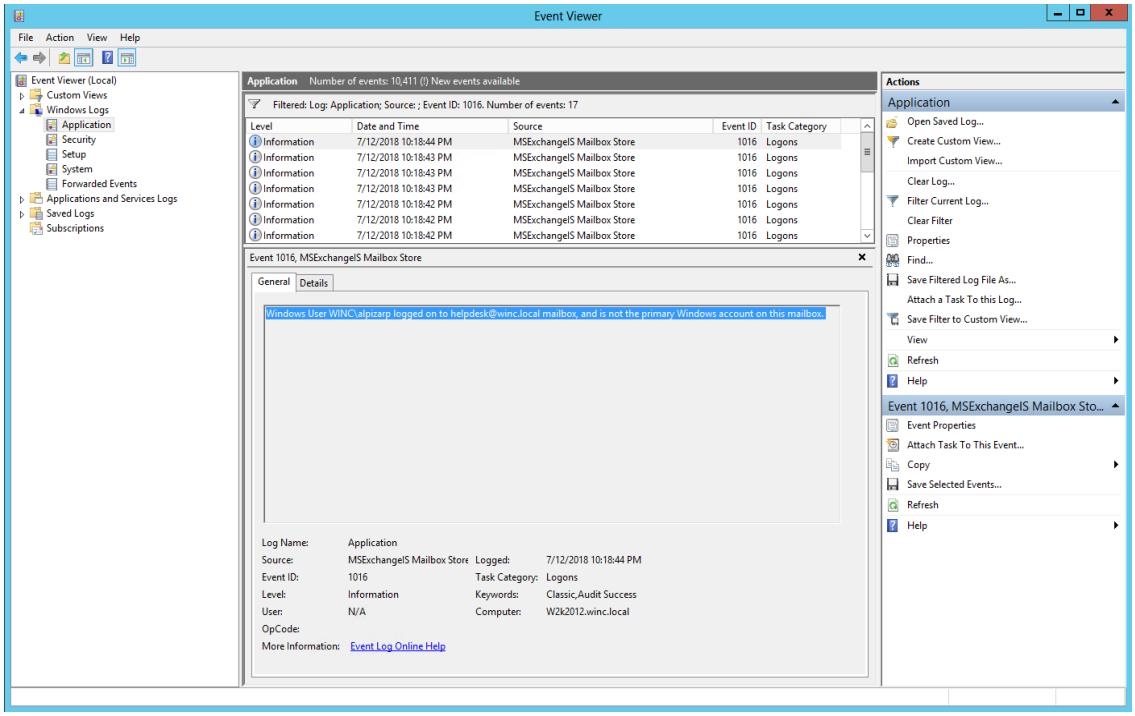
1. Select that server in the Exchange Management Console and then select the **Manage Diagnostics Logging Properties** menu option from the action pane; the **Manage Diagnostics Logging Properties** window is displayed.



2. In this window, expand the **MSExchangeIS** category and then expand the **9000 Private** category.
3. Under the **MSExchangeIS\9000 Private** category, configure MailBox Store for Event 1016 by selecting **Logons**.
4. When you have finished configuring the mailbox store levels, click **Configure**.
5. To view events, go to Windows Event Viewer, 1016 events are saved in Application Windows Events.

Accessing the Audited Information

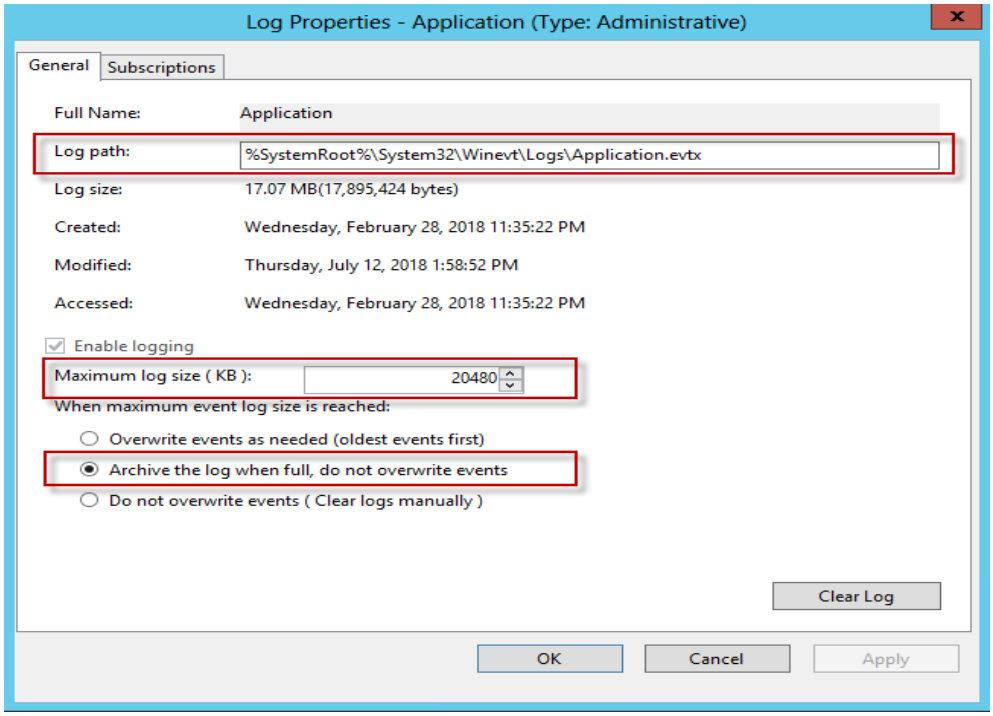
To view the information logged, navigate to **Event Viewer > Applications & Services Log > Exchange Auditing**.



Changing Default Log Storage location

By default, the logs are stored in the Exchange Server installation directory (`Drive\Program Files\Microsoft\Exchange Server\Logging\AuditLogs`). The logs are archived by default when the location gets full. Therefore, make sure that the location of the logs is changed to a drive that has enough free space.

To modify the log storage location, select the properties for the Exchange Auditing log and change the options.



Excluding Service Accounts

Service accounts that have full access to the mailboxes might fill up your mailbox access log with events. To exclude service accounts from being audited, run the following command:

```
Get-MailboxDatabase -identity "server\sg\dbname" | Add-ADPermission -User
"service account" -ExtendedRights ms-Exch-Store-Bypass-Access-Auditing -
InheritanceType All
```

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

General Exchange Events Mappings

ArcSight ESM Field	Device-Specific Field
Device Vendor	Microsoft
Device Product	Exchange Server

Exchange Events 1016 Mappings

ArcSight ESM Field	Device-Specific Field
Device Customer String3	%2 (Mail Box)
Source Nt Domain	%1
Source User Name	%1

Microsoft Forefront Protection 2010

Microsoft Forefront Protection 2010 for Exchange Server (FPE) provides protection against malware and spam by including multiple scanning engines in a single solution. FPE provides customers with an administration console that includes customizable configuration settings, filtering options, monitoring features and reports, anti-spam protection, and integration with the Forefront Online Protection for Exchange (FOPE) product.

This section provides information about configuring Microsoft Forefront Protection and its event mappings to ArcSight data fields. This connector supports Microsoft Forefront Protection 2010 events for Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 Standard with Exchange 2010.

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft Forefront Protection.

Configuring Forefront Protection

To enable writing events to the Windows Event Log from Forefront Protection:

1. In the Forefront Protection 2010 for Exchange Server Administrator Console, click **Policy Management**, and under **Global Settings**, click **Advanced Options**.
2. In the **Global Settings - Advanced Options** pane, under the **Logging Options** section, select the **Enable event logging** check box. When checked (the default), you can use the associated check boxes to individually enable or disable the following options (which are enabled by default):
   - **Incidents**—Enables or disables event logging for incidents.
   - **Engines**—Enables or disables event logging for engines.
   - **Operational**—Enables or disables logging for all other events, such as system information and health events.

   When the **Enable event logging** check box is cleared, incidents logging is suspended for incidents, engines, and operational events.
3. Click **Save**.

Note: The relevant Microsoft Exchange and Microsoft Forefront Server protection services must be restarted in order for any changes to these settings to take effect. This typically includes the Microsoft Exchange Transport, Microsoft Exchange Information Store, and Microsoft Forefront Server Protection Controller services.

For more information, see **Microsoft TechNet** > **Microsoft Forefront TechCenter Library** > **Forefront Protection 2010 for Exchange Server** > **Operations** > **Configuring logging options**.

Device Event Mapping to ArcSight Fields

The following sections lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Windows 2008

General

ArcSight ESM Field	Device-Specific Field
Device Product	'Forefront Protection'
Device Vendor	'Microsoft'

Event ID 7000

ArcSight ESM Field	Device-Specific Field
Message	'All the antimalware engines selected in the Forefront Administration Console for scanning have been enabled for updates.'
Name	‘All the antimalware engines selected in the Forefront Administration Console’

Event ID 7001

ArcSight ESM Field	Device-Specific Field
Message	'Not all the antimalware engines selected in the Forefront Administration Console for scanning have been enabled for updates.'
Name	‘Not all the antimalware engines selected in the Forefront Administration Console’

Event ID 7002

ArcSight ESM Field	Device-Specific Field
Name	'All the antimalware engines enabled for updates have been updated successfully at the last attempt'

Event ID 7003

ArcSight ESM Field	Device-Specific Field
Name	'Not all of the antimalware engines enabled for updates have successfully updated at the last attempt’

Event ID 7004

ArcSight ESM Field	Device-Specific Field
Name	'Less than half of the antimalware engines enabled for updates have updated successfully at the last attempt.'

Event ID 7005

ArcSight ESM Field	Device-Specific Field
Name	‘All the antimalware engines enabled for updates have updated successfully in the last five days’

Event ID 7006

ArcSight ESM Field	Device-Specific Field
Name	‘At least one of the antimalware engines enabled for updates has not been updated in the last five days.’

Event ID 7007

ArcSight ESM Field	Device-Specific Field
Name	'None of the antimalware engines enabled for updates have been updated in the last five days.'

Event ID 7008

ArcSight ESM Field	Device-Specific Field
Name	'The antimalware engines selected for transport scanning have been initialized.'

Event ID 7010

ArcSight ESM Field	Device-Specific Field
Name	The antimalware engines selected for realtime scanning have been initialized.'

Event ID 7012

ArcSight ESM Field	Device-Specific Field
Name	'The transport scan job is enabled’

Event ID 7015

ArcSight ESM Field	Device-Specific Field
Name	'The realtime scan job is enabled.'

Event ID 7018

ArcSight ESM Field	Device-Specific Field
Name	'The realtime scanning processes are running normally with no issues.'

Event ID 7021

ArcSight ESM Field	Device-Specific Field
Name	'The transport scanning processes are running normally with no issues.'

Event ID 7024

ArcSight ESM Field	Device-Specific Field
Name	'The MS Exchange Transport Service is running and the Forefront Agent is registered.'
Destination Service Name	‘MS Exchange Transport Service’

Event ID 7025

ArcSight ESM Field	Device-Specific Field
Name	‘The MS Exchange Transport Service is running but the Forefront Agent is not registered’
Destination Service Name	‘MS Exchange Transport Service’

Event ID 7026

ArcSight ESM Field	Device-Specific Field
Name	'The MS Information Store is running and the Forefront VSAPI Library is registered.'

Event ID 7028

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Product is within the license period.'

Event ID 7033

ArcSight ESM Field	Device-Specific Field
Name	‘The Forefront Protection Product is within the license period’

Event ID 7035

ArcSight ESM Field	Device-Specific Field
Name	'There is at least amount of disk space available.'

Event ID 7040

ArcSight ESM Field	Device-Specific Field
Name	'The Eventing Service (FSCEventing) is functioning.'
Destination Service Name	‘FSC Eventing’

Event ID 7044

ArcSight ESM Field	Device-Specific Field
Name	'The Mail Pickup Service (FSEMailPickup) is functioning.'
Destination Service Name	‘FSEMailPickup’

Event ID 7046

ArcSight ESM Field	Device-Specific Field
Name	‘Content Filter is enabled and definitions have been updated in the last one hour’

Event ID 7048

ArcSight ESM Field	Device-Specific Field
Name	'Content Filter is enabled and the last definition update was over 12 hours ago.'

Event ID 7051

ArcSight ESM Field	Device-Specific Field
Name	'The Monitor Service (FSCMonitor) is functioning.'
Destination Service Name	‘FSCMonitor’

Event ID 7064

ArcSight ESM Field	Device-Specific Field
Name	‘No archived undeliverable items exist’

FSC Controller

Event ID 1000

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service is running.'
Destination Service Name	‘Forefront Protection’

Event ID 1001

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service has stopped.'
Destination Service Name	‘Forefront Protection’

Event ID 1020

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service is starting.'
Destination Service Name	‘Forefront Protection’

Event ID 1021

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service is stopping.'
Destination Service Name	‘Forefront Protection’

Event ID 1022

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Version'
Device Version	%1 (version)
Additional data	%2 (Virus Protection Feature)

Event ID 1023

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Service Pack'
Additional data	%1 (ServicePack)
Message	Both (‘Forefront Protection Service Pack:’,%1)

Event ID 1024

ArcSight ESM Field	Device-Specific Field
Name	'Product ID'
Additional data	%1 (ProductID)
Message	Both (‘Product ID:’, %1)

Event ID 1025

ArcSight ESM Field	Device-Specific Field
Name	'Licensed Components'
Message	All of (Licensed Components: Component, License Type, Expiration Date)

Event ID 1026

ArcSight ESM Field	Device-Specific Field
Name	'Licensed Engines'
Additional data	%1 (LicensedEngines)
Message	Both (‘Licensed Engines:’, %1)

Event ID 1028

ArcSight ESM Field	Device-Specific Field
Name	'System Information'
Additional data	%1 (System Information)
Message	Both (‘System Information:’, %1)

Event ID 1037

ArcSight ESM Field	Device-Specific Field
Name	'Event Tracing session has been started.'
Device Severity	'Information'

Event ID 1041

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan has been started'

Event ID 1043

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan has stopped'

Event ID 1044

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan has completed'

Event ID 2102

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection application is still within the license period'

Event ID 5167

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection Monitor detected abnormal process shutdown'
Source Process Name	%1 (process name)
Message	Both ('Microsoft Forefront Protection Monitor detected abnormal' %1,' shutdown')

Event ID 5183

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan exceeded the allowed scan time limit'

Event ID 8046

ArcSight ESM Field	Device-Specific Field
Name	‘AD Mark Created’

Event ID 8055

ArcSight ESM Field	Device-Specific Field
Name	‘Ad Mark Removed’
Message	‘Failed to Delete Reg Key’

FSC Eventing

Event ID 1075

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Eventing Service has started.'
Destination Service Name	‘Forefront Protection Eventing’

Event ID 1076

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Eventing Service has stopped.'
Destination Service Name	‘Forefront Protection Eventing’

FSC Manual Scanner

Event ID 1045

ArcSight ESM Field	Device-Specific Field
Name	'On-Demand Scan started.'
Request Client Operation	%1 (Request Client Operation)

Event ID 1048

ArcSight ESM Field	Device-Specific Field
Name	'On-Demand Scan stopped.'
Request Client Operation	%1 (Request Client Operation)

Event ID 1052

ArcSight ESM Field	Device-Specific Field
Name	'On-Demand Scan has been completed.'
Request Client Operation	%1 (Request Client Operation)

FSC Scheduled Scanner

Event ID 2080

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan enabled.'

Event ID 2081

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan disabled.'

Event ID 3009

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan found virus.'
Device Custom String 4	mailbox name
Message	%2 (Message)
Device Custom String 1	virus name
Device Custom String 6	incident
Additional data	%4 (scan engine)
Device Action	%5 (Device Action)
File Name	%3 (File Name)

FSC Realtime Scanner

Event ID 2000

ArcSight ESM Field	Device-Specific Field
Name	'Realtime scan enabled.'

Event ID 2001

ArcSight ESM Field	Device-Specific Field
Name	'Realtime scan disabled.'

FSC Transport Scanner

Event ID 2007

ArcSight ESM Field	Device-Specific Field
Name	'Transport scan enabled.'

Event ID 2008

ArcSight ESM Field	Device-Specific Field
Name	'Transport scan disabled.'

Event ID 3002

ArcSight ESM Field	Device-Specific Field
Name	'Internet scan found virus'
File Path	%1 (folder)
Message	%2 (Message)
File Name	%4 (file name)
Device Custom String 6	Incident
Device Action	%6 (Device Action or State)
Device Custom String 1	virus name
Additional data	%3 (message ID)
Additional data	%5 (scan engine)

FSC Monitor

Event ID 1007

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor detected Information Store process started.'
Destination Process Name	‘Information Store’

Event ID 1008

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor detected Information Store shutdown.'
Destination Process Name	‘Information Store’

Event ID 1013

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor is active.'

Event ID 1014

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor is inactive.'

FSE On Demand Nav

Event ID 1049

ArcSight ESM Field	Device-Specific Field
Name	'The FseOnDemandNav service is running.'
Destination Process Name	‘FseOnDemandNav’

Event ID 1050

ArcSight ESM Field	Device-Specific Field
Name	'The FseOnDemandNav service has stopped.'
Destination Process Name	‘FseOnDemandNav’

FSE Mail Pickup

Event ID 1029

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Mail Pickup service is running.'
Destination Service Name	‘Forefront Protection Mail Pickup’

Event ID 1030

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Mail Pickup service has stopped.'
Destination Service Name	‘Forefront Protection Mail Pickup’

FSE IMC

Event ID 1002

ArcSight ESM Field	Device-Specific Field
Name	'FSEIMC service started.'
Destination Service Name	‘FSEIMC’

Event ID 1003

ArcSight ESM Field	Device-Specific Field
Name	'FSEIMC sertice stopped.'
Destination Service Name	‘FSEIMC’

FSE VS API

Event ID 5066

ArcSight ESM Field	Device-Specific Field
Name	‘Realtime scan exceeded the allowed scan time limit’

FSC VSS Writer

Event ID 1094

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection VSS Writer Service has started.'
Destination Service Name	‘Forefront Protection VSS Writer Service’

Event ID 1095

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection VSS Writer Service has stopped.'
Destination Service Name	‘Forefront Protection VSS Writer Service’

Get Engine Files

Event ID 2011

ArcSight ESM Field	Device-Specific Field
Name	‘Microsoft Forefront Protection did not detect any new scan engine updates’
Additional data	%1 (scan engine)
Request URL	%2 (request URL)

Event ID 2012

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection performed a successful scan engine update’
Additional data	%1 (scan engine)
Request URL	%2 (request URL)

Event ID 2017

ArcSight ESM Field	Device-Specific Field
Name	‘Forefront Protection has rolled back a scan engine’
Additional data	%1 (scan engine)

Event ID 2034

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection is attempting a scan engine update.'
Request URL	%2 (request url)
Additional data	%1 (scan engine)

Event ID 2109

ArcSight ESM Field	Device-Specific Field
Name	‘The VBuster scan engine is no longer supported’
Message	‘Updates are no longer available for this engine, and therefore the update check for this engine has been disabled. Please review the scan engine chosen for your scan jobs and make another selection to ensure up-to-date protection’
Additional data	%1 (scan engine)
Request URL	%2 (request URL)

Event ID 6012

ArcSight ESM Field	Device-Specific Field
Name	‘Microsoft Forefront Protection encountered an error while performing a scan engine update’
Additional data	%1 (scan engine)
Reason	%2 (Error Code)
Message	%3 (Error Detail)

Event ID 6014

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update.'
Additional data	%1 (scan engine)
Request URL	%2 (request url)
Additional data	%3 (proxy settings)
Reason	%4 (Error Code)
Message	%5 (Error Detail)

Event ID 6019

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update'
Additional data	%1 (scan engine)
Message	%2 (Error Detail)

Event ID 6020

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update'
Additional data	%1 (scan engine)
Request URL	%2 (request URL)
Message	%3 (Message)

Microsoft Netlogon

Netlogon is a Windows Server process in Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2008. The process is responsible for communication between systems in response to a logon request. This handles authentication of users and other services within a domain.

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Netlogon Logs and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides main mappings for the Windows Event Log SmartConnectors. The field mappings listed in this document are specifically for Microsoft Remote Access.

Configuring Microsoft Netlogon Logs

For information about Microsoft's netlogon events logs configuration, see https://support.microsoft.com/en-in/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc in the Microsoft TechNet Library.

Mappings for Microsoft Netlogon

General

ArcSight Field	Vendor Field
Device Product	''NETLOGON''
Device Vendor	'Microsoft'

Event 5827

ArcSight Field	Vendor Field
Device Custom String 1	%3 (Account Type)
Device Custom String 1 Label	"Account Type"
Device Custom String 4	%4 (Machine Operating System)
Device Custom String 4 Label	"Machine Operating System"
Device Custom String 5	%5 (Machine Operating System Build)
Device Custom String 5 Label	"Machine Operating System Build"
Device Custom String 6	%6 (Machine Operating System Service Pack)
Device Custom String 6 Label	"Machine Operating System Service Pack"
Event Outcome	"Denied"
Source Host Name	%1 (Machine SamAccountName)
Source Nt Domain	%2 (Domain)
Name	"Netlogon service denied vulnerable Netlogon secure channel connection from a machine account"

Event 5828

ArcSight Field	Vendor Field
Destination Nt Domain	%3 (Trust Target)
Device Custom String 1	%1 (Account Type)
Device Custom String 1 Label	"Account Type"
Event Outcome	"Denied"
Source Address	%4 (Client IP Address)
Source Nt Domain	%2 (Trust Name)
Name	"Netlogon service denied a vulnerable Netlogon secure channel connection using a trust account"

Event 5829

ArcSight Field	Vendor Field
Device Custom String 1	%3
Device Custom String 1 Label	"Account Type"

ArcSight Field	Vendor Field
Device Custom String 4	%4
Device Custom String 4 Label	"Machine Operating System"
Device Custom String 5	%5
Device Custom String 5 Label	"Machine Operating System Build"
Device Custom String 6	%6
Device Custom String 6 Label	"Machine Operating System Service Pack"
Event Outcome	"Allowed"
Source Host Name	%1
Source Nt Domain	%2
Name	"Netlogon service allowed a vulnerable Netlogon secure channel connection"

Event 5830

Device Custom String 1	%3
Device Custom String 1 Label	"Account Type"
Device Custom String 4	%4
Device Custom String 4 Label	"Machine Operating System"
Device Custom String 5	%5
Device Custom String 5 Label	"Machine Operating System Build"
Device Custom String 6	%6
Device Custom String 6 Label	"Machine Operating System Service Pack"
Event Outcome	"Allowed"
Source Host Name	%1
Source Nt Domain	%2
Name	"Netlogon service allowed a vulnerable Netlogon secure channel connection because account is allowed in group policy"

Event 5831

ArcSight Field	Vendor Field
Destination Nt Domain	%3
Device Custom String 1	%1

ArcSight Field	Vendor Field
Device Custom String 1 Label	"Account Type"
Event Outcome	"Allowed"
Source Address	%4
Source Nt Domain	%2
Name	"Netlogon service allowed a vulnerable Netlogon secure channel connection because trust account is allowed in group policy"

Microsoft Network Policy Server

Internet Authentication Service (IAS) was renamed Network Policy Server (NPS) starting with Windows Server 2008. The content of this guide applies to both IAS and NPS. Throughout the text, NPS is used to refer to all versions of the service, including the versions originally referred to as IAS.

Windows Server 2008 and Windows Server 2016 are supported.

Following sections provide information about configuring Microsoft Network Policy Server (NPS) and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft Network Policy Server.

Configuring NPS Logging

NPS logging is also called RADIUS accounting, and should be configured to your requirements whether NPS is used as a RADIUS server, proxy, NAP policy server, or any combination of the three configurations.

To configure NPS logging, you must configure the events logged and viewed with Event Viewer and determine other information you want to log. In addition, you must decide whether you want to log user authentication and accounting information to text log files stored on the local computer or to a SQL Server database on either the local computer or a remote computer.

Using the event logs in Event Viewer, you can monitor Network Policy Server (NPS) errors and other events that you configure NPS to record.

NPS records connection request failure events in the System and Security event logs by default. Connection request failure events consist of requests that are rejected or discarded by NPS. Other NPS authentication events are recorded in the Event Viewer system log on the basis of

the settings that you specify in the NPS snap-in. Some events that might contain sensitive data are recorded in the Event Viewer security log.

Use this procedure to configure Network Policy Server (NPS) to record connection request failure and success events in the Event Viewer system log.

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

To configure NPS event logging using the Windows interface:

1. Open the Network Policy Server (NPS) snap-in.
2. Right-click NPS (Local), and then click Properties.
3. On the General tab, select each required option, and then click OK.

Mappings for Network Policy Server

Mappings for Windows 2016, 2012, and 8

General

ArcSight ESM Field	Device-Specific Field
Device Vendor	'Microsoft'
Device Product	'NPS'

Event 13

ArcSight ESM Field	Device-Specific Field
Name	'A RADIUS message was received'
Message	Both ('A RADIUS message was received from the invalid RADIUS client IP address',%1)
Source Address	%1 (client IP address)

Event 25

ArcSight ESM Field	Device-Specific Field
Name	'The address of remote RADIUS server in remote RADIUS server group resolves to local address will be ignored'
Message	Both ('The address of remote RADIUS server ',%1,' in remote RADIUS server group ',%2,' resolves to local address ',%3,'. The address will be ignored.')

ArcSight ESM Field	Device-Specific Field
Source Address	%3 (address)
Additional data	%2 (ServerGroup)
Destination Address	%1 (address)

Event 4400

ArcSight ESM Field	Device-Specific Field
Name	'A LDAP connection with domain controller for domain is established’
Message	Both (‘A LDAP connection with domain controller ‘,%1,’ for domain ‘,%2,’ is established’)
Destination Host Name	%1 (host name)
Destination NT Domain	%2 (domain name)

Event 4402

ArcSight ESM Field	Device-Specific Field
Name	'No Domain controller available for domain'
Message	Both (‘There is no domain controller available for domain ‘,%1)
Destination NT Domain	%1 (domain name)

Event 4405

ArcSight ESM Field	Device-Specific Field
Name	'NPS cannot log accounting information in the primary data store'
Message	Both (‘NPS cannot log accounting information in the primary data store (‘,%1,’). Due to this logging failure, NPS will discard all connection requests. Error information: ‘,%2)’
Destination NT Domain	%1 (domain name)
Reason	%2 (reason code)

Mappings for Windows 2008 R2

General

ArcSight ESM Field	Device-Specific Field
Device Vendor	‘Microsoft’
Device Product	‘NPS’

Event 13

ArcSight ESM Field	Device-Specific Field
Name	‘A RADIUS message was received’
Source Address	%1 (client IP address)
Message	Both (‘A RADIUS message was received from the invalid RADIUS client IP address ‘,’%1)

Event 4400

ArcSight ESM Field	Device-Specific Field
Name	'A LDAP connection with domain controller for domain is established’
Destination Host Name	%1 (host name)
Destination NT Domain	%2 (domain name)
Message	Both (A LDAP connection with domain controller ‘,%1,’ for domain ‘,%2,’ is established)

Event 4402

ArcSight ESM Field	Device-Specific Field
Name	'No Domain controller available for domain'
Message	Both (‘There is no domain controller available for domain’ ‘,%1)
Destination NT Domain	%1 (domain name)

Event 4405

ArcSight ESM Field	Device-Specific Field
Name	'NPS cannot log accounting information in the primary data store'
Destination Host Name	%1 (host name)

ArcSight ESM Field	Device-Specific Field
Reason	%2 (reason code)
Message	Both (‘NPS cannot log accounting information in the primary data store (‘,%1,’). Due to this logging failure, NPS will discard all connection requests. Error information: ‘,%2’)

Microsoft Service Control Manager

Service Control Manager (SCM) is a special system process under Windows NT family of operating systems that starts, stops, and interacts with Windows service processes. It is located in %SystemRoot%\System32\services.exe executable. Service processes interact with SCM through a well-defined API, and the same API interface is used internally by the interactive Windows service management tools such as the MMC snap-in Services.msc and the command-line Service Control utility sc.exe.

The following sections provide information about configuring Service Control Manager and its event mappings to ArcSight data fields.

Supported versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft Service Control Manager.

Mappings for Windows 2016, 2012, 8, and 10

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'
Device Custom String 4	Reason or Error Code

7000

ArcSight Field	Vendor Field
Name	'Service failed to start'
Message	'The 'param1' service failed to start due to error: 'param2''

ArcSight Field	Vendor Field
Destination Service Name	param1
Device Custom String 4	param2 (Reason or Error Code)
Reason	param2

7001

ArcSight Field	Vendor Field
Name	'A service depends on other service which failed to start'
Message	'The 'param1' service depends on the 'param2' service which failed to start because of error: 'param3''
Destination Service Name	param1
Source Service Name	param2
Device Custom String 4	param3 (Reason or Error Code)
Reason	param3

7002

ArcSight Field	Vendor Field
Name	'The 'param1' service depends on the 'param2' group and no member of this group started'
Destination Service Name	param1

7003

ArcSight Field	Vendor Field
Name	'A service depends on a nonexistent service'
Message	'The 'param1' service depends on a nonexistent service 'param2''
Destination Service Name	param1
Source Service Name	param2

7005

ArcSight Field	Vendor Field
Name	'The 'param1' call failed with error 'param2'
Device Custom String 4	Param2 (Reason or Error Code)

7006

ArcSight Field	Vendor Field
Name	'The 'param1' call failed for 'param2' with the following error 'param3''
Device Action	param2 (action)
Device Custom String 4	Param3 (Reason or Error Code)

7007

ArcSight Field	Vendor Field
Name	'The system reverted to its last known good configuration'
Message	'The system is restarting'

7008

ArcSight Field	Vendor Field
Name	'No backslash is in the account name'

7009

ArcSight Field	Vendor Field
Name	'Timeout waiting for the service to connect'
Message	'Timeout 'param1' waiting for the 'param2' service to connect'
Destination Service Name	param2

7010

ArcSight Field	Vendor Field
Name	'Timeout waiting for ReadFile'

7011

ArcSight Field	Vendor Field
Name	'Timeout waiting for a transaction response from the 'param2' service'
Destination Service Name	param2

7012

ArcSight Field	Vendor Field
Name	'Message returned in transaction has incorrect size'

7015

ArcSight Field	Vendor Field
Name	'Boot-start or system-start driver 'param1' must not depend on a service'

7016

ArcSight Field	Vendor Field
Name	'The 'param1' service has reported an invalid current state'
Destination Service Name	param1

7017

ArcSight Field	Vendor Field
Name	'Detected circular dependencies demand starting 'param1''
Destination Service Name	param1

7018

ArcSight Field	Vendor Field
Name	'Detected circular dependencies auto-starting services'

7019

ArcSight Field	Vendor Field
Name	'Circular dependency: The 'param1' service depends on a service in a group which starts later.'
Destination Service Name	param1

7020

ArcSight Field	Vendor Field
Name	'Circular dependency: The 'param1' service depends on a group which starts later'
Destination Service Name	param1

7021

ArcSight Field	Vendor Field
Name	'About to revert to the last known good configuration because the 'param1' service failed to start'
Destination Service Name	param1

7022

ArcSight Field	Vendor Field
Name	'The 'param1' service hung on starting'
Destination Service Name	param1

7023

ArcSight Field	Vendor Field
Name	'A service terminated with error.'
Message	The 'param1' service terminated with the following error 'param2''
Destination Service Name	param1
Reason	param2
Device Custom String 4	param2 (Reason or Error Code)

7024

ArcSight Field	Vendor Field
Name	'The 'param1' service terminated with the following service-specific error'
Destination Service Name	param1
Device Custom String 4	param2 (Reason or Error Code)

7025

ArcSight Field	Vendor Field
Name	'At least one service or driver failed during system startup'
Message	'Use Event Viewer to examine the event log for details'

7026

ArcSight Field	Vendor Field
Name	'The boot-start or system-start driver(s) did not load'
Message	'The following boot-start or system-start driver(s) did not load: 'param1''
Device Process Name	param1

7027

ArcSight Field	Vendor Field
Name	'Windows could not be started as configured'
Message	'A previous working configuration was used instead'

7028

ArcSight Field	Vendor Field
Name	'The 'param1' Registry key denied access to SYSTEM account programs'
Message	'The Service Control Manager took ownership of the Registry key'
File Name	param1

7030

ArcSight Field	Vendor Field
Name	'The 'param1' service is marked as an interactive service'
Destination Service Name	param1
Message	'The system is configured to not allow interactive services. This service may not function properly.'

7031

ArcSight Field	Vendor Field
Name	Both (‘The ‘,param1,’ service terminated unexpectedly’)
Destination Service Name	param1 (service name)
Message	Both (‘The ‘,param1,’ service terminated unexpectedly. It has done this ‘,param2,’ time(s). The following corrective action will be taken in ‘,param3,’ milliseconds: ‘,param5)
Device Action	param5 (action)

7032

ArcSight Field	Vendor Field
Name	‘The Service Control Manager tried to take a corrective action ‘param1’ after the unexpected termination of the ‘param2’ service’
Device Action	param1
Message	‘This action failed with error’
Destination Service Name	param2
Device Custom String 4	param3 (Reason or Error Code)

7033

ArcSight Field	Vendor Field
Name	‘The Service Control Manager did not initialize successfully’
Message	‘The security configuration server (scesrv.dll) failed to initialize with error ‘param1’. The system is restarting.’
Device Custom String 4	param1 (Reason or Error Code)

7034

ArcSight Field	Vendor Field
Name	‘A service terminated unexpectedly’
Message	‘It has done this ‘param2’ times’
Destination Service Name	param1
Device Custom Number 3	param2 (Count)

7035

ArcSight Field	Vendor Field
Name	'The 'param1' service was successfully sent a 'param2' control'
Destination Service Name	param2

7036

ArcSight Field	Vendor Field
Name	'Service entered the 'param2" state'
Message	The 'param1' service entered the 'param2' state.'
Destination Service Name	param1
Device Action	param2

7037

ArcSight Field	Vendor Field
Name	'The Service Control Manager encountered an error undoing a configuration change to the 'param1' service'
Message	'The service's 'param2' is currently in an unpredictable state. If you do not correct this configuration, you may not be able to restart the 'param1' service or may encounter other errors. To ensure that the service is configured properly, use the Services snap-in in Microsoft Management Console (MMC)'
Destination Service Name	param1

7038

ArcSight Field	Vendor Field
Name	'A service was unable to log on with the currently configured password'
Message	'The 'param1' service was unable to log on as 'param2' with the currently configured password due to the following error: 'param3'. To ensure that the service is configured properly, use the Services snap-in in Microsoft Management Console (MMC)'
Destination Service Name	param1
Destination User Name	param2
Device Custom String 4	param3 (Reason or Error Code)
Reason	param3

7039

ArcSight Field	Vendor Field
Name	'A service process other than the one launched by the Service Control Manager connected when starting the 'param1' service'
Destination Service Name	param1
Message	'The Service Control Manager launched process 'param2' and process 'param3' connected instead. Note that if this service is configured to start under a debugger, this behavior is expected.'

7040

ArcSight Field	Vendor Field
Name	'Start type of 'param1' service was changed from 'param2' to 'param3''
Message	'Start type of 'param1' service was changed from 'param2' to 'param3''
Destination Service Name	param1
Device Action	param3

7041

ArcSight Field	Vendor Field
Name	'A service was unable to log on with the currently configured password.'
Destination Service Name	param1
Destination User Name	param2
Device Custom String 4	'Logon failure: the user has not been granted the requested logon type at this computer'
Message	'The 'param1' service was unable to log on as 'param2' with the currently configured password due to error. This service account does not have the necessary user right \'Log on as a service\''
Reason	'Logon failure: the user has not been granted the requested logon type at this computer'

7042

ArcSight Field	Vendor Field
Name	‘A service was successfully sent a control’
Destination Service Name	param1 (service name)
Device Custom String 4	Reason or Error Code
Message	‘The ‘param1’ service was successfully sent a ‘param2’ control. The reason specified was ‘param3’ [‘param4’’] Comment: ‘param5’’
Reason	Both (‘param3,’ ‘param4’)

7043

ArcSight Field	Vendor Field
Name	‘The ‘param1’ service did not shutdown properly after receiving a preshutdown control’
Destination Service Name	param1

7045

ArcSight Field	Vendor Field
Name	‘A service was installed in the system’
Destination Service Name	ServiceName
File Path	ImagePath
Device Custom String 5	StartType
Device Custom String 6	AccountName

Microsoft SQL Server Audit

With SQL Server 2008, Microsoft introduced an SQL Server Audit feature that provides a true auditing solution for enterprise customers. While SQL Trace can be used to satisfy many auditing needs, SQL Server Audit offers a number of advantages that can help DBAs more easily achieve their goals, such as meeting regulatory compliance requirements.

The SQL Server Audit feature is intended to replace SQL Trace as the preferred auditing solution. SQL Server Audit is meant to provide full auditing capabilities and only auditing capabilities, unlike SQL Trace, which is also used for performance debugging.

The following sections provide information about configuring Microsoft SQL Server Audit and its event mappings to ArcSight data fields.

Supported Versions

Microsoft Windows Server Version	Microsoft SQL Server Version
2008, 2008 R2	2008, 2012
2012	2012 SP1, 2014, 2016

SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft SQL Server Audit.

Configuring SQL Server Audit

For complete information about auditing in SQL Server, see Microsoft's SQL Server documentation at https://msdn.microsoft.com/en-us/library/cc280525(v=sql.120).aspx. This link takes you to the SQL Server 2014 version. You can select another version from the **Other Versions** drop down menu, but the basic steps are the same for sending audit events to an application log. From the left pane at this link, click **Create a Server Audit** and **Server Audit Specification** for detailed instructions.

Using SQL Server Management Studio, create a server audit as follows:

1. In Object Explorer, expand the **Security** folder.
2. Right-click the **Audits** folder and select **New Audit** to open a **Create Audit** window.
3. Enter a name for your audit (for example, **LoginFailed**). For **Audit destination**, select **ApplicationLog** from the list.
4. Click **OK** to accept the default settings and save the new audit specification.
5. The new audit will appear in the **Audits** folder. To enable the audit, select the audit you created, right-click, and select **Enable Audit**.

Customizing Event Source Mapping

For information about customizing event source mapping, see Customizing Event Source Mapping.

Microsoft SQL Server Audit Application Event Log Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'SQL Server'
Destination User Name	""

Event 615

ArcSight Field	Vendor Field
Name	'Could not find database'
Message	'Could not find database ID ',%1,', name ',%2,'

Event 849

ArcSight Field	Vendor Field
Name	'Using locked pages for buffer pool'
Message	'Using locked pages for buffer pool'

Event 852

ArcSight Field	Vendor Field
Name	'Using conventional memory in the memory manager'
Message	'Using conventional memory in the memory manager'

Event 919

ArcSight Field	Vendor Field
Name	'User is changing database script level'
Message	'User ',%1,' is changing database script level entry ',%2,' to a value of ',%3
Source User Name	%1
Device Custom Number 1	%2 (Level entry)
Device Custom Number 2	%3 (Changed value)

Event 958

ArcSight Field	Vendor Field
Name	'The resource database build version'
Message	'The resource database build version is ',%1
Device Custom String 4	%1 (Database build version)

Event 1486

ArcSight Field	Vendor Field
Name	'Database Mirroring Transport is disabled in the endpoint configuration'
Message	'Database Mirroring Transport is disabled in the endpoint configuration'

Event 1814

ArcSight Field	Vendor Field
Name	'Could not create tempdb'
Message	'Could not create tempdb. You may not have enough disk space available.'

Event 1945

ArcSight Field	Vendor Field
Name	‘Warning! The maximum key length’
Message	One of ('Warning! The maximum key length for a ",%1," index is ",%2," bytes. The index ",%3," has maximum length of ",%4," bytes. For some combination of large values, the insert/update operation will fail."), ('Warning! The maximum key length is ",%1," bytes. The index '",%2,"' has maximum length of ",%3," bytes. For some combination of large values, the insert/update operation will fail.')
Device Custom String 1	Both (One of (%2, %1), 'bytes') (Maximum key length)
Device Custom String 2	One of (%3,%2) (Index)
Device Custom String 3	Both (One of (%4, %3), 'bytes') (Maximum index)
Device Custom String 4	%1 (Index Type)

Event 2007

ArcSight Field	Vendor Field
Name	‘The module depends on the missing object’
Message	‘The module ‘,%1,’ depends on the missing object ‘,%2,’. The module will still be created; however, it cannot run successfully until the object exists.’
Device Custom String 1	%1 (Module)
Device Custom String 2	%2 (Missing object)

Event 2812

ArcSight Field	Vendor Field
Name	‘Could not find stored procedure’
Message	‘Could not find stored procedure ‘,%1
Device Custom String 2	%1 (Stored procedure)

Event 3406

ArcSight Field	Vendor Field
Name	‘Transactions rolled forward in database’
Message	%1’ transactions rolled forward in database ‘,%2, ‘(‘,%3,’)’

ArcSight Field	Vendor Field
Device Custom Number 2	%1 (Transactions quantity)
Device Custom String 1	%2 (Database name)
Device Custom Number 1	%3 (Database ID)

Event 3407

ArcSight Field	Vendor Field
Name	'Transactions rolled back in database'
Message	%1,' transactions rolled back in database ',%2,' (',%3,') '
Device Custom Number 2	%1 (Transactions quantity)
Device Custom String 1	%2 (Database name)
Device Custom Number 1	%3 (Database ID)

Event 3408

ArcSight Field	Vendor Field
Name	'Recovery is complete'
Message	'Recovery is complete. This is an informational message only. No user action is required.'

Event 3421

ArcSight Field	Vendor Field
Name	'Recovery completed for database'
Message	'Recovery completed for database ',%1,' (database ID ',%2',) in ',%3,' second(s) (analysis ',%4,' ms, redo ',%5,' ms, undo ',%6,' ms.)'
Device Custom String 1	%1 (Database name)
Device Custom String 2	%4 ms (Analysis time)
Device Custom String 3	%5 ms (Redo time)
Device Custom String 4	%6 ms (Undo time)
Device Custom String 5	%3 s (Completed recovery time)
Device Custom String 6	%2 (Database ID)

Event 3454

ArcSight Field	Vendor Field
Name	'Recovery is writing a checkpoint in database.'
Message	'Recovery is writing a checkpoint in database ',%1,' (',%2,') '
Device Custom String 1	%1 (Database name)
Device Custom Number 1	%2 (Database ID)

Event 5084

ArcSight Field	Vendor Field
Name	'Setting database option'
Message	'Setting database option ',%1,' to ',%2,' for database ',%3,' '
Device Custom String 1	%3 (Database name)
Device Custom String 2	%1 (Old option)
Device Custom String 3	%2 (New option)

Event 5579

ArcSight Field	Vendor Field
Name	'File system access'
Message	'#FILESTREAM: effective level =',%1,', configured level = ',%2,', file system access share name = ',%3,' '

Event 5701

ArcSight Field	Vendor Field
Name	'Changed database context'
Message	'Changed database context to ',%1
Device Custom String 1	%1 (Database name)
Device Action	'Changed'

Event 5703

ArcSight Field	Vendor Field
Name	'Changed language setting'
Message	'Changed language setting to ',%1
Device Custom String 1	%1 (Language setting)
Device Action	'Changed'

Event 6253

ArcSight Field	Vendor Field
Name	'Common language runtime (CLR) functionality initialized using CLR'
Message	'Common language runtime (CLR) functionality initialized using CLR version ',%1,' from ',%2
File Path	%2
Device Custom String 4	%1 (File version)

Event 6527

ArcSight Field	Vendor Field
Name	'.NET Framework runtime has been stopped'
Message	'.NET Framework runtime has been stopped'

Event 8128

ArcSight Field	Vendor Field
Name	'Execute extended stored procedure.'
Message	'Using ',%1,' version ',%2,' to execute extended stored procedure ',%3,'. This is an informational message only; no user action is required.'
File Name	%1
Device Custom String 3	%2 (File version)
Device Custom String 4	%3 (Extended stored procedure)

Event 9013

ArcSight Field	Vendor Field
Name	'Tail of the log for database is being rewritten'
Message	'Tail of the log for database ',%1,' is being rewritten to match the new sector size of ',%2,' bytes. ',%3,' bytes at offset ',%4,' in file ',%5,' will be written'

Event 9666

ArcSight Field	Vendor Field
Name	'Service endpoint is in disabled or stopped state'
Message	'The ',%1,' endpoint is in disabled or stopped state'
Destination Service Name	%1

Event 9688

ArcSight Field	Vendor Field
Name	'Service Broker manager has started'
Message	'Service Broker manager has started'

Event 9689

ArcSight Field	Vendor Field
Name	'Service Broker manager has shut down'
Message	'Service Broker manager has shut down'

Event 10981

ArcSight Field	Vendor Field
Name	'Resource governor reconfiguration succeeded'
Message	'Resource governor reconfiguration succeeded'

Event 12288

ArcSight Field	Vendor Field
Name	'Package started'
File Name	%1

Event 12291

ArcSight Field	Vendor Field
Name	'Package failed
File Name	%1

Event 15268

ArcSight Field	Vendor Field
Name	'Authentication mode'
Message	'Authentication mode is ',%1
Device Custom String 3	%1 (Authentication mode)

Event 15457

ArcSight Field	Vendor Field
Name	'Configuration option changed'
Message	'Configuration option ',%1,' changed from ',%2,' to ',%3,'. Run the RECONFIGURE statement to install'
Device Custom String 3	%1 (Configuration option)
Device Custom Number 1	%2 (Old value)
Device Custom Number 2	%3 (New value)

Event 15477

ArcSight Field	Vendor Field
Name	'Caution: Changing any part of an object name could break scripts and stored procedures'
Message	'Caution: Changing any part of an object name could break scripts and stored procedures'

Event 17069

ArcSight Field	Vendor Field
Name	'Microsoft SQL Server 2012 (SP1)'
Message	%1

Event 17101

ArcSight Field	Vendor Field
Name	'Microsoft Corporation'
Message	'Microsoft Corporation'

Event 17103

ArcSight Field	Vendor Field
Name	'All rights reserved'
Message	'All rights reserved'

Event 17104

ArcSight Field	Vendor Field
Name	'Server process ID"
Message	'Server process ID is ',%1
Destination Process ID	%1

Event 17107

ArcSight Field	Vendor Field
Name	'Perfmon counters for resource governor pools and groups failed to initialize and are disabled'
Message	'Perfmon counters for resource governor pools and groups failed to initialize and are disabled'

Event 17108

ArcSight Field	Vendor Field
Name	'Password policy update was successful'
Message	'Password policy update was successful'
Device Action	'Update'

Event 17110

ArcSight Field	Vendor Field
Name	'Registry startup parameters'
Message	'Registry startup parameters ',%1
Device Custom String 1	%1 (Parameters)

Event 17111

ArcSight Field	Vendor Field
Name	'Logging SQL Server messages'
Message	'Logging SQL Server messages in file ',%1
File Name	%1

Event 17115

ArcSight Field	Vendor Field
Name	'Command Line Startup'
Message	'Command Line Startup Parameters: ',%1
Device Action	'Startup'
Device Custom String 1	%1 (Parameters)

Event 17125

ArcSight Field	Vendor Field
Name	'Using dynamic lock allocation'
Message	'Using dynamic lock allocation. Initial allocation of ',%1,' Lock blocks and ',%2,' Lock Owner blocks per node'

ArcSight Field	Vendor Field
Device Custom Number 1	%1 (Lock blocks)
Device Custom Number 2	%2 (Lock owner blocks)

Event 17126

ArcSight Field	Vendor Field
Name	'SQL Server is now ready for client connections'
Message	'SQL Server is now ready for client connections'

Event 17136

ArcSight Field	Vendor Field
Name	'Clearing tempdb database'
Message	'Clearing tempdb database'

Event 17137

ArcSight Field	Vendor Field
Name	'Starting up database'
Message	'Starting up database ',%1
Device Custom String 1	%1 (Database name)

Event 17147

ArcSight Field	Vendor Field
Name	'SQL Server is terminating because of a system shutdown'
Message	'SQL Server is terminating because of a system shutdown. This is an informational message only. No user action is required.'

Event 17148

ArcSight Field	Vendor Field
Name	'SQL Server is terminating'
Message	'SQL Server is terminating in response to a 'stop' request from Service Control Manager'

Event 17152

ArcSight Field	Vendor Field
Name	'Node configuration'
Message	'Node configuration: node ',%1,': CPU mask: ',%2,' : '%3,' Active CPU mask: ',%4,': ',%5,'. This message provides a description of the NUMA configuration for this computer. This is an informational message only. No user action is required.'
Device Custom String 2	%1 (Node)
Device Custom String 3	%2 (CPU mask)
Device Custom String 4	%4 (Active CPU mask)
Device Custom String 5	%3 (Flag CPU mask)
Device Custom String 6	%5 (Flag Active CPU mask)

Event 17162

ArcSight Field	Vendor Field
Name	'SQL Server is starting'
Message	'SQL Server is starting at normal priority base (=7)'

Event 17164

ArcSight Field	Vendor Field
Name	'SQL Server detected sockets'
Message	'SQL Server detected ',%1,' sockets with ',%2,' cores per socket and ',%3,' logical processors per socket, ',%4,' total logical processors; using ',%5,' logical processors based on SQL Server licensing. This is an informational message; no user action is required.'
Device Custom Number 1	%1 (Detected sockets)
Device Custom Number 2	%2 (Cores per socket)
Device Custom Number 3	%3 (Processors per socket)
Device Custom String 3	%4 (Total processors)
Device Custom String 4	%5 (Using processors)

Event 17176

ArcSight Field	Vendor Field
Name	'This instance of SQL Server last reported using a process ID'
Message	'This instance of SQL Server last reported using a process ID of ',%1,' at ',%2,' (local) ',%3,' (UTC). This is an informational message only; no user action is required.'
Destination Process ID	%1
Device Custom Date 1	%2, 'MM/dd/yyyy hh:mm:ss aa' (Last Report Time (local)
Device Custom Date 2	%3 'MM/dd/yyyy hh:mm:ss aa' (Last Report Time (UTC))

Event 17177

ArcSight Field	Vendor Field
Name	'This instance of SQL Server has been using a process ID"
Message	'This instance of SQL Server has been using a process ID of ',%1,' since ',%2,' (local) ',%3,' (UTC). '

Event 17199

ArcSight Field	Vendor Field
Name	'Restart SQL Server using the trace flag'
Message	'Dedicated administrator connection support was not started because it is disabled on this edition of SQL Server. If you want to use a dedicated administrator connection, restart SQL Server using the trace flag ',%1,'. This is an informational message only. No user action is required.'
Device Custom Number 1	%1 (Trace flag)

Event 17201

ArcSight Field	Vendor Field
Name	'Dedicated admin connection support was established'
Message	'Dedicated admin connection support was established for listening locally on port ',%1
Destination Port	%1

Event 17550

ArcSight Field	Vendor Field
Name	'DBCC TRACEON, server process'
Message	'DBCC TRACEON ',%1,' server process ID (SPID) ',%2,'. This is an informational message only; no user action is required."
Destination Process Name	'DBCC TRACEON' %1
Destination Process ID	%2

Event 17551

ArcSight Field	Vendor Field
Name	'DBCC TRACEOFF, server process'
Message	'DBCC TRACEOFF ',%1,', server process ID (SPID) ',%2,'. This is an informational message only; no user action is required.'
Destination Process Name	'DBCC TRACEON' ,%1
Destination Process ID	%2

Event 17561

ArcSight Field	Vendor Field
Name	'index restored'
Message	'index restored for ' ,%2, '.', %3
Device Custom String 1	%2 (Report server database)
Device Custom String 3	%3 (Object name)

Event 17656

ArcSight Field	Vendor Field
Name	'Warning'
Message	'Warning **********'

Event 17658

ArcSight Field	Vendor Field
Name	'SQL Server started in single-user mode'
Message	'SQL Server started in single-user mode. This is an informational message only. No user action is required.'

Event 17663

ArcSight Field	Vendor Field
Name	'Server name'
Message	'Server name is ',%1
Destination Host Name	%1

Event 17811

ArcSight Field	Vendor Field
Name	'The maximum number of dedicated administrator connections for this instance'
Message	'The maximum number of dedicated administrator connections for this instance is '",%1,"'."
Device Custom Number 1	%1 (Maximum administrator connections)

Event 18453

ArcSight Field	Vendor Field
Name	'Login succeeded'
Message	'Login succeeded for user. Connection made using Windows authentication'
Destination User Name	%1
Destination NT Domain	%1
Device Custom String 1	%2 (Windows authentication)

Event 18454

ArcSight Field	Vendor Field
Name	'Login succeeded'
Message	'Login succeeded for user. Connection made using SQL Server authentication'
Source User Name	%1
Source Address	%2
Device Custom IPv6 Address 2	%2 (Source IPv6 Address)

Event 18456

ArcSight Field	Vendor Field
Name	'Login failed for user'
Message	'Login failed for user ',%1,'. ',%2' ',%3
Device Custom String 3	%2 (Login failed)
Source User Name	%1
Source Address	%3

Event 18488

ArcSight Field	Vendor Field
Name	'Login failed for user'
Message	'Login failed for user ',%1,'. Reason: The password of the account must be changed. ',%2
Source User Name	%1
Source Address	%2

Event 18496

ArcSight Field	Vendor Field
Name	'System Manufacturer and System Model Information'
Message	'System Manufacturer: ',%1,' System Model: ',%2,' '
Device Custom String 1	%1 (System Manufacturer)
Device Custom String 2	%2 (System Model)

Event 19030

ArcSight Field	Vendor Field
Name	'SQL Trace was started'
Message	'SQL Trace ID ',%1,' was started by login ',%2,' '
Device Custom String 1	%1 (Trace ID)
Source User Name	%2

Event 19031

ArcSight Field	Vendor Field
Name	'SQL Trace stopped'
Message	'SQL Trace stopped. Trace ID = ',%1,'. Login Name = ',%2
Source User Name	%2

Event 19032

ArcSight Field	Vendor Field
Name	'SQL Trace was stopped due to server shutdown'
Message	'SQL Trace was stopped due to server shutdown. Trace ID = ',%1,'. This is an informational message only; no user action is required.'
Device Custom Number 1	%1 (Trace ID)

Event 26018

ArcSight Field	Vendor Field
Name	'A self-generated certificate was successfully loaded for encryption'
Message	'A self-generated certificate was successfully loaded for encryption'

Event 26022

ArcSight Field	Vendor Field
Name	'Server is listening'
Message	'Server is listening on [',%1,' <',%2,'> ',%3,']'

ArcSight Field	Vendor Field
Device Custom String 4	%1 (Listening Address)
Application Protocol	%2
Destination Port	%3

Event 26037

ArcSight Field	Vendor Field
Name	'SQL Server Network Interface library could not register the Server Principal Name'
Message	'Error: ',%1,', state: ',%2,'. Failure to register an SPN may cause integrated authentication to fall back to NTLM instead of Kerberos'

Event 26048

ArcSight Field	Vendor Field
Name	'Server local connection provider is ready to accept connection'
Message	'Server local connection provider is ready to accept connection on ['',%1,']'
File Path	%1

Event 26067

ArcSight Field	Vendor Field
Name	'SQL Server Network Interface library could not register the Service Principal Name (SPN)'
Message	'The SQL Server Network Interface library could not register the Service Principal Name (SPN) ',%1,' for the SQL Server service. Windows return code: ',%2,', state: ',%3,'. Failure to register a SPN might cause integrated authentication to use NTLM instead of Kerberos. This is an informational message. Further action is only required if Kerberos authentication is required by authentication policies and if the SPN has not been manually registered.'
Source Service Name	%1
Reason	%2
Device Custom String 1	%3 (State)

Event 26076

ArcSight Field	Vendor Field
Name	'SQL Server is attempting to register a Service Principal Name (SPN)'
Message	'SQL Server is attempting to register a Service Principal Name (SPN) for the SQL Server service. Kerberos authentication will not be possible until a SPN is registered for the SQL Server service. This is an informational message. No user action is required.'

Event 30090

ArcSight Field	Vendor Field
Name	'New instance of full-text filter daemon host process has been successfully started.'
Message	'A new instance of the full-text filter daemon host process has been successfully started.'

Event 33090

ArcSight Field	Vendor Field
Name	'Attempting to load library into memory'
Message	'Attempting to load library ',%1,' into memory. This is an informational message only. No user action is required'
File Name	%1

Event 33204

ArcSight Field	Vendor Field
Name	'SQL Server Audit could not write to the security log'
Message	'SQL Server Audit could not write to the security log'

Event 33205

ArcSight Field	Vendor Field
Source Service Name	EventSource
Device Event Class ID	All of (class_type, '|', action_id)
Device Action	action_id

ArcSight Field	Vendor Field
Event Outcome	succeeded
File ID	object_id
File Type	class_type
File Name	object_name
File Size	sequence_number
File Hash	audit_schema_version
Old File ID	transaction_id
Message	statement
Source User ID	server_principal_id
Source User Name	server_principal_name
Source NT Domain	server_principal_name
Destination User ID	One of (server_principal_id, target_server_principal_id)
Destination NT Domain	One of (target_server_principal_name, server_principal_name)
Destination Host Name	server_instance_name
Device Custom Number 1	session_id
Device Custom Number 2	database_principal_id
Device Custom Number 3	target_database_principal_id
Device Custom String 1	object_name
Device Custom String 2	statement
Device Custom String 3	database_name
Device Custom String 4	Device Custom String 4 = database_principal_name
Device Custom String 5	One of (target_database_principal_name, database_principal_name)
Device Custom String 6	schema_name
Old File Name	All of('Additional Information : ',additional_information)
Source Address	One of(additional_information, device address (In case the address is local machine))
Source Host Name	device host name (In case the address is local machine)
Destination User Name	One Of(target_server_principal_name,server_principal_name)
Device Custom IPv6 Address 2	additional_information

Event 33217

ArcSight Field	Vendor Field
Name	'SQL Server Audit is starting the audits'
Message	'SQL Server Audit is starting the audits. This is an informational message. No user action is required.'

Event 33218

ArcSight Field	Vendor Field
Name	'SQL Server Audit has started the audits'
Message	'SQL Server Audit has started the audits. This is an informational message. No user action is required.'

Event 49903

ArcSight Field	Vendor Field
Name	'Detected RAM'
Message	'Detected ',%1,' of RAM. This is an informational message; no user action is required.'
Device Custom Number 1	%1 (Detected RAM)

Event 49904

ArcSight Field	Vendor Field
Name	'Service account'
Message	'The service account is ',%1,'. This is an informational message; no user action is required.'
Source Service Name	%1

Event 49910

ArcSight Field	Vendor Field
Name	'Software Usage Metrics is disabled'
Message	'Software Usage Metrics is disabled'

Event 49916

ArcSight Field	Vendor Field
Name	'UTC adjustment'
Message	'UTC adjustment.'
Device Custom String 1	All of 1%, :, 2% (UTC Adjustment)

Event 49917

ArcSight Field	Vendor Field
Name	'Default collation'
Message	All of 'Default collation',%1,' (',%2,' ',%3,').'
Device Custom String 1	%2 (Language)
Device Custom String 4	%1 (SQL collation)
Device Custom Number 2	%3 (Language ID)

Microsoft Sysmon

Microsoft Sysmon Logs is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.

It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, users can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

The following sections provide information about Microsoft Sysmon Logs and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

This connector supports Microsoft Sysmon Operational version 11 events.

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Configuring Microsoft Sysmon Logs

For complete information about Microsoft's Reporting and Microsoft Sysmon Logs, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)": http://technet.microsoft.com/en-us/library/hh831416

Mappings for Microsoft Sysmon Logs

General

ArcSight Field	Vendor Field
Destination Process Id	ProcessId
Device Product	'Sysmon'
Device Vendor	‘Microsoft’
Device Version	'Unknown'

Event 1

ArcSight Field	Vendor Field
Destination Process Name	Image
Destination Service Name	CommandLine
Device Action	'Process Create'
Device Custom String 1	IntegrityLevel
Device Custom String 4	CommandLine
Device Custom String 6	LogonGuid
Device Receipt Time	UtcTime
File Hash	Hashes
File Id	ProcessGuid
Message	Description
Name	'Process Created'
Old File Hash	MITRE ID
Old File Id	ParentProcessGuid
Old File Name	OriginalFileName
Old File Path	CurrentDirectory
Source Nt Domain	__extractNTDomain(User)
Source Process Id	ParentProcessId
Source Process Name	ParentImage

ArcSight Field	Vendor Field
Source Service Name	ParentCommandLine
Source User Id	LogonId
Source User Name	__extractNTUser(User)

Event 2

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'File creation time changed'
Device Receipt Time	UtcTime
File Create Time	CreationUtcTime
File Id	ProcessGuid
File Path	TargetFilename
Message	'File creation time changed'
Name	'File creation time changed'
Old File Create Time	PreviousCreationUtcTime
Old File Hash	MITRE ID

Event 3

ArcSight Field	Vendor Field
Destination Address	__oneOfAddress(DestinationIp) (for destination aware)
Device Custom IPv6 Address 2	__stringToIPv6Address(SourceIp) (for non-destination aware)
Device Custom IPv6 Address 3	__stringToIPv6Address(DestinationIp) (for non-destination aware)
Destination Host Name	DestinationHostname
Destination Port	__safeToInteger(DestinationPort)
Destination Process Name	Image
Device Action	__concatenate("Initiated :",Initiated)
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Network connection detected'
Name	'Network connection detected'

ArcSight Field	Vendor Field
Old File Hash	MITRE ID
Source Address	__oneOfAddress(SourceIp) (for destination aware)
Source Host Name	SourceHostname
Source Nt Domain	__extractNTDomain(User)
Source Port	__safeToInteger(SourcePort)
Source Port Name	SourcePortName
Source User Name	__extractNTUser(User)
Transport Protocol	Protocol

Event 4

ArcSight Field	Vendor Field
Additional Data.Schema Version	SchemaVersion
Device Action	State
Device Receipt Time	UtcTime
Message	'Sysmon service state changed'
Name	'Sysmon service state changed'

Event 5

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Process Terminated'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Process Terminated'
Name	'Process Terminated'
Old File Hash	MITRE ID

Event 6

ArcSight Field	Vendor Field
Device Action	'Driver Loaded'
Device Receipt Time	UtcTime
File Hash	Hashes
File Name	ImageLoaded
File Permission	SignatureStatus
File Type	Signed
Message	'Driver Loaded'
Name	'Driver Loaded'
Old File Hash	MITRE ID

Event 7

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Image Loaded'
Device Receipt Time	UtcTime
File Hash	Hashes
File Id	ProcessGuid
File Name	ImageLoaded
File Permission	SignatureStatus
File Type	Signed
Message	Description
Name	'Image Loaded'
Old File Hash	MITRE ID
Old File Name	OriginalFileName

Event 8

ArcSight Field	Vendor Field
Destination Process Name	TargetImage
Device Action	'CreateRemoteThread detected'
Device Process Id	SourceProcessId
Device Receipt Time	UtcTime
File Id	TargetProcessGuid
Message	'CreateRemoteThread detected'
Name	'CreateRemoteThread detected'
Old File Hash	MITRE ID
Old File Id	SourceProcessGuid
Source Process Name	SourceImage

Event 9

ArcSight Field	Vendor Field
Device Action	'RawAccessRead detected'
Device Custom String 5	Device
Device Receipt Time	UtcTime
Destination Process Name	Image
File Id	ProcessGuid
Message	'RawAccessRead detected'
Name	'RawAccessRead detected'
Old File Hash	MITRE ID

Event 10

ArcSight Field	Vendor Field
Additional Data.Source Thread Id	SourceThreadId
Destination Process Name	TargetImage
Device Action	'Process accessed'
Device Custom String 1	GrantedAccess

ArcSight Field	Vendor Field
Device Process Id	__safeToInteger(SourceProcessId)
Device Receipt Time	UtcTime
File Id	TargetProcessGUID
Message	'Process accessed'
Name	'Process accessed'
Old File Id	SourceProcessGUID
Old File Hash	MITRE ID
Old File Path	CallTrace
Source Process Name	SourceImage

Event 11

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'File Created'
Device Receipt Time	UtcTime
File Create Time	CreationUtcTime
File Id	ProcessGuid
File Path	TargetFilename
Message	'File created'
Name	'File created'
Old File Hash	MITRE ID

Event 12

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Registry object added or deleted'
Device Custom String 1	EventType
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Path	TargetObject

ArcSight Field	Vendor Field
Message	'Registry object added or deleted'
Name	'Registry object added or deleted'
Old File Hash	MITRE ID

Event 13

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Registry value set'
Device Custom String 1	EventType
Device Custom String 4	Details
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Path	TargetObject
Message	'Registry value set'
Name	'Registry value set'
Old File Hash	MITRE ID

Event 14

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Registry key and value rename'
Device Custom String 1	EventType
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Path	NewName
Name	'Registry key and value rename'
Old File Hash	MITRE ID
Old File Path	TargetObject

Event 15

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'File stream created'
Device Receipt Time	UtcTime
File Hash	Hash
File Id	ProcessGuid
File Create Time	CreationUtcTime
File Path	TargetFilename
Message	'File stream created'
Name	'File stream created'
Old File Hash	MITRE ID

Event 16

ArcSight Field	Vendor Field
Device Action	'Sysmon config state changed'
Device Receipt Time	UtcTime
File Hash	ConfigurationFileHash
Message	'Sysmon config state changed'
Name	'Sysmon config state changed'
Source Process Name	Configuration

Event 17

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Pipe Created'
Device Custom String 1	EventType
Device Custom String 6	PipeName
Device Receipt Time	UtcTime
File Id	ProcessGuid

ArcSight Field	Vendor Field
Message	'Create Pipe'
Name	'Create Pipe'
Old File Hash	MITRE ID

Event 18

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Pipe Connected'
Device Custom String 1	EventType
Device Custom String 6	PipeName
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Pipe Connected'
Name	'Pipe Connected'
Old File Hash	MITRE ID

Event 19

ArcSight Field	Vendor Field
Device Action	Operation
Device Custom String 1	EventType
Device Custom String 4	Name
Device Receipt Time	UtcTime
Name	'WmiEventFilter activity detected'
Old File Hash	MITRE ID
Old File Path	EventNamespace
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)

Event 20

ArcSight Field	Vendor Field
Device Action	Operation
Device Custom String 1	EventType
Device Custom String 4	Name
Device Receipt Time	UtcTime
File Path	Destination
File Type	Type
Name	'WmiEventConsumer activity detected'
Old File Hash	MITRE ID
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)

Event 21

ArcSight Field	Vendor Field
Device Action	Operation
Device Custom String 1	EventType
Device Custom String 4	Filter
Device Custom String 5	Consumer
Device Receipt Time	UtcTime
Name	'WmiEventConsumerToFilter activity detected'
Old File Hash	MITRE ID
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)

Event 22

ArcSight Field	Vendor Field
Destination Address	__regexToken(QueryResults)
Destination Process Name	Image
Device Action	'Dns query'

ArcSight Field	Vendor Field
Device Custom String 1	QueryName
Device Custom String 4	QueryResults
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Dns query'
Name	'Dns query'
Old File Hash	MITRE ID

Event 23

ArcSight Field	Vendor Field
Device Custom String 1	IsExecutable
Device Custom String 4	Archived
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Hash	Hashes
File Path	TargetFilename
Message	__concatenate("File has been deleted from ",__extractNTDomain (TargetFilename))
Name	'File Delete'
Old File Hash	MITRE ID
Source Nt Domain	__extractNTDomain(User)
Source Process Name	Image
Source User Name	__extractNTUser(User)

Event 255

ArcSight Field	Vendor Field
Device Receipt Time	UtcTime
Device Action	__stringConstant("Level : Error")
Message	Description
Name	'Error report'
Source Process Name	ID

User 32 Service

Routing and Remote Access is a network service in Windows Server 2008 R2 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

The following sections provide information about User 32 Service and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows Server 2008 R2

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft User 32.

Configuring Remote Access

For complete information about Microsoft's Reporting and Remote Access Service, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)": http://technet.microsoft.com/en-us/library/hh831416

Mappings for Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 1074

ArcSight Field	Vendor Field
Name	The process has initiated the shutdown/restart of computer.
Message	concatenate(The process ",%1," has initiated the ",%5," of computer ",%2," on behalf of user ",%7," for the following reason: ",%3)
Source Process Name	%1
Destination Host Name	%2
Reason	%3
Device Custom String4	Reason Code
Device Custom String5	Shutdown Type
Device Custom String6	Comment

Microsoft Windows AppLocker

Microsoft Windows AppLocker is a network service in Windows 10, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 and Windows 2019 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

The following sections provide information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows AppLocker and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Configuring Microsoft Windows AppLocker

For complete information about Microsoft's Reporting and Microsoft Windows AppLocker, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":http://technet.microsoft.com/en-us/library/hh831416

Mappings for Microsoft Windows AppLocker

Event 8001

ArcSight Field	Vendor Field
Name	"The AppLocker policy was applied successfully to this computer."

Event 8002

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath or FilePath

Event 8003

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run but would have been prevented from running if the AppLocker policy were enforced."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath or FilePath

Event 8004

ArcSight Field	Vendor Field
Name	FilePath," was prevented from running."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath or FilePath

Event 8005

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath or FilePath

Event 8006

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run but would have been prevented from running if the AppLocker policy were enforced."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath or FilePath

Event 8007

ArcSight Field	Vendor Field
Name	FilePath," was prevented from running."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6:	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath or FilePath

Microsoft Windows ESENT

Microsoft Windows ESENT is an embeddable and transactional database engine which is used for data storage. You can use ESENT for applications that need reliable, high-performance, and low-overhead storage of structured or semi-structured data. The ESENT engine can help with data needs ranging from something as simple as a hash table that is too large to store in memory to something more complex such as an application with tables, columns, and indexes.

The following sections provide information about configuring Microsoft Windows ESENT Logs and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (*)

Mappings for Microsoft Windows ESENT Logs

General

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'ESENT'
Device Version	'Unknown'

Event Id 102

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine is starting a new instance

Event Id 103

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine stopped the instance

Event Id 105

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine started a new instance

Event Id 224

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4 to %5
Name	Deleting log files

Event Id 225

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	No log files can be truncated

Event Id 300

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine is initiating recovery steps

Event Id 301

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4
File Type	%6
Device Custom String 1	%7
Device Custom String 1 Label	Number of times log record seen
Name	The database engine has finished replaying log file

Event Id 302

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine has successfully completed recovery steps

Event Id 325

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine created a new database"

ArcSight Field	Vendor Field
Source Process Id	%2
Source Service Name	%1

Event Id 326

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine attached a database"
Source Process Id	%2
Source Service Name	%1
Source Process Name	%3

Event Id 327

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine detached a database"
Source Process Id	%2
Source Service Name	%1

Event Id 330

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4
Device Custom String 4	%7
Device Custom String 4 Label	Default engine version
Name	The database format version is being held back

Event Id 335

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%5
Reason	%7
Name	Replay of a create for database at log position was deferred

Event Id 455

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4
Device Custom String 4	%5
Device Custom String 4 Label	Error
Name	Error occurred while opening log file

Event Id 641

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Device Custom String 4	%5
Device Custom String 4 Label	Log format version
Device Custom String 5	%6
Device Custom String 5 Label	Current log format version
Name	The log format feature version could not be used

Microsoft Windows BITS Client Logs

Microsoft Windows Background Intelligent Transfer Service (BITS) helps programmers and system administrators to download files from or upload files to HTTP web servers and share files using Server Message Block (SMB) protocol. BITS will take the cost of the transfer into consideration, as well as the network usage so that the user's foreground work has as little impact as possible. It also handles network interruptions, pausing, and automatically resuming transfers, even after a reboot. BITS includes `PowerShell cmdlets` for creating and managing transfers as well as the BitsAdmin command-line utility.

The following sections provide information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows BITS Client Logs and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (*)

Mappings for Microsoft Windows BITS Client

General

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Microsoft Windows BITS Client'

Event ID 3

ArcSight Field	Vendor Field
Destination Nt Domain	string2
Destination User Name	string2
Device Custom String 4	string

ArcSight Field	Vendor Field
Device Custom String 4 Label	"Job Title"
Message	All of("The BITS service created a new job: ",string," , with owner ",string2)
Name	"The BITS service created a new job"

Event ID 4

ArcSight Field	Vendor Field
Device Custom Number 1	fileCount
Device Custom Number 1 Label	"File count"
Device Custom String 4	jobTitle
Device Custom String 4 Label	"Job Title"
Device Custom String 5	jobId
Device Custom String 5 Label	"Job ID"
Device Custom String 6	jobOwner
Device Custom String 6 Label	"Job Owner"
Message	All of("The transfer job is complete.User: ",User,", Transfer job: ",jobTitle,", Job ID: ",jobId,", Owner: ",jobOwner,", File count: ",fileCount)
Name	"The transfer job is complete"
Source Nt Domain	User
Source User Name	User

Event ID 59

ArcSight Field	Vendor Field
Bytes In	bytesTransferredFromPeer
Bytes Out	bytesTransferred
Destination Host Name	peer
Device Custom Number 1	bytesTotal
Device Custom Number 1 Label	"Total Bytes"
Device Custom String 1	transferId
Device Custom String 1 Label	"Transfer ID"
Device Custom String 4	name

ArcSight Field	Vendor Field
Device Custom String 4 Label	"Job Title"
Device Custom String 5	Id
Device Custom String 5 Label	"Job ID"
File Create Time	fileTime
File Path	url
File Size	fileLength
Message	All of("BITS started the ",name," transfer job that is associated with the ",url," URL")
Name	"BITS started the transfer for job"

Event ID 60

ArcSight Field	Vendor Field
Bytes In	bytesTransferredFromPeer
Bytes Out	bytesTransferred
Destination Host Name	peer
Device Custom Number 1	bytesTotal
Device Custom Number 1 Label	"Total Bytes"
Device Custom String 1	transferId
Device Custom String 1 Label	"Transfer ID"
Device Custom String 4	name
Device Custom String 4 Label	"Job Title"
Device Custom String 5	Id
Device Custom String 5 Label	"Job ID"
File Create Time	fileTime
File Path	url
File Size	fileLength
Message	All of("BITS stopped the ",name," transfer job that is associated with the ",url," URL. The status code is 0x",hr)
Name	"BITS stopped transferring for job"
Old File Name	Both("Proxy :",proxy)
Old File Path	Both("Bandwidth Limit :",bandwidthLimit)
Reason	Both ("0x",hr)

Event ID 61

ArcSight Field	Vendor Field
Bytes Out	bytesTransferred
Destination Host Name	peer
Device Custom Number 1	bytesTotal
Device Custom Number 1 Label	"Total Bytes"
Device Custom String 1	transferId
Device Custom String 1 Label	"Transfer ID"
Device Custom String 4	name
Device Custom String 4 Label	"Job Title"
Device Custom String 5	Id
Device Custom String 5 Label	"Job ID"
File Create Time	fileTime
File Path	url
File Size	fileLength
Message	All of("BITS stopped the ",name," transfer job that is associated with the ",url," URL. The status code is 0x",hr)
Name	"BITS stopped transferring the job"
Old File Name	Both("Proxy :",proxy)
Reason	Both("0x",hr)

Microsoft Windows Event

The Windows event log is a detailed record of system, security and application notifications stored by the Windows operating system that is used by administrators to diagnose system problems and predict future issues.

These event logs are used to record important hardware and software actions that the administrator can use to troubleshoot issues with the operating system. The Windows operating system tracks specific events in its log files, such as application installations, security management, system setup operations on initial startup, and problems or errors.

The following sections provide information about the Microsoft Windows Event Log and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

  Microsoft Windows Server 2019

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Windows Event Log.

Configuring Windows Update Client

For complete information about Microsoft's Reporting and Windows-Windows Update Client, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":http://technet.microsoft.com/en-us/library/hh831416

Windows Update Client

Windows-Windows Update Client is a network service in Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, and Windows Server 2016 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

The following sections provides information about Windows Update Client and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Configuring Windows Update Client

For complete information about Microsoft's Reporting and Windows-Windows Update Client, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":http://technet.microsoft.com/en-us/library/hh831416

Mappings for Windows-WindowsUpdateClient

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft-Windows-WindowsUpdateClient'

Event 16

ArcSight Field	Vendor Field
Name	'Unable to Connect: Windows is unable to connect to the automatic updates service'

Event 17

ArcSight Field	Vendor Field
Name	'Installation Ready: The following updates are downloaded and ready for installation'

Event 18

ArcSight Field	Vendor Field
Name	'Installation Ready : The updates are downloaded and scheduled for installation'
Device Custom String 4 Label	stringConstant("Scheduled Install Date")
Device Custom String 4	schedinstalldate
Device Custom String 5 Label	stringConstant("Scheduled Install Time")
Device Custom String 5	schedinstalltime
Device Custom String 6 Label	stringConstant("Update List")
Device Custom String 6	updatelist

Event 19

ArcSight Field	Vendor Field
Name	'Installation Successful: Window successfully installed the updates'
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant("Update Revision Number"))

Event 20

ArcSight Field	Vendor Field
Name	Installation Failure: Windows failed to install the Updates
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant("Update Revision Number"))

Event 21

ArcSight Field	Vendor Field
Name	Restart Required : The computer must be restarted
Device Custom String 6 Label	stringConstant("Update List")
Device Custom String 6	updatelist

Event 22

ArcSight Field	Vendor Field
Name	Restart Required : The computer will be restarted

Event 27

ArcSight Field	Vendor Field
Name	Automatic Updates is now paused

Event 28

ArcSight Field	Vendor Field
Name	Automatic Update is now resumed

Event 43

ArcSight Field	Vendor Field
Name	Installation Started: Windows has started installing the updates
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant("Update Revision Number"))

Event 44

ArcSight Field	Vendor Field
Name	Downloading Started: Windows Update started downloading an update
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant("Update Revision Number"))

Microsoft Windows WMI Activity Trace

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment.

WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components.

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows WMI Activity Trace and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Mappings for Microsoft Windows WMI Activity Trace

Event 11

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	Microsoft Windows WMI Activity Trace
Name	WMI-Activity Query executed on Win23 BIOS
Device Custom String 1	ClientMachineFQDN
Device Custom String 3	CorrelationId
Device Custom String 4	IsLocal
Device Custom String 5	Operation
Device Custom Number 1	OperationId
Device Custom Number 2	GroupOperationId
Source Host Name	ClientMachine
Source User Name	User

ArcSight Field	Vendor Field
Source Process Id	ClientProcessId
File Create Time	ClientProcessCreationTime
File Path	NamespaceName

Microsoft Windows WMI Analytic and Operational

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment.

WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components.

The following sections provide information aboutWindows Update Client and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

  Microsoft Windows Server 2019

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Mappings for WMI Analytics Opereations

Mappings for Microsoft Windows WinRM Analytic

Event 788

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'
Name	Processing Client Request For Operation
Device Action	operationName

Event 789

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'

ArcSight Field	Vendor Field
Name	"Entering The Plugin For Operation".
Device Action	operationName
Request Url	resourceUri

Event 1050

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'
Name	"Sending Response For Operation"
Device Action	operationName

Event 1295

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'
Name	User Authenticated Successfully
Destination User Name	username

Mappings for Microsoft Windows WinRM Operational

Event 6

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'
Name	Creating WSMan Session
File Path	connection

Event 11

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'

ArcSight Field	Vendor Field
Name	Creating WSMan Shell
File Id	shellId
Request Url	resourceUri

Event 15

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'
Name	WSMan Command

Event 142

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'
Name	WSMan Operation Identify Failed
Device Action	operationName
Device Custom Number 3	errorCode
Device Custom Number 3 Label	Error Code

Event 161

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'
Name	WinRM Cannot Process The Request
Message	authFailureMessage

Event 162

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'
Name	Authenticating The User Failed

Event 169

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'
Name	The Message Resource Is Present But The Message Was Not Found In The Message Table
Destination User Name	username
Request Method	authenticationMechanism

Event 81

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'
Name	The Message Resource Is Present But The Message Was Not Found In The Message Table
Device Action	operationName

Event 82

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'Windows Remote Management'
Name	The Message Resource Is Present But The Message Was Not Found In The Message Table
Device Action	operation
Request Url	resourceURI

Microsoft WINS Server

Microsoft WINS servers are designed to prevent the administrative difficulties that are inherent in the use of both IP broadcasts and static mapping files such as LMHOSTS files. Microsoft WINS is designed to eliminate the need for IP broadcasts (which use valuable network bandwidth and cannot be used in routed networks), while providing a dynamic, distributed database that maintains computer name-to-IP-address mappings.

WINS servers use a replicated database that contains NetBIOS computer names and IP address mappings (database records). When Windows-based computers log on to the network, their computer name and IP address mapping are added (registered) to the WINS server database, providing support for dynamic updates. The WINS server database is replicated among multiple WINS servers in a LAN or WAN. One of the benefits of this database design is that it prevents different users from registering duplicate NetBIOS computer names on the network.

WINS clients, referred to as WINS- enabled clients, are configured to use the services of a WINS server. Windows NT- based clients are configured with the IP address of one or more WINS servers by using the WINS Address tab on the Microsoft TCP/IP Properties page in Control Panel > Network.

The following sections provide information about configuring Microsoft WINS Server and its event mappings to ArcSight data fields.

Supported versions

- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft WINS Server.

Configuring WINS

You can run the Registry Editor program at the command prompt to configure a WINS server by changing the values of the Registry parameters. Parameters for logging include:

Configuration Option	Description
Logging Enabled	Specifies whether logging of database changes to J50.log files should be turned on.
Log Detailed Events	Specifies whether logging events is verbose mode. (This requires considerable computer resources and should be turned off if you are tuning for performance.)

Windows 2016, 2012, and 8

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'
Device Custom String 4	Reason or Error Code

4097

ArcSight Field	Vendor Field
Name	'WINS initialized properly and is now fully operational'

4098

ArcSight Field	Vendor Field
Name	'WINS was terminated by the service controller'
Message	'WINS will gracefully terminate'

4119

ArcSight Field	Vendor Field
Name	'WINS received a packet that has the wrong format'

4143

ArcSight Field	Vendor Field
Name	'WINS scavenged its records in the WINS database'
Message	'The number of records scavenged is given in the data section'

4178

ArcSight Field	Vendor Field
Name	'The WINS Pull configuration key could not be created or opened'
Message	'Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem'

4179

ArcSight Field	Vendor Field
Name	'The WINS Push configuration key could not be created or opened'
Message	'Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem'

4180

ArcSight Field	Vendor Field
Name	'The WINS\\Parameters key could not be created or opened'
Message	'Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem'

4181

ArcSight Field	Vendor Field
Name	'# The subkey could not be created or opened'
Message	'This key should be there if you want WINS to do consistency checks on its database periodically. NOTE: Consistency checks have the potential of consuming large amounts of network bandwidth. Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem'

4224

ArcSight Field	Vendor Field
Name	'WINS encouintered a database error'
Message	'This may or may not be a serious error. WINS will try to recover from it'

4252

ArcSight Field	Vendor Field
Name	'WINS did not find any subkeys under the Pull key'

4253

ArcSight Field	Vendor Field
Name	'WINS did not find any subkeys under the Push key'

4309

ArcSight Field	Vendor Field
Name	'System Resource Information'
Device Custom Number 1	Processor Count
Device Custom Number 2	Physical Memory
Device Custom Number 3	Memory available for allocation

4318

ArcSight Field	Vendor Field
Name	'WINS could not start due to a missing or corrupt database'
Message	'Restore the database using WINS Manager (or winscl.exe found in the Windows 2000 Resource Kit) and restart WINS'

4325

ArcSight Field	Vendor Field
Name	'WINS could not read the Initial Challenge Retry Interval from the registry'

4326

ArcSight Field	Vendor Field
Name	'WINS could not read the Challenge Maximum Number of Retries from the registry'

4329

ArcSight Field	Vendor Field
Name	'The WINS server has started a scavenging operation'

4330

ArcSight Field	Vendor Field
Name	'The WINS server has completed the scavenging operation'

4337

ArcSight Field	Vendor Field
Name	'WINS Server could not initialize security to allow the read-only operations'

5001

ArcSight Field	Vendor Field
Name	'WINS is scavenging the locally owned records from the database'
Message	'The version number range that is scavenged is given in the data section, in the second to fifth words, in the order: from_version_number (low word, high word) to_version_number (low word, high word)'

5002

ArcSight Field	Vendor Field
Name	'WINS is scavenging a chuck on N records in the version number range from X to Y'
Message	'N, X and Y (low word, high word for version numbers) are given in the second to sixth words in the data section'

Oracle Audit

Auditing is a default feature of the Oracle server. The standard audit commands allow all system privileges to be audited along with access at the object level to any table or view on the database for select, delete, insert or update. Audit can be run for either successful or unsuccessful attempts or both. It can be for each individual user or for all users, and it can also be done at the session level or access level. At action level a single record is created per action and at session level one record is created for all audit actions per session.

Note: None of the connector versions support Oracle Multitenant at this time.

The following sections provide information about the SmartConnector for Microsoft Windows Event Log – Native: Oracle Audit and its event mappings to ArcSight data fields. Oracle database versions 10*g*, 11*g*, 12*c*R1 and 18*c* with Microsoft Windows Server 2012 are supported.

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Oracle Audit.

Configuring Auditing

For complete information about Oracle database auditing, see "Configuring Auditing" in the *Oracle Database Security Guide* for your database version.

Enabling Auditing

Database auditing is enabled and disabled by the AUDIT_TRAIL initialization parameter in the database initialization parameter file, `init.ora`. Setting it to `OS` enables database auditing and directs all audit records to an operating system file:

```
AUDIT_TRAIL=OS
```

Auditing Administrative Users

Sessions for users who connect as SYS can be fully audited, including all users connecting as SYSDBA or SYSOPER. Use the `AUDIT_SYS_OPERATIONS` initialization parameter to specify whether such users are to be audited. For example, the following setting specifies that SYS is to be audited:

```
AUDIT_SYS_OPERATIONS = TRUE
```

The default value, `FALSE`, disables SYS auditing.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Oracle Windows Event Log Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Source Service Name	EventSource
Device Vendor	'Oracle'

Event ID 4

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	Both ('Initializing SGA for instance ',%1)
Name	'Initializing SGA for instance'

Event ID 5

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	'Both ('Initializing SGA for process ',%1,' in instance ',%2)
Name	'Initializing SGA for process in instance'
Destination Process Name	%1 (Destination Process Name)

Event ID 8

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	Both ('Shutdown normal performed on instance ',%1)
Name	'Shutdown normal performed on instance'

Event ID 12

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	‘Oracle’
Message	Both (‘All process in instance ‘,%1,’ stopped’)
Name	‘All process in instance stopped’

Oracle Audit SYSDBA Event Mappings to ArcSight ESM Fields

Event ID 34

ArcSight ESM Field	Device-Specific Field
Destination Process Name	ProcessId
Destination User Name	DATABASE USER
Destination User Privileges	PRIVILEGE
Device Action	first word from ACTION
Device Custom Number 1	STATUS
Device Custom String 6	CLIENT TERMINAL
Device Event Class Id	first word of ACTION
Device External ID	DBID
Device Product	'ORACLESYSDBA'
Device Vendor	'ORACLE'
Message	first word from ACTION
Name	first word from ACTION
Source Host Name	CLIENT TERMINAL
Source User Name	CLIENT USER

Oracle Audit Trail Event Mappings to ArcSight ESM Fields

Event ID 34

ArcSight ESM Field	Device-Specific Field
Additional data	LOGOFF_DEAD
Additional data	LOGOFF_LREAD
Additional data	LOGOFF_LWRITE
Additional data	LOGOFF_PREAD
Additional data	OBJ_CREATOR
Additional data	SESSIONCPU
Additional data	SES_TID
Additional data	STATEMENT
Destination Host Name	USERHOST
Destination NT Domain	USERHOST
Destination Process Name	ProcessId
Destination User Name	USERID
Destination User Privileges	PRIV_USED
Device Action	ACTION
Device Custom Number 1	RETURNCODE
Device Custom Number 2	SESSIONID
Device Custom Number 3	ENTRYID
Device Custom String 1	COMMENT_TEXT
Device Custom String 2	TERMINAL
Device Custom String 4	SES_LABEL
Device Custom String 5	SES_ACTIONS
Device Event Class Id	ACTION
Device External ID	DBID
Device Product	'Oracle'
Device Severity	RETURNCODE
Device Vendor	'ORACLE'
File Name	Object name

ArcSight ESM Field	Device-Specific Field
Name	ACTION
Source Address	extracted IP address from SES_LABEL (will auto map to Source Host Name)
Source NT Domain	OSSUSERID
Source User Name	OS_USERID
Reason	RETURNCODE
Transport Protocol	PROTOCOL
Device Custom IPv6 Address 2	Source IPv6 Address
File Name	Name
Source Port	Port

Oracle Unified Audit Trail Event Mappings to ArcSight ESM Fields

Event ID 36

ArcSight ESM Field	Device-Specific Field
Device External ID	DBID
Device Custom Number 2	SESID
Device Custom Number 3	ENTRYID
Destination User Name	DBUSER
Source User Name	CURUSER
Device Action	ACTION
Name	ACTION
Device Custom Number 1	RETCODE
Reason	RETCODE
Device Event Class Id	ACTION
File Name	OBJNAME
Device Product	'Oracle'
Device Custom String 3	SCHEMA
Old File ID	CLIENTID

Powershell

PowerShell is a task-based command-line shell and scripting language built on .NET. PowerShell helps system administrators and power-users rapidly automate tasks that manage operating systems (Linux, macOS, and Windows) and processes.

PowerShell commands let you manage computers from the command line. PowerShell providers let you access data stores, such as the registry and certificate store, as easily as you access the file system. PowerShell includes a rich expression parser and a fully developed scripting language.

As it is widely used by the black hat community for initial access and further lateral movement within an enterprise, it is critical to properly collect and parse Windows Powershell logs. This would open the doors to writing correlation and hunt/search tools to find the APT's and other advanced threats.

The following sections provide information about the SmartConnector for Microsoft Windows Event Log – Native: Powershell and its event mappings to ArcSight data fields.

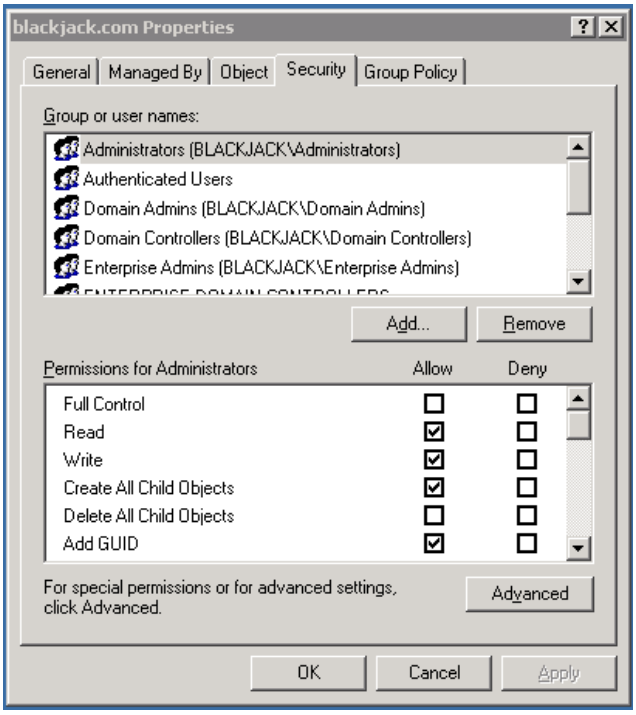
The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Microsoft Powershell Windows Event Log – Native: Powershell.

Configuring Auditing for Specific Powershell Objects

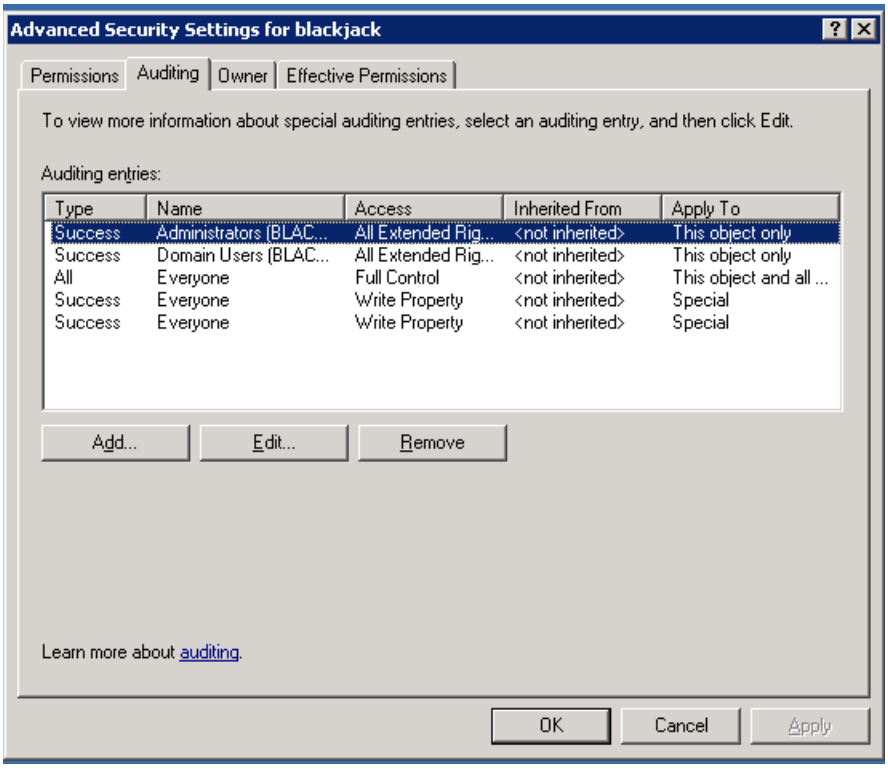
After you configure an audit policy setting, you can configure auditing for specific objects, such as users, computers, organizational units, or groups, by specifying both the types of access and the users whose access you want to audit.

To configure auditing for specific Powershell objects (steps may vary for differing Windows operating systems):

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Powershell Users and Computers**.
2. Verify that **Advanced Features** is selected on the **View** menu (the command has a checkmark beside it).
3. Right-click on the Powershell object you want to audit (`blackjack.com` in the example) and select **Properties**.



4. Click the **Security** tab, then click the **Advanced** button; **Advanced Security Settings** for the object is displayed. Click the **Auditing** tab.



5. To add an object, click **Add**.

6. Either enter the name of either the user or the group whose access you want to audit in the **Enter the object name to select** box, then click **OK**, or browse the list of names and then double-click either the user or the group whose access you want to audit.
7. Click to select either the **Successful** checkbox or the **Failed** checkbox for the actions you want to audit, then click **OK**. Click **OK** on the next two windows to exit.

Mappings for PowerShell Events

General Mappings

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'PowerShell'

Windows PowerShell Mappings

Event 400, 403

ArcSight Field	Vendor Field
Name	'Engine state is changed'
Message	'Engine state is changed from',%2,'to',%1
File Hash	%1
Old FileHash	%2
Device Custom Number 2	SequenceNumber(Sequence Number)
Device Custom String 4	All of ('Host Name: ',HostName,', Host Version: ',HostVersion,', Host ID: ',HostId) (Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	CommandName
File Type	CommandType
Old File Name	ScriptName
File Path	CommandPath
File Permission	CommandLine
Source NT Domain	UserId
Source User Name	UserId

Event 500, 501

ArcSight Field	Vendor Field
Name	'Command State'
Message	'Command "',%1,'" is ',%2
Device Custom Number 2	SequenceNumber(Sequence Number)
Device Custom String 4	All of ('Host Name: ',HostName,', Host Version: ',HostVersion,', Host ID: ',HostId) (Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	CommandName
File Type	CommandType
Old File Name	ScriptName
File Path	CommandPath
File Permission	CommandLine
Source NT Domain	UserId
Source User Name	UserId

Event 600

ArcSight Field	Vendor Field
Name	'Provider State'
Message	'Provider "',%1,'" is ',%2
Device Custom Number 2	SequenceNumber(Sequence Number)
Device Custom String 4	All of ('Host Name: ',HostName,', Host Version: ',HostVersion,', Host ID: ',HostId) (Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	CommandName
File Type	CommandType
Old File Name	ScriptName

ArcSight Field	Vendor Field
File Path	CommandPath
File Permission	CommandLine
Source NT Domain	UserId
Source User Name	UserId

Event 800

ArcSight Field	Vendor Field
Name	'Pipeline execution details for command line'
Message	'Pipeline execution details for command line: ',%1
Device Custom String 1	%3(Details)
Device Custom Number 2	SequenceNumber(Sequence Number)
Device Custom String 4	All of ('Host Name: ',HostName,', Host Version: ',HostVersion,', Host ID: ',HostId) (Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
Old File Name	ScriptName
File Permission	CommandLine
Source NT Domain	UserId
Source User Name	UserId

Windows Microsoft-Windows-PowerShell/Operational Mappings

Event 4100

ArcSight Field	Vendor Field
Name	'Error Message'
Device Custom String 1	UserData(User Data)
Device Severity	Severity
Device Custom String 4	All of ('Host Name: ',Host Name,', Host Version: ',Host Version,', Host ID: ',Host Id)(Host Information)
Request Client Application	HostApplication

ArcSight Field	Vendor Field
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	CommandName
File Type	CommandType
Old File Name	ScriptName
File Permission	CommandLine
Device Custom Number 2	SequenceNumber(Sequence Number)
Source NT Domain	User
Source User Name	User
Device Custom String 6	Connected User(Connected User)
Request Context	Shell ID
Message	Error Message,' ',Recommended Action
Reason	Fully Qualified Error ID

Event 4103

ArcSight Field	Vendor Field
Name	'Command Invocation'
Message	Payload
Device Custom String 1	UserData(User Data)
Device Severity	Severity
Device Custom String 4	All of ('Host Name: ',Host Name,', Host Version: ',Host Version,', Host ID: ',Host Id)(Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	Command Name
File Type	Command Type
Old File Name	Script Name
File Path	Command Path
File Permission	Command Line
Device Custom Number 2	SequenceNumber(Sequence Number)

ArcSight Field	Vendor Field
Source NT Domain	User
Source User Name	User
Device Custom String 6	Connected User(Connected User)
Request Context	Shell ID

Event 4104

ArcSight Field	Vendor Field
Name	'Creating Scriptblock text'
Message	'Creating Scriptblock text(',MessageNumber,' of ',MessageTotal,'\\):',ScriptBlockText
Device Custom Number 1	MessageNumber(Message Number)
Device Custom Number 2	Message Total
File Name	ScriptBlockText
File Path	Path

Event 4105

ArcSight Field	Vendor Field
Name	'Started invocation of ScriptBlock'
Message	'Started invocation of ScriptBlock ID',ScriptBlockId
File ID	ScriptBlockId
Old File ID	RunspaceId

Event 8193

ArcSight Field	Vendor Field
Name	'Creating Runspace object'
Message	'Creating Runspace object Instance Id:',param1
Device Custom String 5	param1(Instance Id)

Event 8194

ArcSight Field	Vendor Field
Name	'Creating RunspacePool object'
Message	'Creating RunspacePool object Instance Id:',InstanceId

ArcSight Field	Vendor Field
Device Custom String 5	param1(Instance Id)
Device Custom Number 1	MaxRunspaces(Max Runspaces)
Device Custom Number 2	MinRunspaces(Min Runspaces)

Event 8195

ArcSight Field	Vendor Field
Name	'Opening RunspacePool'
Message	'Opening RunspacePool'

Event 8196, 12039

ArcSight Field	Vendor Field
Name	'Modifying activity Id and correlating'
Message	'Modifying activity Id and correlating'

Event 8197

ArcSight Field	Vendor Field
Name	'Runspace state changed'
Message	'Runspace state changed to ',param1
Device Action	param1

Event 24577

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE has started to run script file'
Message	'Windows PowerShell ISE has started to run script file ',FileName
File Path	FileName

Event 24579

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stopping the current command'
Message	'Windows PowerShell ISE is stopping the current command'

Event 24580

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is resuming the debugger'
Message	'Windows PowerShell ISE is resuming the debugger'

Event 24581

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stopping the debugger'
Message	'Windows PowerShell ISE is stopping the debugger'

Event 24582

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stepping into debugging'
Message	'Windows PowerShell ISE is stepping into debugging'

Event 24583

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stepping over debugging'
Message	'Windows PowerShell ISE is stepping over debugging'

Event 24584

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stepping out of debugging'
Message	'Windows PowerShell ISE is stepping out of debugging'

Event 24592

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is enabling all breakpoints'
Message	'Windows PowerShell ISE is enabling all breakpoints'

Event 24593

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is disabling all breakpoints'
Message	'Windows PowerShell ISE is disabling all breakpoints'

Event 24594

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is removing all breakpoints'
Message	'Windows PowerShell ISE is removing all breakpoints'

Event 24595

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is setting the breakpoint'
Message	'Windows PowerShell ISE is setting the breakpoint at line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 24596

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is removing the breakpoint'
Message	'Windows PowerShell ISE is removing the breakpoint on line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 24597

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is enabling the breakpoint'
Message	'Windows PowerShell ISE is enabling the breakpoint on line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 24598

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is disabling the breakpoint'
Message	'Windows PowerShell ISE is disabling the breakpoint on line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 24599

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE has hit a breakpoint'
Message	'Windows PowerShell ISE has hit a breakpoint on line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 40961

ArcSight Field	Vendor Field
Name	'PowerShell console is starting up'
Message	'PowerShell console is starting up'

Event 40962

ArcSight Field	Vendor Field
Name	'PowerShell console is ready for user input'
Message	'PowerShell console is ready for user input'

Event 53249

ArcSight Field	Vendor Field
Name	'Scheduled Job started'
Message	'Scheduled Job ',ScheduledJobDefName,' started at ',StartTime
Device Custom String 1	ScheduledJobDefName(Scheduled Job Name)
Start Time	Start Time

Event 53250

ArcSight Field	Vendor Field
Name	'Scheduled Job completed'
Message	'Scheduled Job ',ScheduledJobDefName,' completed at ',StopTime,' with state ',State
Device Custom String 1	ScheduledJobDefName(Scheduled Job Name)
End Time	StopTime
Device Action	State

Event 53504

ArcSight Field	Vendor Field
Name	'Windows PowerShell has started an IPC listening thread'
Message	'Windows PowerShell has started an IPC listening thread on process: ',param1,' in AppDomain: ',param2
Destination Process Id	param1
Device Custom String 1	param2(App Domain)

Remote Access

Routing and Remote Access is a network service in Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, and Windows Server 2016 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

The following sections provide information about the SmartConnector for Microsoft Windows Event Log – Native: Remote Access Service and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Configuring Remote Access

For complete information about Microsoft's Reporting and Remote Access Service, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)": http://technet.microsoft.com/en-us/library/hh831416

Mappings for Remote Access Events

Mappings for Windows 2016, 2012, 2012 R2, 8, and 10

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

20088

ArcSight Field	Vendor Field
Name	'Remote Access Server acquired IP Address'
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')
Destination Address	%1 (Assigned Address)

20106

ArcSight Field	Vendor Field
Name	'Unable to add interface'
Message	One of ('Unable to add the interface ',%1,' with the Router Manager for the ',%2,' protocol. The following error occurred: ',%3), ('Unable to add the interface ',%2,' with the Router Mnager for the ',%3,' protocol. The following error occurred: ',%4))
Device Outbound Interface	One of (%1, %2)
Application Protocol	One of (%2, %3)
Device Custom String 5	Routing Domain ID

20169

ArcSight Field	Vendor Field
Name	'Unable to contact a DHCP server'
Message	Both ('The Automatic Private IP Address ',%1,' will be assigned to dial-in clients. Clients may be unable to access resources on the network.')
Source Address	%2 (Address)

20184

ArcSight Field	Vendor Field
Name	'Interface is unreachable'
Message	Both ("Interface ",One of(%1,%2)," is unreachable because it is not currently connected to the network.")
Device Inbound Interface	One of (%1, %2)
Device Custom String 5	Routing Domain ID

20249

ArcSight Field	Vendor Field
Name	'Failed to authenticate'
Message	Both ('The user ',%2,' has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)

20252

ArcSight Field	Vendor Field
Name	'Authentication process did not complete'
Message	Both ('The user connected to port ',%2,' has been disconnected because the authentication process did not complete within the required amount of time.')
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)

20255

ArcSight Field	Vendor Field
Name	'Connection was prevented'
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Message	%4 (Message Text)

20258

ArcSight Field	Vendor Field
Name	'Account does not have Remote Access privilege'
Message	Both ('The account for user ',%3,' connected on port ',%4,' does not have Remote Access privilege. The line has been disconnected.')
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)

20266

ArcSight Field	Vendor Field
Name	'Successfully authenticated'
Message	Both ('The user ',One of (%2, %3),' has connected and has been successfully authenticated on port ',One of (%3, %4),'. Data sent and received over this link is strongly encrypted.')
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Source User Name	One of (%2, %3)
Source NT Domain	One of (%2, %3)
Application Protocol	One of (%3, %4)
Source Port	One of (%3, %4)

20271

ArcSight Field	Vendor Field
Name	'Failed an authentication attempt'
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)

ArcSight Field	Vendor Field
Source Address	%3 (Address)
Message	Both (‘The user ‘,%2,’ connected from ‘,%3,’ but failed an authentication attempt due to the following reason: ‘,%4’)
Reason	%5 (Reason)

20272

ArcSight Field	Vendor Field
Name	‘User connected and disconnected’
Message	Both (The user ‘,One of (%2, %3),’ connected on port ‘,One of (%3, %4),’ on ‘,One of (%4, %5),’ at ‘,One of (%5, %6),’ and disconnected on ‘,One of (%6, %7),’ at ‘,One of (%7, %8),’. The user was active for ‘,One of (%8, %9),’ minutes ‘, One of (%9, %10),’ seconds. ‘, One of (%10, %11),’ bytes were received. The reason for disconnecting was ‘, One of (%12, %13),’. The tunnel used was ‘, One of (%13, %14),’. The quarantine state was ‘, One of (%14, %15),’.’)
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Source User Name	One of (%2, %3)
Source NT Domain	One of (%2, %3)
Application Protocol	One of (%3, %4)
Source Port	One of (%3, %4)
Start Time	Both (One of (%4, %5),’ ‘,One of (%5, %6)))
End Time	Both (One of(%6,%7)," ",One of(7,%8))
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	One of (%10, %11)
Bytes In	One of (%11, %12)
Additional data	One of (%12, %13)
Additional data	One of (%13, %14)
Additional data	One of (%14, %15)

20274

ArcSight Field	Vendor Field
Name	'User connected and has been assigned address'
Message	Both ('The user ',One of (%2, %3),' connected on port ',One of (%3, %4),' has been assigned address ',One of (%4, %5))
Device Custom String 4	correlation-ID
Device Custom String 5	Routing Domain ID
Source User Name	One of (%2, %3)
Source NT Domain	One of (%2, %3)
Application Protocol	One of (%3, %4)
Source Port	One of %3, %4)
Destination Address	One of (%4, %5)

20275

ArcSight Field	Vendor Field
Name	'User disconnected'
Message	Both ('The user with ip address ',One of (%2, %3),' has disconnected')
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Source Address	One of (%2, %3)

Mappings for Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	%1 (Assigned Address)

ArcSight Field	Vendor Field
Message	Both (‘The Remote Access Server acquired IP Address ‘,%1,’ to be used on the Server Adapter.’)

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	%1 (Interface)
Application Protocol	%2 (Protocol)
Message	%3 (Message Text)

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	%1 (Interface)
Message	Both (‘Interface ‘,%1,’ is unreachable because it is not currently connected to the network.’)

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Message	Both (‘The user ‘,%2,’ has connected and failed to authenticate on port ‘,%3,’. The line has been disconnected.’)

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	Both (‘The user connected to port ‘,%2,’ has been disconnected because the authentication process did not complete within the required amount of time.’)

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	%4 (Message Text)

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both (‘The account for user ‘,%3,’ connected on port ‘,%4,’ does not have Remote Access privilege. The line has been disconnected.’)

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)

ArcSight Field	Vendor Field
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The user ',One of (%2,%3),' has connected and has been successfully authenticated on port ',One of (%3,%4),'. Data sent and received over this link is strongly encrypted.')

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Source Address	%3 (Address)
Reason	%5 (Reason)
Message	%4 (Message Text)

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Start Time	Both (%4, %5)
End Time	Both (%5, %6)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	%10 (Bytes Out)
Bytes In	%10 (Bytes In)

ArcSight Field	Vendor Field
Additional data	%12
Additional data	%13
Additional data	%14
Message	Both (‘The user ‘,%2,’ connected on port ‘,%3,’ on ‘,%4,’ at ‘,%5,’ and disconnected on ‘,%6,’ at ‘,%7,’. The user was active for ‘,%8,’ minutes, ‘,%9,’ seconds, ‘,%10,’ bytes were sent and ‘,%11,’ bytes were received. The reason for disconnecting was ‘,%12,. The tunnel used was ‘,%13,’. The quarantine state was ‘,%14,’.’)

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Destination Address	%4 (Assigned Address)
Message	Both (‘The user ‘,%2,’ connected on port ‘,%3,’ has been assigned address ‘,%4’)

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID
Source Address	%2 (Address)
Message	Both (‘The user with ip address ‘,%2,’ has disconnected’)

Collecting Forwarded Events

The connector has the ability to read events forwarded to a Windows Event Collector host. Windows Event Collection is a Microsoft capability that lets a Windows host collect events from multiple sources. Collecting forwarded events is different than the traditional event collection because the events are collected from multiple sources.

With Microsoft Windows Event Collector (WEC), you can subscribe to receive and store events on a local computer (event collector) that are forwarded from any number of remote computers (event sources). Before using this feature, refer to Microsoft Windows documentation, to know more about Windows Event Collector functionality.

Note: When configuring Windows Event Collection (WEC), Microsoft by default adds to every forwarded event a RenderingInfo section that is a textual description of an event. This extra section introduces negative impacts on the resource usage of the WEC machine as well as the performance of the connector. Therefore, Micro Focus advises that you disable the RenderingInfo section.

To do so, run the following command from the Windows command console: wecutil ss <subscription-name> /cf:events , where subscription-name is the WEC configuration created for event forwarding.This can be found in the Event Viewer > Subscriptions folder.

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 connector would normally have access.

Note: Security events cannot be forwarded to the Security event log on a collector machine, but can be forwarded to other log types

Source Hosts Windows OS Version

When the connector is configured with the log that has forwarded events, the Windows OS version of the event source host is not populated automatically in the normalized events. To have this value populated, the Windows OS version should be provided as a source host file or the Active Directory should be configured. If the Windows OS version is available from the source host file as well as Active Directory, the value from Active Directory takes precedence. 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. Newly discovered hosts are added to the lookup automatically without reconfiguring the connector itself.

Active Directory information is checked upon connector startup and every 24 hours (86400000 milliseconds). To change the time setting, locate the agent.properties file in $ARCSIGHT_HOME/current/agent and set the hostbrowsingthreadsleeptime parameter to the number of milliseconds between host browsing queries.) This value should be greater than 0; if the value is set to 0, it will not perform periodic host browsing. For the connector to be able to browse the Active Directory to retrieve source host Windows version information, it should be placed within the same forest as the Active Directory.

File as Source for OS Version

When this selection is chosen during connector configuration, create a source host file in .csv format that contains the host name and Windows OS versionand upload this file during the connector installation/configuration process (the WEF Source Hosts File Name in step 9).

Note: The host file, which is imported to or exported from the host table during installation, and the source host file specified in the WEF Source Hosts File Name field are two different entities. The source host file contains only the host name and version information to populate the version in the device version field.

When creating a source host file, make sure to specify the FQDN registered with Active Directory, as the connector finds the version information using the computer name in the event. An example of the source host file could be:

```
hostsa.domaina.com,Windows 7
```

```
hostsb.domainb.com,Windows 8
```

```
hostsc.domainb.com,Windows Server 2012
```

```
Hostsd.domaind.com,Windows Server 2016
```

The valid versions descriptions (case sensitive) that can be used in source hosts files are:

```
Windows Vista
```

```
Windows Server 2008
```

```
Windows Server 2008 R2
```

```
Windows Server 2012
```

```
Windows Server 2012 R2
```

```
Windows Server 2016
```

```
Windows 7
```

```
Windows 8
```

```
Windows 10
```

Note: OS version information is optional; events may still be parsed in a majority of cases.

Once configured, the OS version is loaded from the source host file when the connector is running on its first run, and is reloaded on the next startup of the connector when the source host file has a timestamp different from the one loaded from the last file processed.

The device version will not be populated in the normalized events.

Additional Connector Configurations

You can refer to the following sections for additional and optional connector configurations:

Configuring Custom Logs and Filtering

If you selected **Custom logs** in the **Select logs for event collection** section of the initial configuration window,and you want to add filtering for the local host, check **Custom Logs** in the **Select logs for event collection** section to ensure this window is displayed for you to enter filter parameters.

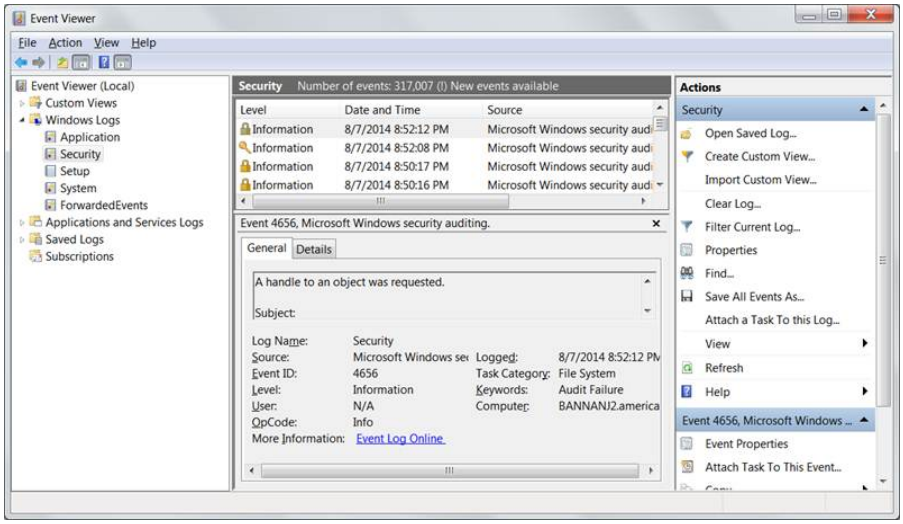
The parameters for each host are given in full along with descriptions in the following table. Selections from the initial parameter entry window for the local host are reflected in the first row of the table. Select options and provide custom log and filter information for each additional host manually.

After entering the parameter information, click **Next**.

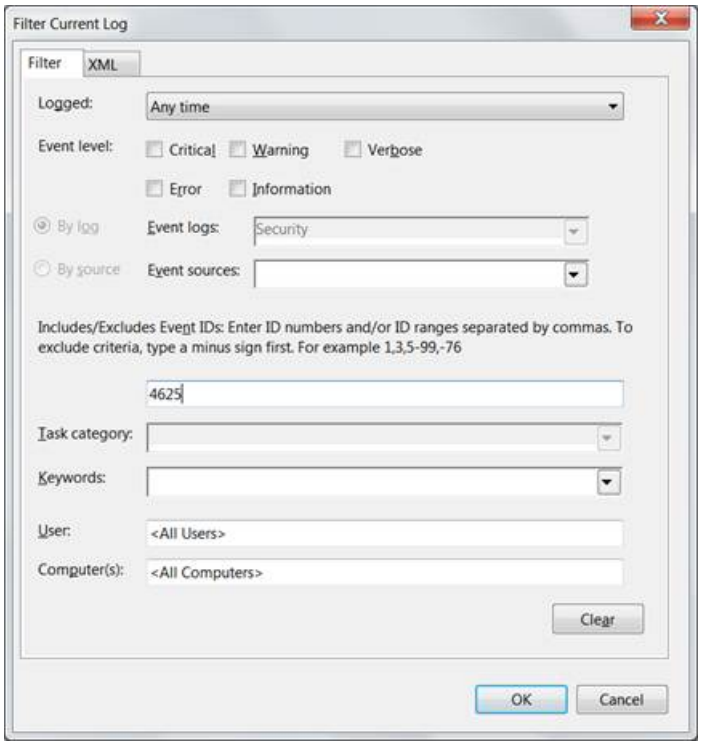
Configuring Filter

To configure a filter, first launch the event viewer and select the event log that needs the filter setting.

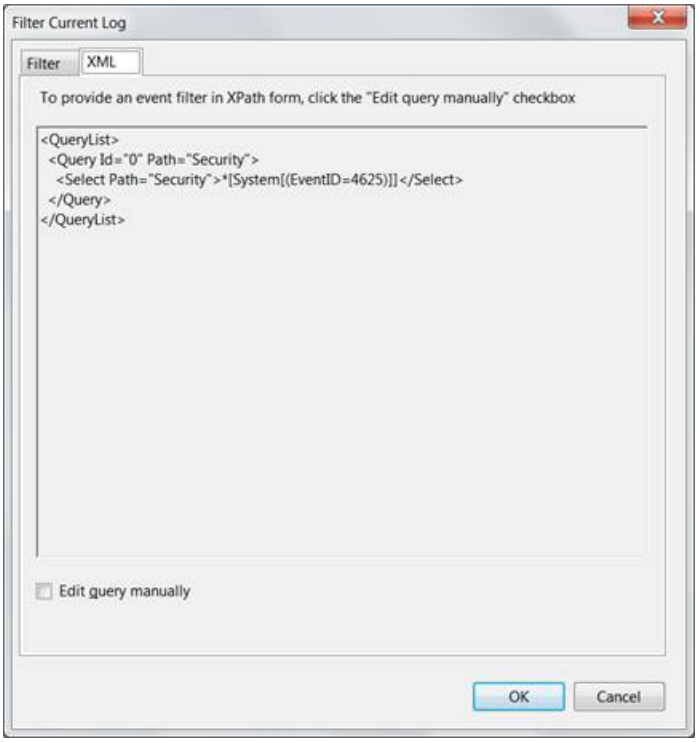
1. Click **Filter current log** to set the filter.



For example, to collect the logon failure events whose Event ID is 4625, enter the Event ID number as shown in the following figure.



2. Click the **XML** tab. The query is displayed in XML.



The expression that appears between `<Select>` and `</Select>` is the value that can be entered in the filter. Here it writes `*[System[(EventID=4625)]]`. This can be copied to the **Filter** column in the host table parameter for the desired event log.

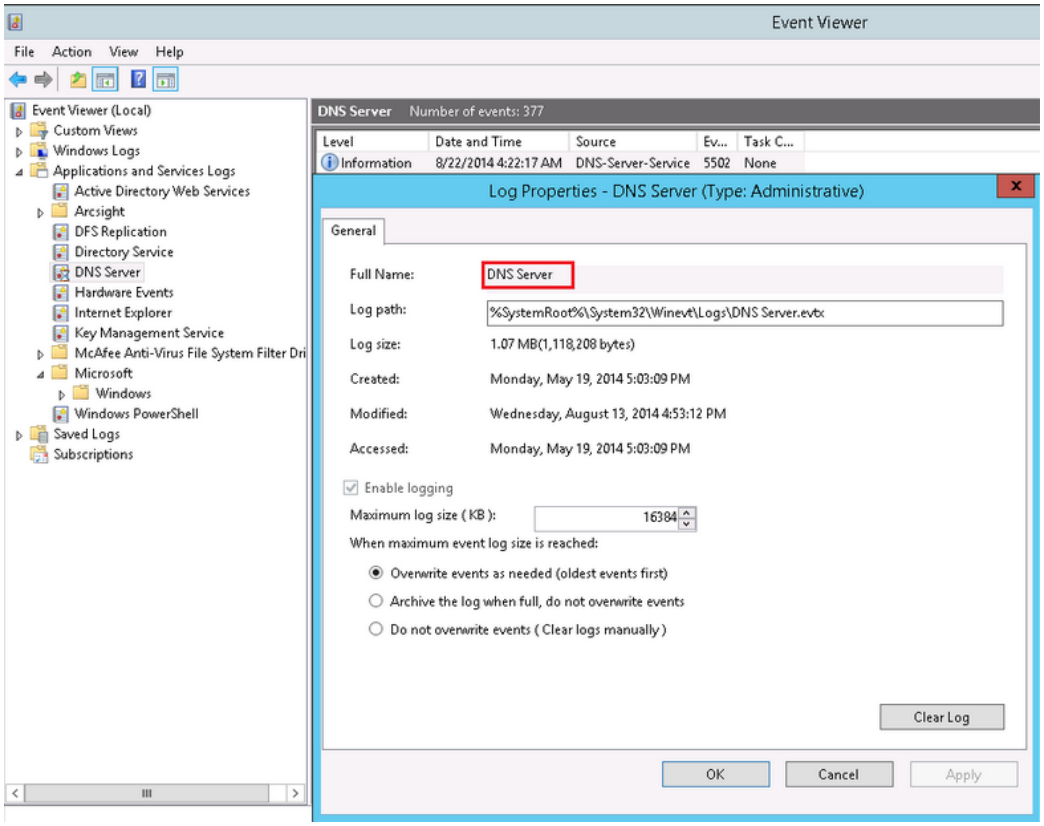
Note: In certain cases, the text cannot be directly copied to the Filter column in the UI wizard. If the filter text contains “gt;”, “lt;”, “gt;=” or “lt;=” , you must replace it with “>”,“<”, “>=” or “<=” respectively.

Specifying 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. Applications also can generate events for a custom application event log, such as DNS Server, Directory Service, Exchange Auditing, and so on. (Parsing support for only the event header is supported for application events.)

For example, specify `Directory Service` for Active Directory and `Exchange Auditing` for Microsoft Exchange Audit. For Microsoft Windows Print Service Admin log, use `Microsoft-Windows-PrintService/Admin`.

To identify the Custom Event Log Name, select the **Custom Application Event Log** in the Microsoft Windows **Event Viewer**. The log name can be found from the properties of the event log in the **Full Name** field, as shown in the following figure.



For more information about setting this parameter, see "Advanced Configuration Parameters per Host."

Configuring the Host Browsing Thread Sleep Time

If you selected **Use Active Directory for OS version** to specify the Windows OS version for the hosts from which you want to collect eventSelect this option, then the connector retrieves the host details from the configured Active Directory to identify the event source host Windows version information.

Newly discovered hosts are added to the lookup automatically without having to reconfigure the connector itself. Active Directory information is verified every time the connector starts and every 24 hours (86400000 milliseconds).

To change the time setting:

1. Open the `agent.properties` file in `$ARCSIGHT_HOME/current/agent`
2. Set the **hostbrowsingthreadsleeptime** parameter to the number of milliseconds between host browsing queries. This value must be greater than 0. If the value is set to 0, then it does not perform periodic host browsing.

Creating a Source Hosts File

During connector configuration, if **File as Source for OS Version** is selected, then create a source host file in .csv format with the host name and Windows OS version, and upload the file during the connector configuration.

Note: The host file, which is imported to or exported from the host table during installation, and the source host file specified in the **WEF Source Hosts File Name** field are two different entities. The source host file contains only the host name and version information to populate the version in the device version field.

When creating a source host file, make sure to specify the FQDN registered with Active Directory, as the connector finds the version information using the computer name in the event. An example of the source host file could be:

```
hostsa.domaina.com,Windows 7
hostsb.domainb.com,Windows 8
hostsc.domainb.com,Windows Server 2012
Hostsd.domaind.com,Windows Server 2016
```

The valid versions descriptions (case sensitive) that can be used in source hosts files are:

```
Windows Vista
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows 7
Windows 8
Windows 10
```

Note: OS version information is optional; events may still be parsed in a majority of cases.

After the configuration, the OS version is loaded from the source host file when the connector is running on its first run, and is reloaded on the next startup of the connector when the source host file has a timestamp different from the one loaded from the last file processed.

The device version will not be populated in the normalized events.

Collecting Events from the Event Log

To set up the connector to collect application events:

1. From $ARCSIGHT_HOME\current\bin, double-click **runagentsetup.bat**.
2. Select **Modify Connector** on the window displayed and click **Next**.
3. Select **Modify connector parameters** and click **Next**.
4. Select Navigate to the **Modify table parameters** window.
5. To collect events from an application log, modify the **Application** field by selecting **true** for event collection in the Application field and enter **Directory Service** in the **Custom Log Names** field.

   You can specify multiple Custom Log Names in a comma-separated format; for example:

   ```
   Directory Service, Exchange Auditing
   ```
6. Click **Next** to update the parameters; when you receive the successful update message, click **Next**.
7. Select **Exit** and click **Next** to exit the configuration wizard.
8. Restart the connector for your changes to take effect.

For more information about application event support, see the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Native*.

Configuring Advanced Options

This section documents some of the advanced configuration parameters available with this connector. The table following the procedure for accessing advanced configuration parameters details the parameters you may choose to adjust, depending upon the needs of your enterprise.

Accessing Advanced Parameters

After SmartConnector installation, you can edit the `agent.properties` file to modify parameters. This file can be found at `$ARCSIGHT_HOME\current\user\agent`.

Advanced Container Configuration Properties

Specify	Parameter	Default
The protocol used between the connector and the collector. Currently supports TCP protocol.	`mq.transport.protocol`	`tcp`
The port used between the connector and the collector. The specified port will be bound during the connector installation. If more than one connector is to be installed on the same host, configure this with an unused port number.	`mq.server.listener.port`	`61616`
The maximum disk size (in Kilobytes) to be used for message persistence by the MQ component.	`mq.persistent.storage.limit`	`409600`
The maximum memory size (in Kilobytes) to be used by the MQ component.	`mq.memory.limit`	`65536`
The frequency to clean up the processed messages from persistent store in milliseconds. The storage needs to be cleaned up in order to receive more messages from `winc-agent`.	`mq.persistent.storage.cleanup.interval`	`10000`
The number of messages, event batches to preload in memory. Received messages from the winc-agent are persisted into the memory store, but it has to be loaded into the memory for processing. Preloading reduces the waiting time for the data loading and helps with performance.	`mq.consumer.prefetch.size`	`80`

Specify	Parameter	Default
Whether the SID translation is required or not. The SID should be present in the remote host. **Note:** There may be a slight performance hit when being used.	`winc.winc-agent.enableSidTranslation`	`True`
This property enables disk space check.	`mq.enable.space.check`	`True`
Time interval to check if the persist storage is more than 70%.	`mq.storage.check.interval`	`10`
If the activemq persist storage usage is greater than 70%, the space increases. The modified storage limit is updated in `agent.properties`.	`mq.max.percentage.used`	`70`
Maximum allocated divisions in the disk space.	`mq.max.disk.allocation`	`50`
If the mq persist store usage is less than 30%, the space decreases. The mq persist storage space should not be less than 409600 (default). The modified storage limit is updated in `agent.properties`.	`mq.min.percentage.used`	`30`

Advanced Common Configuration Parameters

Specify	Parameter	Default
Thread count for event processing threads dedicated for a single collector.	`eventprocessthreadcount`	`10`
The queue size used to hold the ready to execute event processing task to improve performance. Larger queue length means bigger memory footprint and it does not necessarily help with performance improvement, as a limited number of threads are available for processing.	`Executequeuelength`	`100`
By default the statistics are calculated every 10 minutes and dumped into both the `agent.log` and to the `EventStats` report file in `user/agent/agentdata`. This interval governs how often stats are calculated. Stats include average per last interval for events per second.	`pdastatsinterval`	`600000ms`
Whether to preserve the last ID processed before connector terminated or device went down.	`preservestate`	`true`
Event count before writing the preserve state.	`preservedstatecount`	`100`
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
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

Advanced Configuration Parameters for SID and GUID Translation

Specify	Parameter	Default
To enable GUID translation	`enableguidtranslation`	`false`
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`
Interval in milliseconds (ms) at which the SID and GUID entries are to be expired from the caches	`sidguidcacheexpirationthreadsleeptime`	`600000`
Interval in ms at which the SID and GID 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`

Customizing Event Source Mapping

The Windows Event Log – Native 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:

```
<Channel>\<ProviderName>.sdkkeyvaluefilereader.properties
```

This convention works in the vast majority of cases but sometimes the parser needs more flexibility. In these cases, you can customize where to find these parsers by redirecting the variables `Channel` and `ProviderName`. For even more flexibility, the input `ProviderName` can be matched against a regular expression to avoid duplicate entries with minimal changes.

Creating an Override Map File

1. Navigate to `$ARCSIGHT_HOME/current/user/agent/fcp/winc/core_maps` and create an override map file with the name `customeventsource.map.csv` including the following columns:

   ```
   SourceChannel
   SourceProviderNamePattern
   TargetProviderName
   TargetChannel
   ```

   The `SourceProviderNamePattern` value can be a string or a regular expression.
2. If there is no `winc/coremaps` subdirectory at `$ARCSIGHT_HOME/current/user/agent/fcp`, create one.
3. The last field `TargetChannel` is optional and, if empty, will be understood as the same as `SourceChannel`.

Customizing Event Parsing in a Clustered Environment

The default parser filename convention can cause problems in clustered environments, where the same event from different clusters can have different customized provider names. For example, SQL Server application events have the ProviderName `MSSQLSERVER`, resulting in a parser name of `application\mssqlserver.sdkkeyvaluefilereasder.properties`.

In a clustered SQL Server environment, you can customize and configure the provider name for each cluster as `SQLSERVER01`, `SQLSERVER02`, and so forth. However, if the connector expects `MSSQLSERVER` as the provider name, the parsing fails for events with customized provider names, if the different providers have different names

To avoid this outcome, you can map all these different providers into one provider name value using the map file `$ARCSIGHT_HOME/user/agent/fcp/winc/core_maps/customeventsource.map.csv`.

The following are example entries based for a clustered environment:

```
Application, MSSQLSERVER01, MSSQLSERVER, Application
Application, MSSQLSERVER\d*, MSSQLSERVER, Application
Application, MSSQLSERVER.*, MSSQLSERVER, Application
```

The following are contents of a sample `customeventsource.map.csv` file with two entries:

```
#SourceChannel, SourceProviderNamePattern, TargetProviderName,
 System,        Service.*,                 service_control_manager,
 Application,   MSSQLSERVER.*,             MSSQLSERVER,
```

Creating Custom Parsers for System and Application Events

The SmartConnector provides complete parsing of both the Windows event header and event description for all security events and some system events.

For all system and application events, the connector provides complete parsing of the Windows event header. Also, the connector provides a framework to create and deploy your own parsers to parse the event description. Such a parser can parse events specific to a Channel and ProviderName.

- 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**.

Note: Custom Parsers or overrides you create are customizations. These are not certified for use through the ArcSight Quality Assurance Life Cycle of Testing. These are to be developed, tested, and maintained by the creator of the Custom Parser or override.

Before Creating a Parser

Complete the following steps 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 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 in JSON format. Using these generated raw events, see "Create and Deploy Your Own Parser" to map the values of these keys to the ArcSight event schema fields by creating a parser file.

   Note: Not all raw events will have key-value pairs in the event body. Such events do not require that you create a parser to map anything to the ArcSight event schema fields. But you can still choose to create a parser to map the event name or description for such events.

Creating and Deploying Your Own Parser

To create and deploy your own parser:

1. Navigate to the directory location to deploy the parser file:

   ```
   $ARCSIGHT_HOME\user\agent\fcp\winc
   ```

2. Identify the Channel for the events that need to be parsed (for example: System, Application, Directory Service, DNS Server, Key Management Service, and so on).
3. Identify the provider name of the events that need to be parsed, as events collected from a single channel can be generated by multiple provider names. For example, events collected from `Channel: System` can be generated by `ProviderName`: `Service Control Manager`, `WINS`, and so on.
4. Identify the `SectionName` of the event body that needs to be parsed, such as `EventData`, `UserData`, and so on.
   a. To parse the `EventData` section of the event body, create a key value parser file with the following naming convention, in the directory location identified in **Step 1**.

      ```
      \{Normalized Channel}\{Normalized ProviderName}.sdkkeyvaluefilereader.
      properties
      ```

      For example, the key-value parser file name for:

      - Channel: `Security`
      - ProviderName: `Microsoft Windows Event Log`
      - SectionName: `EventData`

      will be:

      ```
      \security\microsoft_windows_eventlog.sdkkeyvaluefilereader.properties
      ```

   b. To parse the other sections of the event body, such as `UserData`, create a JSON parser file with the following naming convention, in the directory location identified in **Step 1**.

      ```
      \{Normalized Channel}\{Normalized ProviderName}.{Normalized
      SectionName}. jsonparser.properties
      ```

      For example, the key-value parser file name for:

      - Channel: `Security`
      - ProviderName: `Microsoft Windows Event Log`
      - SectionName: `UserData`

      will be:

```
\security\microsoft_windows_eventlog.userdata.jsonparser.properties
```

Note: Normalize the `Channel`, `ProviderName`, and `SectionName` values by changing all letters to lower case, and then replacing each character that is not a letter or digit (including special characters and spaces) with an underscore character (_). Do not normalize the `Locale` and `Encoding` values.

5. Create mappings in these parsers as per your requirements by using conditional mappings based upon the ArcSight `externalId` field, which is already mapped to the Windows Event ID.

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

   a. The following event header key-value parser can be used as a reference for:

   - Channel: `Security`
   - ProviderName: `Microsoft Windows Event Log`
   - SectionName: `EventData`

   to map the event name fields:

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

event.deviceVendor=__getVendor("Microsoft")

conditionalmap.count=1
conditionalmap[0].field=event.externalId
conditionalmap[0].mappings.count=2

# The event logging service has shut down.
conditionalmap[0].mappings[0].values=1100
conditionalmap[0].mappings[0].event.flexString1=
conditionalmap[0].mappings[0].event.name=__stringConstant("The event
logging service has shut down.")

# The security log is now full.
conditionalmap[0].mappings[1].values=1104
conditionalmap[0].mappings[1].event.flexString1=
conditionalmap[0].mappings[1].event.name=__stringConstant("The security
log is now full.")
```

Make sure that no trailing spaces appear in your file after you copy and paste this example.

b. The `UserData` section from following sample JSON parser can be used as a reference:

- Channel: `Security`
- ProviderName: `Microsoft Windows Event Log`
- SectionName: `UserData`

Sample `UserData` section:

```
{
   "UserData": {
      "LogFileCleared":
```

```
         "@xmlns:auto-ns3":
"http://schemas.microsoft.com/win/2004/08/events",
         "@_xmlns_":
http://manifests.microsoft.com/win/2004/08/windows/eventlog",
         "SubjectUserSid": "S-1-5-18",
         "SubjectUserName": "SYSTEM",
         "SubjectDomainName": "NT AUTHORITY",
         "SubjectLogonId": "0x3e7"
         }
      }
}
```

c. The following EventBody JSON parser can be used as a reference:

- Channel: `Security`
- ProviderName: `Microsoft Windows Event Log`
- SectionName: `UserData`

Sample `EventBody` section:

```
trigger.node.location=/UserData
event.deviceVendor=__getVendor("Microsoft")
token.count=7
token[0].name=SubjectUserSid
token[0].location=LogFileCleared/SubjectUserSid
token[0].type=String

token[1].name=SubjectUserName
token[1].location=LogFileCleared/SubjectUserName
token[1].type=String

token[2].name=SubjectDomainName
token[2].location=LogFileCleared/SubjectDomainName
```

```
token[2].type=String

token[3].name=SubjectLogonId
token[3].location=LogFileCleared/SubjectLogonId
token[3].type=String

token[4].name=Reason
token[4].location=AuditEventsDropped/Reason
token[4].type=String

token[5].name=Channel
token[5].location=AutoBackup/Channel
token[5].type=String

token[6].name=BackupPath
token[6].location=AutoBackup/BackupPath
token[6].type=String

conditionalmap.count=1
conditionalmap[0].field=event.externalId
conditionalmap[0].mappings.count=3

conditionalmap[0].mappings[0].values=1101
conditionalmap[0].mappings[0].event.name=__stringConstant("Audit events
have been dropped by the transport. The real time backup file was
corrupt due to improper shutdown.")
conditionalmap[0].mappings[0].event.deviceCustomNumber3=__safeToLong
(Reason)
conditionalmap[0].mappings[0].event.deviceCustomNumber3Label=__
stringConstant("Reason Code")

conditionalmap[0].mappings[1].values=1102
conditionalmap[0].mappings
[1].event.destinationNtDomain=SubjectDomainName
conditionalmap[0].mappings[1].event.destinationUserName=__extractNTUser
(__oneOf(SubjectUserName,SubjectUserSid))
conditionalmap[0].mappings[1].event.destinationUserId=SubjectLogonId
conditionalmap[0].mappings[1].event.name=__stringConstant("The audit log
was cleared.")

conditionalmap[0].mappings[2].values=1105
conditionalmap[0].mappings[2].event.fileType=Channel
conditionalmap[0].mappings[2].event.fileName=BackupPath
conditionalmap[0].mappings[2].event.name=__stringConstant("Event log
automatic backup")
```

Make sure that no trailing spaces appear in your file after you copy and paste this example.

6. Start the connector.

Verify categorization of new events to see if additional categorization are required. For information about categorization, see the Technical Note *ArcSight Categorization: A Technical Perspective* available from the Micro Focus Software Support site. For more information about creating parsers, see the Developer's Guide to FlexConnectors.

Customizing Localization Support for the Native Connector

ArcSight SmartConnectors provide the event collection layer for ArcSight SIEM. Therefore, in the context of SmartConnectors, localization is related to the collection, parsing, and normalization of event messages that are generated by localized events and written in non-English languages. Localization (L10 N) is the process of converting a program to run in a particular locale or country, which includes displaying all the text and translating the user interface into the native language.

To add location support beyond that provided by ArcSight, complete the following these steps.

1. Identify the Channel, ProviderName, locale, and encoding of the event for which you want to localize the event data.
2. Configure the host table parameters with the appropriate locale and encoding parameter values identified in step 1.

   ```
   agents[x].windowshoststable[y].locale=<Locale>
      agents[x].windowshoststable[y].encoding=<Encoding>
   ```

   where x is the index of the connector and y is the index of hosts in the connector configuration.

   Example:

   ```
   agents[0].windowshoststable[0].locale=de_DE
      agents[0].windowshoststable[0].encoding=UTF-8
   ```

3. To add support for locales and encodings not shown in the connector host table configuration selections, change the `Locale` and `Encoding` values of the following lines in the `agent.properties` file (which can be found at `$ARCSIGHT_HOME\current\user\agent`):
4. Enter the type of character set encoding of the events in the log file, for example `event.name`. Create your content relative to this location: `$ARCSIGHT_HOME\user\agent\fcp\winc\`.

5. Identify the parser from which you want to invoke the localization extra-processor map file.

```
$ARCSIGHT_HOME\user\agent\winc\<NormalizedChannel>\
   <NormalizedProviderName>.sdkkeyvaluefilereader.properties
```

Example:

```
$ARCSIGHT_HOME\user\agent\winc\security\
   microsoft_windows_security_auditing.sdkkeyvaluefilereader.properties
```

Note: Normalize the **Channel**, **ProviderName**, and **SectionName** values by changing all letters to lower case, and then replacing each character that is not a letter or digit (including special characters and spaces) with an underscore character (_). Do not normalize the **Locale** and **Encoding** values.

6. For each locale and encoding combination, declare an extra-processor map file within this parser.

```
extraprocessor[4].type=map
extraprocessor
[4].filename=winc/<NormalizedChannel>/<NormalizedProviderName.
   <Locale>.<Encoding>.map.csv
extraprocessor[4].conditionfield=event.oldFileHash
extraprocessor[4].conditiontype=equals
extraprocessor[4].conditionvalues=<Locale>|<Encoding>
extraprocessor[4].charencoding=<Encoding>
extraprocessor[4].allowoverwrite=true
extraprocessor[4].overrideeventmappings=true
extraprocessor[4].clearfieldafterparsing=false
extraprocessor[4].flexagent=false
```

Example:

```
extraprocessor[4].type=map
extraprocessor[4].filename=winc/security/
   microsoft_windows_security_auditing.fr_CA.UTF-8.l10n.map.csv
extraprocessor[4].conditionfield=event.oldFileHash
extraprocessor[4].conditiontype=equals
extraprocessor[4].conditionvalues=fr_CA|UTF-8
extraprocessor[4].charencoding=UTF-8
extraprocessor[4].allowoverwrite=true
extraprocessor[4].overrideeventmappings=true
extraprocessor[4].clearfieldafterparsing=false
extraprocessor[4].flexagent=false
```

7. Create the L10N extra-processor map file:

```
$ARCSIGHT_HOME\user\agent\winc\<NormalizedChannel>\
   <NormalizedProviderName>.<Locale>.<Encoding>.l10n.map.csv
```

Note: When creating, editing, or saving the L10N extra-processor map file, don't use an application with a default of **ASCII**, **UTF-8**, or other generic encoding. Create the file on the localized device or in a localized editor, and be sure that the encoding isn't overwritten when you save it.

Example:

```
$ARCSIGHT_HOME\user\agent\winc\security\
   microsoft_windows_security_auditing.fr_CA.UTF-8.l10n.map.csv
```

Note: Normalize the **Channel**, **ProviderName**, and **SectionName** values by changing all letters to lower case, and then replacing each character that is not a letter or digit (including special characters and spaces) with an underscore character (_). Do not normalize the **Locale** and **Encoding** values.

8. Within this file, declare the getters and setters, and add all the localization content. Use the event.externalId field as the getter, and the field that you want to localize as the setter. A sample file is shown for French:

```
event.externalId,set.event.name
"4886","Les services de certificats ont reçu une demande de certificat."
"4887","Les services de certificats ont approuvé une demande de
certificat et émis un certificat."
"4884","Les services de certificats ont importé un certificat dans sa base
de données."
"4885","Le filtre d'audit des services de certificats modifié."
"4882","Les autorisations de sécurité pour les services de certificats ont
été modifiées."
"4883","Les services de certificats ont récupéré une clé archivée."
"4880","Les services de certificats ont démarré."
"4881","Les services de certificats se sont arrêtés."
...
...
```

Note: Additional mapping can be set from ESM. Go to your ESM Console and run **Get Additional Data**. The command can only collect additional data from supported sources. Unsupported sources collect additional data from the event header.

Troubleshooting

This section has the following information:

Connector stops processing events when a MQ is full

Issue: While the connector is running, it stops processing events and displays the message in the **wincagent.log** file as follows:

Example: `EventLogManager - Collected 0 events, 1112188 total, Eps=0, processing queue=495(99% full), batching queue=1600(100% full), sending queue=25(100% full)`

Workaround: This error might occur when the MQ is full.

To fix this:

1. Stop the connector.
2. Open the `arcsight\Connectors\current\config\agent\agent.default.properties` file.
3. Modify the **mq.enable.space.check=true** parameter value to **false**. By default, this value is set to **true**. The **mq.enable.space.check** parameter is available in ArcSight SmartConnector 8.2.0 or later.
4. Restart the connector.

Parameters not functioning as expected

Issue: The **RenameFileInTheSameDirectory** and **DeleteFile** parameters are not functioning as expected.

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

Log message for resource adjustment

Issue: While the connector is starting, it logs that the temporary store will be downsized.

```
2015-01-26 15:11:17,668][ERROR]
[default.org.apache.activemq.broker.BrokerService]
[external] Temporary Store limit is 51200 mb, whilst the temporary data
```

```
directory: C:\arcsight\SmartConnectors\current\activemq-data\localhost\tmp_
storage only has
47568 mb of usable space - resetting to maximum available 47568 mb.
```

Workaround: This message indicates that the system disk space is low. Although this may not cause an immediate impact, check for adequate disk storage to ensure it does not run out while running the connector. To avoid this log message, make sure the system has 50 GB of disk space available.

A Non-administrator User Is Unable to Run Windows Native Connector and the Log File Has Permission Error

Issue: If any user other than administrator tries to run Windows Native connector, it does not run and the log file shows the following error:

```
[FATAL][default.com.arcsight.agent.am.e][init] Could not initialize the
Obfuscation key manager
[FATAL][default.com.arcsight.agent.am.e][init]
com.arcsight.common.config.n: An error occured in configuration. Unable to
load properties from file ‘<install
path>\current\user\agent\keys\obfuscationkey'.
Error was: ‘<install path>\current\user\agent\keys\obfuscationkey (Access is
denied)'
```

Workaround: This issue occurs because only the administrators are authorized to access `<install path>\current\user\agent\agent.properties` and `<install path>current\user\agent\keys\obfuscationkey` in the SmartConnector 7.15.0 or later.

For a non-administrator user to run this connector, change the **ownership** of the **agent.properties** and **obfuscationkey** files to a corresponding user with the **Full control** permission. If there are more than one users who need permission to run the connector, add these users in the same group so that the **ownership** of the **agent.properties** and **obfuscationkey** files can be assigned to this group.

For information about taking ownership and full control of files, refer to the Microsoft documentation.

Appendix A: Types of Internal Events

The Windows Event Log – Native connector documents the following types of internal events:

Specific Windows Security Event Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

104

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The log file was cleared'
Message	concatenate('The ',Channel,' log file was cleared')
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName
File Type	Channel
File Path	BackupPath

1100

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	‘The event logging service has shut down.’

1101

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	‘Audit events have been dropped by the transport. The real time backup file was corrupt due to improper shutdown.’
Device Custom Number 3	Reason

1102

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	‘The audit log was cleared.’
Destination NT Domain	SubjectDomainName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination User ID	SubjectLogonId

1104

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The security log is now full'

1105

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	‘Event log automatic backup.’
File Type	Channel
File Name	BackupPath

Collector Connected

Field	Description
Event Name	'Collector'
Device Event Category	'/Informational'
Agent Severity	'2'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Disconnected

Field	Description
Event Name	'Collector Disconnected'
Device Event Category	'/Informational/Warning'
Agent Severity	'3'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Down

Field	Description
Event Name	'Collector Down'
Device Event Category	'/Informational/Warning'

Field	Description
Agent Severity	'3'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Configuration Accepted

Collector Status for "Collector Configuration Accepted"

Field	Description
Event Name	'Collector Configuration Accepted'
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Host Status for "Collector Configuration Accepted"

Field	Description
Event Name	'Collector Configuration Accepted'
Device Host Name	<DeviceHostName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or 'Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason

Field	Description
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<Collector Operating System Version>

Event Log Status for “Collector Configuration Accepted”

Field	Description
Event Name	‘Collector Configuration Accepted’
Device Host Name	<DeviceHostName>
Device Custom String 3 Label	‘Event Log’
Device Custom String 3	<ConfiguredEventLogName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	‘/Informational’ or ‘/Informational/Warning’ depending on the reason
Agent Severity	‘2’ or ‘3’ depending on the reason
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<Collector Operating System Version>

Collector Status Updated

Collector Status for “Collector Status Updated”

Field	Description
Event Name	‘Collector Status Updated’
Reason	<SuccessStatus/FailureReason>
Device Event Category	‘/Informational’ or ‘/Informational/Warning’ depending on the reason

Field	Description
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Host Status for "Collector Status Updated"

Field	Description
Event Name	'Collector Status Updated'
Device Host Name	<DeviceHostName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3, depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Event Log Status for "Collector Status Updated"

Field	Description
Event Name	'Collector Status Updated'
Device Host Name	<DeviceHostName>
Device Custom String 3 Label	'Event Log'
Device Custom String 3	<ConfiguredEventLogName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason

Field	Description
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Event Collection Started

Collector Status for "Collector Collection Started"

Field	Description
Event Name	'Collector Collection Started'
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Host Status for "Collector Collection Started"

Field	Description
Event Name	'Collector Collection Started'
Device Host Name	<DeviceHostName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason

Field	Description
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<Collector Operating System Version>

Event Log Status for “Collector Collection Started”

Field	Description
Event Name	‘Collector Collection Started’
Device Host Name	<DeviceHostName>
Device Custom String 3 Label	‘Event Log’
Device Custom String 3	<ConfiguredEventLogName>
Reason	<Event Collection SuccessStatus/FailureReason>
Device Event Category	‘/Informational’ or ‘/Informational/Warning’ depending on the reason
Agent Severity	‘2’ or ‘3’ depending on the reason
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<Collector Operating System Version>

Collector Up

Field	Description
Event Name	‘Collector Up’
Device Event Category	‘/Informational’
Agent Severity	‘2’
Device Custom String 1 Label	‘Collector Host Name’

Field	Description
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<Collector Operating System Version>

Send Documentation Feedback

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

Feedback on Configuration Guide for for Microsoft Windows Event Log - Native SmartConnector (ArcSight 8.3.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!