Standard Content Guide

Microsoft Windows Monitoring 1.0

for ArcSight™ ESM and
ArcSight Express™ with CORR-Engine

June 28, 2012

ArcSight™
An HP Company

Standard Content Guide - Microsoft Windows Monitoring 1.0

Revision History

Date	Product Version	Description
06/28/2012	Microsoft Windows Monitoring 1.0	Final revision for release.

Document template version: 1.0.5

Contact Information

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

Chapter 1

Microsoft Windows Monitoring Overview

This chapter discusses the following topics.

What is Microsoft Windows Monitoring?

Microsoft Windows Monitoring is standard content that provides additional support for monitoring network activity specific to Windows operating systems.

Microsoft Windows Monitoring content provides monitoring and reporting capability for the following use cases:

- **Microsoft Windows Monitoring** provides an overview of events being monitored through the Account Management, Authentication, Policy Changes, and System Services and Auditing use cases.
- **Account Management** monitors and reports additions, modifications, and deletions to user accounts and computer accounts. Special emphasis is given to privileged user accounts.
- **Authentication** monitors login activity and failed authentications, including information such as the number of failed logins per user and host, or attempted authentications against disabled or non-existent accounts.
- **Policy Changes** monitors policy changes and violations, reports changes to domain group and other security policies, and reports group policy violations. For example, Microsoft Windows Monitoring can report an event in which a user attempts to run software that a group policy specifies cannot be run.
- **System Services and Auditing** monitors new and removed system services, and start/stop or disable/enable status of critical services.

Supported Software

Microsoft Windows Monitoring content supports these Windows operating system versions:

- Windows 2008 R2 Server
- Windows 2008 Server
- Windows 7
- Windows Vista
- Windows 2003 R3 Server
- Windows 2003 Server
- Windows XP

For information on the supported SmartConnectors and ESM versions for Microsoft Windows Monitoring content, refer to the *Microsoft Windows Monitoring 1.0 Release Notes*.

Applicable Events

Each Windows use case targets a different set of Windows log events. You can see these events in Chapter 3, Microsoft Windows Monitoring Content, on page 15. In addition, a summary of the Windows log events for each use case is listed in Appendix A, Events by Use Case, on page 51.

Chapter 2

Installation and Configuration

This chapter discusses the following topics.

Preparing for Installation

Before installing the Microsoft Windows Monitoring content, complete these preparation tasks, which are described in the following sections.

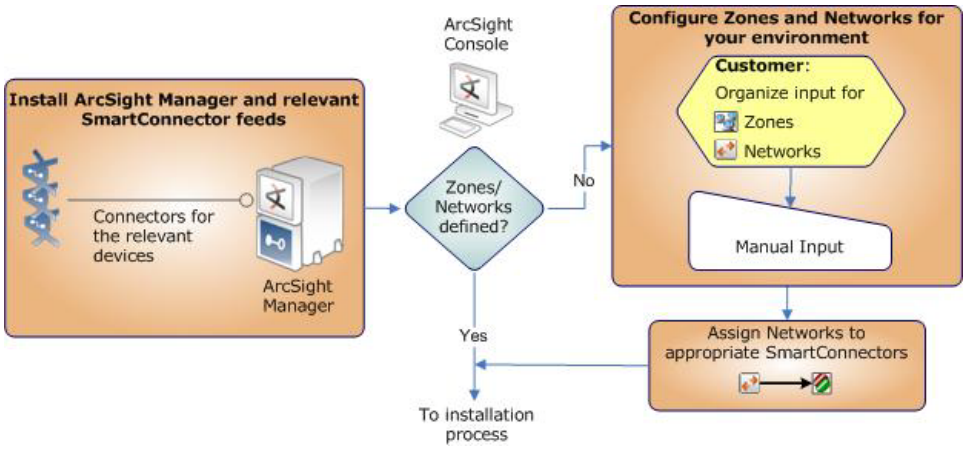
- Prepare your environment
- Verify your environment
- Enable Windows Audit Categories
- Enable parser versioning for field mapping

Preparing Your Environment

Before installing, prepare your environment for the Microsoft Windows Monitoring content.

1. Install and configure the Microsoft Windows Event Log – Unified SmartConnector according to the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Unified*. For details about the supported device versions, refer to the *Microsoft Windows Monitoring 1.0 Release Notes*.
2. *Optional*: Model your network. Learn more about the ArcSight network modeling process in the *ESM 101* guide. Find instructions on how to configure zones and networks in the *ArcSight Console User's Guide* or the ESM online Help.

Figure 2-1 Prepare Your Environment



Verifying Your Environment

Before installing, verify that you have the supported ESM release installed and configured or the supported version of ArcSight Express with CORR-Engine. Refer to the *Microsoft Windows Monitoring 1.0 Release Notes*.

Enabling Windows Audit Categories

On the Windows devices you want to monitor, enable the following Windows audit categories for successful and failed events:

- Audit account logon events
- Audit account management
- Audit logon events
- Audit policy change
- Audit privilege use
- Audit system events

Enabling Parser Versioning for Field Mapping

The Microsoft Windows Monitoring content is designed for parser version 1 of the Microsoft Windows Event Log – Unified SmartConnector. Follow the steps below to enable parser version 1 on the SmartConnector.

The Microsoft Windows Monitoring content only processes events sent by a Microsoft Windows Event Log – Unified SmartConnector with parser version 1 enabled.

To enable parser version 1 on the SmartConnector:

1. From the computer on which the Microsoft Windows Event Log – Unified SmartConnector is installed, open a command window.
2. Browse to the `$ARCSIGHT_HOME\current\bin` directory.
3. Enter the command:

```
arcsight connectorsetup
```

4 When prompted to enter Wizard mode, click **No**.

5 In the **Agents** area of the Configuration Tool window, select the `windowsfg` connector.

6 From the **Options** menu, select **Show Internal Parameters.**

7 In the **Parameters** area, scroll to the `fcp.version` parameter.

8 For Microsoft Windows Monitoring, select **1** as the parser version.

9 Click **OK**.

To learn more about parser versioning and mapping changes in parser version 1 of the Microsoft Windows Event Log – Unified SmartConnector, refer to the document *Security Event Mappings, SmartConnector for Microsoft Windows Event Log - Unified*.

Installing Microsoft Windows Monitoring Content

Follow the procedure below to install the Microsoft Windows Monitoring content package.

To install content package:

1 Download the following content package bundle to the machine where you plan to run the ArcSight Console:

`HP-ArcSight-StandardContent-WindowsMonitoring.1.0.0.<nnnn>.0.arb`

Where `<nnnn>` is the four character build number specified in the *Microsoft Windows Monitoring 1.0 Release Notes*.

Internet Explorer sometimes converts the ARB file to a ZIP file during download. If this occurs, rename the ZIP file back to an ARB file before importing.

2 Log into the ArcSight Console with an account that has administrator privileges.

3 In the Navigator panel, click the **Packages** tab.

4 Click **Import** ( ).

5 In the Open dialog, browse and select the package bundle file, and then select **Open**.

The Progress tab of the Importing Packages dialog shows how the package bundle import is progressing. When the import is complete, the Results tab of the Importing Packages dialog is displayed together with the Packages for Installation dialog.

6 In the Packages for Installation dialog, leave the `Microsoft Windows Monitoring` and `Monitoring Support Data` check boxes selected, and click **Next**.

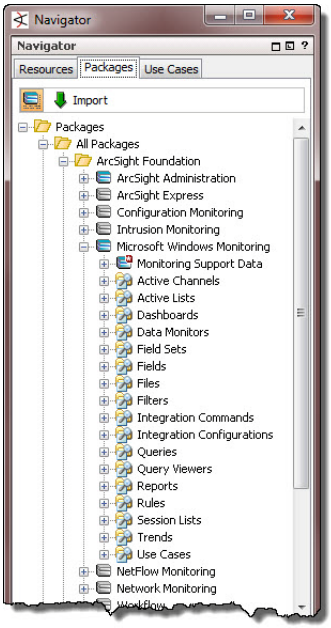
The Installing Packages dialog opens. The Progress tab shows how the installation is progressing. When the installation is complete, the Results tab displays the Summary Report.

7 In the Installing Packages dialog, click **OK**.

8 In the Importing Packages dialog box, click **OK.**

9 On the **Packages** tab of the Navigator panel, expand the `ArcSight Foundation` group to verify that the installation is successful and that the content is accessible in the Navigator panel.

Figure 2-2 Microsoft Windows Monitoring Package



Installation Troubleshooting

If the installation is not successful, refer to the contact information below.

Resource	Description
Support web site	http://support.openview.hp.com provides access to incident reporting, the knowledge base, software downloads, help, and the customer forum.
Protect 724 Community	https://protect724.arcsight.com offers a place for customers to: • Share content, collaborate on best practices, and get feedback • Ask and answer questions • Network with each other • Gain visibility on product roadmaps

Assigning User Permissions

By default, users in the `Default` user group can view the Microsoft Windows Monitoring content, and users in the `ArcSight Administrators` and `Analyzer Administrators` user groups have read and write access to the content. Depending on how you have set up user access controls within your organization, you might need to adjust those controls to make sure the new content is accessible to the right users.

The following procedure assumes that you have user groups set up and users assigned to those groups. In the procedure, assign user permissions to the following resource types:

- Active Channels
- Active Lists
- Dashboards
- Data Monitors
- Field Sets
- Fields
- Files
- Filters
- Integration Commands
- Integration Configuration
- Queries
- Query Viewers
- Reports
- Rules
- Session Lists
- Trends

To assign user permissions:

1. Log into the ArcSight Console with an account that has administrative privileges.
2. For all the resource types listed above, change the user permissions:
   a. In the Navigator panel, go to the resource type and navigate to `ArcSight Foundations/Microsoft Windows Monitoring`.
   b. Right-click the **Microsoft Windows Monitoring** group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.

Configuring Microsoft Windows Monitoring Content

The list below shows the general tasks you need to complete to configure Microsoft Windows Monitoring content with values specific to your environment.

Host Name and Address Consistency

To ensure consistency between host names and addresses, make sure that the system running the Microsoft Windows Event Log – Unified SmartConnector is configured to use the same DNS servers as the Active Directory.

Event data can appear in different formats when the event reaches ESM. For example, the event data might include the host name only or the fully qualified domain name (FQDN). To resolve this format inconsistency, Microsoft Windows Monitoring content uses global variables (such as TargetUser) in reports, rules, and other resources instead of the original field. Be sure to use these global variables when modifying or creating your own content.

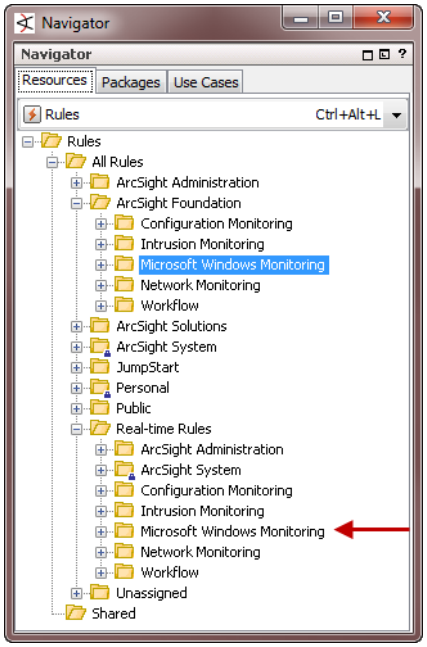
Deploying and Enabling Rules

Rules trigger only if they are deployed in the `Real-time Rules` group and are enabled. Microsoft Windows Monitoring rules are *not* deployed by default in the `Real-time Rules` group and only certain rules are enabled. Follow the procedure below to deploy the rules.

To deploy the Microsoft Windows Monitoring rules:

1. From the Resources tab in the Navigator panel, go to Rules and navigate to the `ArcSight Foundation/Microsoft Windows Monitoring` group.
2. Right-click the `Microsoft Windows Monitoring` group and select **Deploy Real-time Rule(s)**.

A new `Real-time Rules/Microsoft Windows Monitoring` group is created that is a link to the original `ArcSight Foundation/Microsoft Windows Monitoring` group, as shown in the following figure.



To enable a rule:

1. In the Navigator panel, go to Rules and navigate to the `Real-time Rules` group.
2. Navigate to the rule you want to enable.
3. Right-click the rule and select **Enable Rule**.

For a list of the Microsoft Windows Monitoring rules you need to enable, refer to "Account Management" on page 19 and "System Services and Auditing" on page 42.

Configuring Notification Destinations

By default, notifications are disabled in the Microsoft Windows Monitoring content rules. If you want to be notified when some of the rules are triggered, you can configure notification destinations and enable the notification action in the rules.

For details about configuring notification destinations and enabling notifications in rules, refer to the *ArcSight Console User's Guide* or the ESM online Help.

Scheduling Reports

You can run reports on demand, automatically on a regular schedule, or both. Evaluate the reports that come with Microsoft Windows Monitoring, and schedule the reports that are of interest to your organization and business objectives. For instructions about how to schedule reports, refer to the *ArcSight Console User's Guide* or the ESM online Help.

Additional Configuration Tasks

For all use cases, confirm that at least one event source is configured with a connector and is sending events.

Specific configuration for each Microsoft Windows Monitoring use case is described in Chapter 3, Microsoft Windows Monitoring Content, on page 15.

Chapter 3

Microsoft Windows Monitoring Content

The Microsoft Windows Monitoring content provides a series of coordinated resources that monitor and report on system activities pertaining to the Microsoft Windows operating system.

The Microsoft Windows Monitoring resources are grouped together according to use cases, which help address a specific issue or function. The following table lists and describes the use cases.

Use Case	Purpose
"Microsoft Windows Monitoring" on page 16	The Microsoft Windows Monitoring use case includes several resources that provide an overview of events being monitored through the Account Management, Authentication, Policy Changes, and System Services and Auditing use cases.
"Account Management" on page 19	The Account Management use case provides resources that monitor changes to the status of Windows accounts, including accounts that become locked out as a result of multiple login failures, changes to administrator privileges or other access permissions, and creation or disabling of user accounts.
"Authentication" on page 33	The Authentication use case provides resources that monitor login activity in Windows. These resources can provide information such as the number of failed logins per user and host, or attempted authentications against disabled or non-existent accounts. Rules categorize user accounts for which failed authentications occur and enable you to view the authentication failures by category.
"Policy Changes" on page 39	The Policy Changes use case provides resources that monitor changes to policies in your Windows environment, including policies related to password updates, lockouts, and audits.
"System Services and Auditing" on page 42	The System Services and Auditing use case provides resources that monitor Windows activity related to two scenarios: clearing the audit log, and starting or stopping critical operating system services.

Microsoft Windows Monitoring

The Microsoft Windows Monitoring use case includes several resources that provide an overview of events being monitored through the Account Management, Authentication, Policy Changes, and System Services and Auditing use cases.

Resources

The following table lists the information presentation and data processing resources that support the Microsoft Windows Monitoring use case.

Table 3-1 Resources that Support the Microsoft Windows Monitoring Use Case

Resource	Description	Type	URI
Monitor Resources			
Windows Monitoring Events	This live active channel shows events received during the day. It displays all Windows events using the Windows Monitoring field set.	Active Channel	ArcSight Foundation/Microsoft Windows Monitoring/
Windows Monitoring Correlation Events	This active channel shows the correlation events from the Microsoft Windows Monitoring content in the last two hours.	Active Channel	ArcSight Foundation/Microsoft Windows Monitoring/
Windows Monitoring	This dashboard monitors the top Windows users, top Windows event types, and top Windows devices.	Dashboard	ArcSight Foundation/Microsoft Windows Monitoring/
Top Windows Devices by Event Count	This query viewer displays the top Windows devices by event count.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Top Windows Devices by Event Count	This report displays a table showing the top Windows devices by event count. By default, this report runs over the previous day.	Report	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Library Resources			
Top 10 Event Types last Hour	This data monitor displays the top 10 Windows event types in the last hour.	Data Monitor	ArcSight Foundation/Microsoft Windows Monitoring/Windows Monitoring/
Top 10 Windows Users Last Hour	This data monitor displays the top 10 Windows users in the last hour.	Data Monitor	ArcSight Foundation/Microsoft Windows Monitoring/Windows Monitoring/
Target_HostName	This variable displays the Target Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_User	This variable displays the Target User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/

Resource	Description	Type	URI
Target_NTDomain	This variable displays the Target NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_NTDomain	This variable displays the Attacker NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_User	This variable displays the Attacker User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_HostName	This variable displays the Attacker Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_NTDomain	This variable displays the Device NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_HostName	This variable displays the Device Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Windows Monitoring Correlation	This field set is used to display relevant information when investigating Windows correlation events.	Field Set	ArcSight Foundation/Microsoft Windows Monitoring/
Windows Monitoring	This field set is used to display relevant information when investigating Windows events.	Field Set	ArcSight Foundation/Microsoft Windows Monitoring/
Windows Events	This filter is designed to provide only Windows events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/
Target User with Domain Information	This filter is designed for conditional expression variables. It passes events where the target user name contains the Domain information.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
EventID.net	This command can run a search with the external ID and the device event category in the selected event.	Integration Command	ArcSight Foundation/Microsoft Windows Monitoring/
MS - Event Lookup	This configuration is used to configure the EventID.net command. The command can be run on any cell selected in the viewer.	Integration Configuration	ArcSight Foundation/Microsoft Windows Monitoring/
Windows Events by Device Trend	This query selects the device address, device event class ID, and device hostname of Windows events.	Query	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/For Trends/

Resource	Description	Type	URI
Top Windows Devices by Event Count - Trend	This query looks for windows events by Device. It selects the device host name, the device address, and the number of events.	Query	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Windows Events by Event and Device	This trend tracks the number of Windows events by device. It stores the number of Windows events, device address, device event class id, and device host name.	Trend	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Authentication	This use case monitors user logon activity in Windows, focusing on multiple failed logins and logins to disabled and non-existing accounts.	Use Case	ArcSight Foundation/Microsoft Windows Monitoring/
Policy Changes	This use case monitors changes to the audit, password, and account lockout policies in Windows.	Use Case	ArcSight Foundation/Microsoft Windows Monitoring/
System Services and Auditing	This use case monitors the starting and stopping of critical services on Windows systems, changes to system times, and clearing of audit logs.	Use Case	ArcSight Foundation/Microsoft Windows Monitoring/
Account Management	This use case monitors changes to Windows user accounts, including account lockouts and modifications to user and privileged accounts.	Use Case	ArcSight Foundation/Microsoft Windows Monitoring/

Account Management

The Account Management use case provides resources that monitor changes to the status of Windows accounts, including accounts that become locked out as a result of multiple login failures, changes to administrator privileges or other access permissions, and creation or disabling of user accounts.

Applicable Events

The following events apply to this use case.

Windows 2003 family:	**Windows 2008 family:**
• Security:528	• Microsoft-Windows-Security-Auditing:4624
• Security:540	• Microsoft-Windows-Security-Auditing:4720
• Security:624	• Microsoft-Windows-Security-Auditing:4722
• Security:626	• Microsoft-Windows-Security-Auditing:4723
• Security:627	• Microsoft-Windows-Security-Auditing:4724
• Security:628	• Microsoft-Windows-Security-Auditing:4725
• Security:629	• Microsoft-Windows-Security-Auditing:4726
• Security:630	• Microsoft-Windows-Security-Auditing:4728
• Security:632	• Microsoft-Windows-Security-Auditing:4729
• Security:633	• Microsoft-Windows-Security-Auditing:4732
• Security:636	• Microsoft-Windows-Security-Auditing:4733
• Security:637	• Microsoft-Windows-Security-Auditing:4738
• Security:642	• Microsoft-Windows-Security-Auditing:4740
• Security:644	• Microsoft-Windows-Security-Auditing:4741
• Security:645	• Microsoft-Windows-Security-Auditing:4742
• Security:646	• Microsoft-Windows-Security-Auditing:4743
• Security:647	• Microsoft-Windows-Security-Auditing:4756
• Security:660	• Microsoft-Windows-Security-Auditing:4757
• Security:661	• Microsoft-Windows-Security-Auditing:4767
• Security:671	• Microsoft-Windows-Security-Auditing:6279
	• SAM:12294

Configuration Tasks

The Account Management use case requires the following configuration for your environment:

- Configure the following active lists. These active lists are referenced by active channels, filters, rules, reports, and data monitors.
  - Populate the **Privileged Accounts** active list with all the privileged accounts in your environment.

    Use lower case for the User Name and Domain fields.

  - Populate the **Privileged Groups** active list with the group names of all Windows privileged groups.

  For information on how to configure active lists, refer to the *ArcSight Console User's Guide*.

- Enable the following rules:
  - **Account Removed from Privileged Group** detects when user accounts are removed from a privileged group.
  - **Privileged Account Enabled** detects account-enabled events in which the user name is in the Privileged Accounts active list.
  - **Privileged Account Disabled** detects account-disabled events in which the user name is in the Privileged Accounts active list.
  - **Privileged Account Modified** detects account change events in which the user name is in the Privileged Accounts active list.
  - **Account Added to Privileged Group** detects user accounts being added to a privileged group.
  - **Privileged Account Deleted** detects account deleted events in which the user name is in the Privileged Accounts active list.
  - **Privileged Account Locked Out** detects lockout events in privileged accounts.
  - **Privileged Account Password Changed** detects password change events in which the user name is in the Privileged Accounts active list.

  For information about enabling rules, refer to "Deploying and Enabling Rules" on page 12.

- *Optional*: Enable the notification action for the following rules, if appropriate for your organization.
  - **Account Locked Out Multiple Times in 24 Hours**
  - **Privileged Account Locked Out**
  - **Lockout Attempt Failed**
  - **Account Locked Out**

  For information on how to enable notification actions, refer to the *ArcSight Console User's Guide*.

Resources

The following table lists the information presentation and data processing resources that support the Account Management use case.

Table 3-2 Resources that Support the Account Management Use Case

Resource	Description	Type	URI
Monitor Resources			
Account Management	This dashboard shows an overview of Windows account management events. The dashboard displays the User Accounts Created, Deleted, Disabled or Enabled, Windows Account Lockouts, Modified Windows Privileged Accounts, and Privileged Accounts Modified data monitors or query viewers.	Dashboard	ArcSight Foundation/Microsoft Windows Monitoring/
Windows Account Lockouts	This query viewer displays Windows user accounts that have been locked out today.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/
Privileged Accounts Modified - Drilldown	This query viewer is used for drilldown purposes to display detailed information about privileged group member modifications.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Modified Windows Privileged Accounts	This query viewer displays modifications to a Windows privileged account such as enabling or disabling, deleting, or changing the password.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Privileged Accounts Modified	This query viewer displays modifications to a Windows privileged account, such as being added to or removed from a privileged group.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Computer Accounts Deleted Weekly	This report displays a table showing the Windows computer accounts that have been deleted. It also displays a chart showing the number of deleted computer accounts per domain. By default, this report runs over the last 7 days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
User Accounts Deleted Weekly	This report displays a table showing Windows user accounts that have been deleted. It also displays a chart showing the number of deleted user accounts per domain. By default, this report runs over the last 7 days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/

Resource	Description	Type	URI
Daily Accounts Locked Out	This report displays a table showing the Windows user accounts that have been locked out. By default, this report runs over the previous day.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Modified Windows Privileged Group Members	This report displays a table showing additions or removals of users in Windows privileged groups. It also displays a chart showing the number of additions or removals per group.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
User Accounts Enabled Weekly	This report displays a table showing the Windows user accounts that have been enabled. It also displays a chart showing the number of enabled user accounts per domain. By default, this report runs over the last 7 days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Computer Accounts Modified Weekly	This report displays a table showing the Windows computer accounts that have been modified. It also displays a chart showing the number of modified computer accounts per domain. By default, this report runs over the last 7 days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
User Accounts Disabled Weekly	This report displays a table showing the Windows user accounts that have been disabled. It also displays a chart showing the number of disabled user accounts per domain. By default, this report runs over the last 7 days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Modified Windows Privileged Accounts	This report displays a table showing the Windows privileged accounts that have been modified. This table includes any accounts that have been enabled, disabled, deleted, had the password changed, or any other type of modification. It also displays a chart showing the count per change type.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Weekly Accounts Locked Out	This report displays a table showing the Windows user accounts that have been locked out. It also displays a chart showing the number of lockout events per day. By default, this report runs over the last 7 days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/

Resource	Description	Type	URI
Computer Accounts Created Weekly	This report displays a table showing the Windows computer accounts that have been created. It also displays a chart showing the number of created computer accounts per domain. By default, this report runs over the last 7 days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
User Accounts Created Weekly	This report displays a table showing Windows user accounts that have been created. It also displays a chart showing the number of created user accounts per domain. By default, this report runs over the last 7 days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Library - Correlation Resources			
Locked Account Re-enabled	This rule looks for Windows user account logon successful and user account unlocked events. On each event, it will terminate the existing session entry (if any) in the Locked Out Accounts session list. The device and agent severity values are set to Medium.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Lockout Attempt Failed	This rule detects a failure to lock out a Windows account. This event could indicate a possible brute force attack against the default Administrator account. Because this account does not lock out by default, the system event log records SAM event 12294 instead. Investigate even a single occurrence of this event immediately, because this condition can also indicate the presence of an unauthorized operating system. Check the Domain Name field for unknown domains. On each event, a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Computer Account Changed	This rule looks for changes to Windows computer accounts. On every event, the account is added in the Modified Computer Accounts session list, and the device and agent severity values are set to Low.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/

Resource	Description	Type	URI
Account Removed from Privileged Group	This rule looks for Windows user accounts being removed from a privileged group. You can define which groups are considered privileged groups in your environment by editing the Privileged Groups active list. On every event, the user account and group is added to the Privileged Group Members Modified active list and removed from the Privileged Accounts active list, and the device and agent severity values are set to Medium. This rule is disabled by default.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Privileged Account Enabled	This rule looks for Windows account enabled events where the user name is present in the Privileged Accounts active list. On every event, the user account is added to the Privileged Accounts Modified active list, and the device and agent severity values are set to Medium. This rule is disabled by default.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Privileged Account Disabled	This rule looks for Windows account disabled events where the user name is present in the Privileged Accounts active list. On every event, the user account is added to the Privileged Accounts Modified active list, and the device and agent severity values are set to Medium. This rule is disabled by default.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
User Account Deleted	This rule looks for Windows user account deleted events. On every event, the user account is added in the "Deleted User Accounts" session list, terminate the entry in the "Created User Accounts" session list if existing, and the device and agent severity values are set to Low.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Privileged Account Modified	This rule looks for Windows Account Changed events where the user name is present in the Privileged Accounts active list. On every event, the user account is added to the Privileged Accounts Modified active list, and the device and agent severity values are set to Medium. This rule is disabled by default.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/

Resource	Description	Type	URI
Account Added to Privileged Group	This rule looks for Windows user accounts being added to a privileged group. You can define which groups are considered privileged groups in your environment by editing the Privileged Groups active list. On every event, the user account and group are added to the Privileged Group Members Modified and Privileged Accounts active lists, and the device and agent severity values are set to Medium. This rule is disabled by default.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Computer Account Deleted	This rule looks for Windows computer account deleted events. On every event, the account is added in the Deleted Computer Accounts session list, and the device and agent severity values are set to Low.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
User Account Enabled	This rule looks for Windows user account enabled events. On every event, the user account is added in the Enabled User Accounts session list, and the device and agent severity values are set to Low.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
User Account Disabled	This rule looks for Windows user account disabled events. On every event, the user account is added to the Disabled User Accounts session list, and the device and agent severity values are set to Low.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Computer Account Created	This rule looks for Windows computer account creation events. On every event, the account is added in the Created Computer Accounts session list, and the device and agent severity values are set to Low.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
Privileged Account Deleted	This rule looks for Windows account deleted events where the user name is present in the Privileged Accounts active list. On every event, the user account is added to the Privileged Accounts Modified active list and removed from the Privileged Accounts active list. The device and agent severity values are set to Medium. This rule is disabled by default.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/

Resource	Description	Type	URI
Account Locked Out	This rule looks for Microsoft Windows user account locked out events. On each event, the user account is added to the Accounts Locked Out Multiple Times in 24 Hours session list, the device and agent severity values are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled. If the user account is already in the session list, the Locked Count is incremented. The account is also added to the Locked Out Accounts session list for historical purposes.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Privileged Account Locked Out	This rule looks for Windows privileged account lockout events. It uses the Privileged Accounts active list to determine which users have special privileges. On each event, a notification is sent to the SOC Operators team (by default, the notification is disabled) and the device and agent severity values are set to High. This rule is disabled by default.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
User Account Created	This rule looks for Windows user account creation events. On every event, the user account is added to the Created User Accounts session list, and the device and agent severity values are set to Low.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Privileged Account Password Changed	This rule looks for Windows Password Changed events where the user name is present in the Privileged Accounts active list. On every event, the user account is added to the Privileged Accounts Modified active list, and the device and agent severity values are set to Medium. This rule is disabled by default.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Account Locked Out Multiple Times in 24 Hours	This rule looks for Windows user accounts that have been locked out multiple times in 24 hours using the Accounts Locked Out Multiple Times in 24 Hours session list where the Locked Count is greater than 1. On each event, a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Library Resources			

Resource	Description	Type	URI
Privileged Accounts Modified	This active list stores the target account name, target domain, caller user name, caller domain, and the event name (type of modification) when a Windows privileged account is modified. The TTL is set to 7 days by default.	Active List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Privileged Accounts	This active list stores all privileged accounts in the environment as defined by the user.	Active List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Privileged Group Members Modified	This active list stores the account name, group name, target IP address, target zone, target host name, caller user name, caller domain, and the category behavior (type of modification) when a Windows user account is added or removed from a privileged group. The TTL is set to 7 days by default.	Active List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Privileged Groups	This active list stores the group name of all the Windows privileged groups. It needs to be configured to correspond to the privileged groups in your environment. By default, the entries in this list do not expire. Once this active list is populated, the following rules should be enabled: Account Added to Privileged Group Account Removed from Privileged Group Privileged Account Deleted Privileged Account Disabled Privileged Account Enabled Privileged Account Modified Privileged Account Password Changed	Active List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
User Accounts Created, Deleted, Disabled, or Enabled	This data monitor displays the last 20 created, deleted, disabled, or enabled events for a Windows user account. It shows the affected user name, the affected user's domain, the caller user name, the caller user's domain, and the event name. Caller user name is mapped to attacker user name. Caller domain is mapped to attacker domain.	Data Monitor	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/

Resource	Description	Type	URI
admin	This destination is pre-defined for SOX operators. Customize this destination for your environment; for example, specify an email address.	Destination	SOC Operators/Level 1
Target_HostName	This variable displays the Target Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_User	This variable displays the Target User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_NTDomain	This variable displays the Target NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_NTDomain	This variable displays the Attacker NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_User	This variable displays the Attacker User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_HostName	This variable displays the Attacker Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_NTDomain	This variable displays the Device NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_HostName	This variable displays the Device Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Privileged Account	This field set is used to display relevant information when a privileged account is created, deleted, disabled, or enabled.	Field Set	ArcSight Foundation/Microsoft Windows Monitoring/
User Accounts Created, Deleted, Disabled, or Enabled	This filter provides only created, deleted, disabled, or enabled events for Windows user accounts.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/
LockedCount is NULL	This filter is designed for conditional expression variables. It passes events where the LockedCount is NULL. LockedCount is a variable used in the Account Locked Out rule and will retrieve the number of times a Windows account has been locked out from the Accounts Locked Out Multiple Times in 24 Hours session list.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
Windows Events	This filter is designed to provide only Windows events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/

Resource	Description	Type	URI
Target User with Domain Information	This filter is designed for conditional expression variables. It passes events where the target user name contains the Domain information.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
User Accounts Deleted Weekly - Table	This query looks for Windows user accounts that have been deleted. It selects the deleted account name, deleted account domain, deleted account target host, subject account name, subject account domain, and the time the account was deleted.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Weekly Account Lockouts - Chart	This query looks for account lockouts over the last 7 days. It selects the day the lockout occurred and the number of lockouts that occurred each day.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
User Accounts Created Weekly - Chart	This query looks for Windows user accounts that have been created. It selects the domain and the number of created accounts.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
User Accounts Deleted Weekly - Chart	This query looks for Windows user accounts that have been deleted. It selects the domain and the number of deleted accounts.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Computer Accounts Created Weekly - Table	This query looks for Windows computer accounts that have been created. It selects the new account name, new account domain, new account host, subject account name, subject account domain, and the time the account was created.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
Modified Windows Privileged Group Members - Table	This query selects the group name, user name, caller user name, caller domain, and category behavior.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
User Accounts Created Weekly - Table	This query looks for Windows user accounts that have been created. It selects the new account name, new account domain, new account target host, subject account name, subject account domain, and the time the account was created.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Computer Accounts Deleted Weekly - Chart	This query looks for Windows computer accounts that have been deleted. It selects the domain and the number of deleted accounts.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/

Resource	Description	Type	URI
User Accounts Enabled Weekly - Chart	This query looks for Windows user accounts that have been enabled. It selects the domain and the number of enabled accounts.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Daily Account Lockouts	This query looks for account lockouts over the previous day. It selects the user name, the hostname, the user's domain, and the timestamp for the lockout occurred, and queries against the Locked Out Accounts session list.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Modified Privileged Accounts - Table	This query selects the target account name, target domain, caller user, caller domain, event name, and count.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
User Accounts Disabled Weekly - Chart	This query looks for Windows user accounts that have been disabled. It selects the domain and the number of disabled accounts.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Computer Accounts Created Weekly - Chart	This query looks for Windows computer accounts that have been created. It selects the domain and the number of created accounts.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
Computer Accounts Modified Weekly - Chart	This query looks for Windows computer accounts that have been modified. It selects the domain and the number of domain.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
User Accounts Disabled Weekly - Table	This query looks for Windows user accounts that have been disabled. It selects the disabled account name, disabled account domain, disabled account target host, subject account name, subject account domain, and the time the account was disabled.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
User Accounts Enabled Weekly - Table	This query looks for Windows user accounts that have been enabled. It selects the enabled account name, enabled account domain, enabled account target host, subject account name, subject account domain, and the time the account was enabled.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/

Resource	Description	Type	URI
Computer Accounts Deleted Weekly - Table	This query looks for Windows computer accounts that have been deleted. It selects the deleted account name, NT domain controller, deleted account domain, subject account name, subject account domain, and the time the account was deleted.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
Weekly Account Lockouts - Table	This query looks for account lockouts over the last 7 days. It selects the user name, the hostname, the user's domain, the timestamp, and the day that the lockout occurred.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Computer Accounts Modified Weekly - Table	This query looks for Windows computer accounts that have been modified. It selects the modified account name, modified account domain, NT domain controller, subject account name, subject account domain, and the time the account was modified.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
Modified Windows Privileged Group Members - Chart	This query selects the group name, category behavior, and the number of membership changes.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Modified Privileged Accounts - Chart	This query selects the name (type of change) and the count.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Deleted User Accounts	This session list stores the deleted account name, deleted account domain, delete account target host, subject account name, and subject account domain when a Windows user account is deleted.	Session List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Created Computer Accounts	This session list stores the new account name, new account domain, new account host, subject account name, and subject account domain when a Windows computer account is created.	Session List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
Enabled User Accounts	This session list stores the enabled account name, enabled account domain, enabled account target host, subject account name, and subject account domain when a Windows user account is enabled.	Session List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/

Resource	Description	Type	URI
Modified Computer Accounts	This session list stores the modified account name, modified account domain, NT Domain Controller, subject account name, and subject account domain when a Windows computer account is modified.	Session List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
Locked Out Accounts	This session list stores the user name, domain, and host information when a Windows account has been locked out. The Account Locked Out rule will add user accounts to the list for historical tracking and reporting purposes. The Locked Account Re-enabled rule will terminate the session entry.	Session List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Created User Accounts	This session list stores the new account name, new account domain, new account target host, subject account name, and subject account domain when a Windows user account is created.	Session List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Accounts Locked Out Multiple Times in 24 Hours	This session list stores the user name, target host, domain, and number of times a Windows account was locked out in last 24 hours. By default, the entry will expire in one day.	Session List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Disabled User Accounts	This session list stores the disabled account name, disabled account domain, disabled account target host, subject account name, and subject account domain when a Windows user account is disabled.	Session List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Deleted Computer Accounts	This session list stores the deleted account name, NT domain controller, deleted account domain, subject account name, and subject account domain when a Windows computer account is deleted.	Session List	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/

Authentication

The Authentication use case provides resources that monitor login activity in Windows. These resources can provide information such as the number of failed logins per user and host, or attempted authentications against disabled or non-existent accounts. Rules categorize user accounts for which failed authentications occur and enable you to view the authentication failures by category.

Applicable Events

The following events apply to this use case.

Windows 2003 family:

- Security:529
- Security:530
- Security:531
- Security:532
- Security:533
- Security:534
- Security:535
- Security:536
- Security:537
- Security:539
- Security:672
- Security:673
- Security:675
- Security:676
- Security:677
- Security:680
- Security:681

Windows 2008 family:

- Microsoft-Windows-Security-Auditing:4625
- Microsoft-Windows-Security-Auditing:4768
- Microsoft-Windows-Security-Auditing:4769
- Microsoft-Windows-Security-Auditing:4771
- Microsoft-Windows-Security-Auditing:4772
- Microsoft-Windows-Security-Auditing:4773
- Microsoft-Windows-Security-Auditing:4776

Configuration Tasks

Optional: Enable the notification action for the following rules, if appropriate for your organization.

- **Failed Authentication - Windows Domain Account**
- **Authentication Attempted to Non-Existing Account**
- **Authentication Attempted to Disabled Account**
- **Failed Authentication - Windows Workstation**

For information on how to enable notification actions, refer to the *ArcSight Console User's Guide*.

Resources

The following table lists the information presentation and data processing resources that support the Authentication use case.

Table 3-3 Resources that Support the Authentication Use Case

Resource	Description	Type	URI
Monitor Resources			
Windows Failed Authentications - All	This live channel shows events received during the last day. It displays all failed Windows authentication events using the Failed Authentications field set.	Active Channel	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Windows Failed Authentications - Domain Accounts	This live channel shows events received during the last day. It displays Windows domain account failed authentication events using the Failed Authentications field set.	Active Channel	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Windows Failed Authentications - Workstations	This live channel shows events received during the last day. It displays Windows workstation failed authentication events using the Failed Authentications field set.	Active Channel	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Authentication Failed	This dashboard shows an overview of Windows account authentication failure. The dashboard displays the Weekly Hosts With Multiple Failed Authentications, Weekly Users With Multiple Failed Authentications, Weekly User With Multiple Failed Authentications by Reason, and Weekly Users With Multiple Failed Authentications Detail query viewer.	Dashboard	ArcSight Foundation/Microsoft Windows Monitoring/
Weekly Hosts With Multiple Failed Authentications	This query viewer displays the number of failed authentications by IP address.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Weekly Users With Multiple Failed Authentications	This query viewer displays the number of failed authentications by user name.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/

Resource	Description	Type	URI
Weekly Users With Multiple Failed Authentications Detail	This query viewer displays the user name with multiple failed authentications in detail. It shows the target user name, target domain, target IP address, target zone name, failure reason, and number of time failure.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Weekly Users With Multiple Failed Authentications by Reason	This query viewer displays the number of failed authentications by reason.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Weekly Hosts With Multiple Failed Authentications	This report displays a table showing Windows hosts with multiple failed authentication attempts. It also displays a chart showing the top 10 hosts with failed authentication attempts by zone name. By default, this report runs over the last 7 days and the threshold is 5 failures.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Weekly Users With Multiple Failed Authentications	This report displays a table showing Windows users with multiple failed authentication attempts. It also displays a chart showing the number of failed attempts by user name. By default, this report runs over the last 7 days, and the threshold is 5 failures.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Library - Correlation Resources			
Failed Authentication - Windows Domain Account	This rule looks for failed authentication attempts to Windows domain accounts. On every event, the device and agent severity values are set to Medium, the event is added to the Failed Authentications session list, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Authentication Attempted to Non-Existing Account	This rule looks for authentication attempts to non-existent Windows user accounts. On every event, the device and agent severity values are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/

Resource	Description	Type	URI
Authentication Attempted to Disabled Account	This rule looks for authentication attempts to disabled Windows user accounts. On every event, the device and agent severity values are set to Medium and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Failed Authentication - Windows Workstation	This rule looks for failed authentication attempts to Windows workstations. On every event, the device and agent severity values are set to Medium, the event is added to the Failed Authentications session list, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Library Resources			
Logon Types	This active list stores a mapping from encoded logon types to their string equivalents. This list is pre-populated and the entries never expire by default.	Active List	ArcSight Foundation/Microsoft Windows Monitoring/Authentication
admin	This destination is pre-defined for SOX operators. Customize this destination for your environment; for example, specify an email address.	Destination	SOC Operators/Level 1
Target_HostName	This variable displays the Target Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_User	This variable displays the Target User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_NTDomain	This variable displays the Target NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_NTDomain	This variable displays the Attacker NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_User	This variable displays the Attacker User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_Host Name	This variable displays the Attacker Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_NTDomain	This variable displays the Device NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/

Resource	Description	Type	URI
Device_HostName	This variable displays the Device Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Failed Authentications	This field set is used to display relevant information when investigating Windows failed authentication events.	Field Set	ArcSight Foundation/Microsoft Windows Monitoring/
WindowsLogonTypes.csv	This file provides the initial data for the Logon Types active list, which is part of the Microsoft Windows Monitoring/Authentication resources.	File	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Failed Authentication Events - All	This filter is designed to provide only Windows failed authentication events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Failed Authentication Events - Workstation	This filter is designed to provide only Windows workstation failed authentication events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Windows Events	This filter is designed to provide only Windows events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/
Failed Authentication Events - Domain	This filter is designed to provide only Windows domain account failed authentication events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Target User with Domain Information	This filter is designed for conditional expression variables. It passes events where the target user name contains the Domain information.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
Weekly Users With Multiple Failed Authentications by Reason - Chart	This query looks for Windows failed authentications. It selects the number of failures and the reason for the failures. By default, the threshold is set to 5 failures.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Weekly Users With Multiple Failed Authentications - Chart	This query looks for Windows failed authentications. It selects the target user name and the number of failures. By default, the threshold is set to 5 failures.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Weekly Users With Multiple Failed Authentications-Table	This query looks for Windows users with multiple failed authentications. It selects the user name, domain, IP address, zone, failure reason, and the number of failures. By default, the threshold is set to 5 failures.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/

Resource	Description	Type	URI
Weekly Hosts With Multiple Failed Authentications-Table	This query looks for Windows hosts with multiple failed authentications. It selects the IP address, zone, reason, and number of failures. By default, the threshold is set to 5.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Weekly Hosts With Multiple Failed Authentications - Chart	This query looks for Windows hosts with multiple failed authentications. It selects the IP address, zone, and number of failures. By default, the threshold is set to 5 failures.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Failed Authentications	This session list stores information about failed Windows authentications, including the user and host information, failure reason, message, and logon type.	Session List	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/

Policy Changes

The Policy Changes use case provides resources that monitor changes to policies in your Windows environment, including policies related to password updates, lockouts, and audits.

Applicable Events

The following events apply to this use case.

Windows 2003 family:	Windows 2008 family:
• Security:612	• Microsoft-Windows-Security-Auditing:4719
• Security:643	• Microsoft-Windows-Security-Auditing:4739

Configuration Tasks

Optional: Enable the notification action for the following rules, if appropriate for your organization.

- **System Audit Policy Changed**
- **Lockout Policy Changed**
- **Password Policy Changed**

For information on how to enable notification actions, refer to the *ArcSight Console User's Guide*.

Resources

The following table lists the information presentation and data processing resources that support the Policy Changes use case.

Table 3-4 Resources that Support the Policy Changes Use Case

Resource	Description	Type	URI
Monitor Resources			
Policy Changes	This dashboard shows an overview of Windows policy change events. The dashboard displays the Policy Changes data monitor.	Dashboard	ArcSight Foundation/Microsoft Windows Monitoring/
Weekly Policy Changes by Type	This report displays a table showing Windows policy changes. It also displays a chart showing the number of changes per policy type, by domain. By default, this report runs over the last 7 days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Policy Changes/
Library - Correlation Resources			

Resource	Description	Type	URI
System Audit Policy Changed	This rule looks for modifications to the Windows system audit policy. On each event, agent and device severities are set to Medium, the change is added to the Policy Changes session list, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Policy Changes/
Lockout Policy Changed	This rule looks for modifications to the Windows lockout policy. On each event, agent and device severities are set to Medium, the change is added to the Policy Changes session list, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Policy Changes/
Password Policy Changed	This rule looks for modifications to the Windows password policy. On each event, agent and device severities are set to Medium, the change is added to the Policy Changes session list, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/Policy Changes/
Library Resources			
Policy Changes	This data monitor displays the last 10 Windows policy change events. It shows the type of policy that was changed and the affected domain.	Data Monitor	ArcSight Foundation/Microsoft Windows Monitoring/Policy Changes/
admin	This destination is pre-defined for SOX operators. Customize this destination for your environment; for example, specify an email address.	Destination	SOC Operators/Level 1
Target_HostName	This variable displays the Target Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_User	This variable displays the Target User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_NTDomain	This variable displays the Target NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_NTDomain	This variable displays the Attacker NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_User	This variable displays the Attacker User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/

Resource	Description	Type	URI
Attacker_Host Name	This variable displays the Attacker Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_NTDomain	This variable displays the Device NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_HostName	This variable displays the Device Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Policy Changes	This filter is designed to provide only correlation events resulting from changes to Windows policies.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Policy Changes/
Windows Events	This filter is designed to provide only Windows events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/
Target User with Domain Information	This filter is designed for conditional expression variables. It passes events where the target user name contains the Domain information.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
Weekly Policy Changes	This query looks for Windows policy changes. It selects the policy, domain, host name, timestamp, attributes changed, and the number of changes.	Query	ArcSight Foundation/Microsoft Windows Monitoring/Policy Changes/
Policy Changes	This session list stores Windows policy change information. This list is populated by rules in the Microsoft Windows MonitoringPolicy Changes group.	Session List	ArcSight Foundation/Microsoft Windows Monitoring/Policy Changes/

System Services and Auditing

The System Services and Auditing use case provides resources that monitor Windows activity related to two scenarios: clearing the audit log, and starting or stopping critical operating system services.

Applicable Events

The following events apply to this use case.

Windows 2003 family:	Windows 2008 family:
• Security:512	• Microsoft-Windows-Eventlog:1102
• Security:516	• Microsoft-Windows-Security-Auditing:4608
• Security:517	• Microsoft-Windows-Security-Auditing:4612
• Security:520	• Microsoft-Windows-Security-Auditing:4616
• Security:521	• Microsoft-Windows-Security-Auditing:4617
• Security:601	• Microsoft-Windows-Security-Auditing:4697
	• Microsoft-Windows-Security-Auditing:4906
	• Service Control Manager:7035
	• Service Control Manager:7036

Configuration Tasks

The System Services and Auditing use case requires the following configuration for your environment:

- Populate the **Critical Services** active list with the names of Windows services that you consider critical in your environment. For information on how to configure active lists, refer to the *ArcSight Console User's Guide*.
- Configure the **Critical Services** filter with the names of the critical Windows services that require alerts when those services are started or stopped.
- Enable the following rules:
  - **Critical Service Stopped** detects critical Windows services that have stopped, based on the information stored in the Critical Services active list.
  - **Critical Service Started** detects critical Windows services that have started, based on the information stored in the Critical Services active list.
  - **Critical Service Request Start** detects requests for critical Windows services to start.
  - **Critical Service Request Stop** detects requests for critical Windows services to stop.

  For general information about rules, refer to "Deploying and Enabling Rules" on page 12.
- *Optional*: Enable the notification action for the following rules, if appropriate for your organization.
  - **Critical Service Stopped**
  - **Critical Service Started**
  - **Critical Service Request Start**
  - **Critical Service Request Stop**

- **Windows System Time Changed**
- **Windows Security Audit Log Cleared**
- **Windows Audit Events Discarded**
- **Windows System Starting**
- **CrashOnAuditFail Modified**
- **Install Service Attempt**
- **Unable to Log Events**

For information on how to enable notification actions, refer to the *ArcSight Console User's Guide*.

Resources

The following table lists the information presentation and data processing resources that support the System Services and Auditing use case.

Table 3-5 Resources that Support the System Services and Auditing Use Case

Resource	Description	Type	URI
Monitor Resources			
System Services and Auditing	This dashboard shows an overview of Windows critical services and auditing violation events. The dashboard displays the Windows System Services and Auditing Violations and the Critical Services Started or Stopped information.	Dashboard	ArcSight Foundation/Microsoft Windows Monitoring/
Critical Services Started or Stopped	This query viewer displays critical Windows services that have been started or stopped in the last day.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Windows System Time Changes	This report displays a table showing Windows system time-changed events. It also displays a chart showing the number of times the system time was changed per domain. By default, this report runs over the last 7 days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Windows Critical Services Started Or Stopped	This report displays a table showing critical Windows services that have started or stopped. It also displays a chart showing the top 10 start or stop events per service. By default, this report runs over the previous day.	Report	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/

Resource	Description	Type	URI
Windows Security Audit Logs Cleared	This report displays a table showing Windows audit log cleared events. It also displays a chart showing the number of times the audit logs were cleared per domain. By default, this report runs over the previous day.	Report	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Library - Correlation Resources			
Windows Audit Events Discarded	This rule looks for Windows audit events being discarded. On the first event, the device and agent severity values are set to High, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Windows System Starting	This rule looks for Windows hosts starting up. Its primary purpose is to add host information to the Windows - Systems Starting Up active list, which is then used to reduce false positives in the Policy Changes rules. (Many policy change events are generated by Windows when systems are starting.) On every event, the agent and device severity values are set to Low, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Windows System Time Changed	This rule looks for Windows system time change events. On every event, the device and agent severities are set to Medium, the user name, host name, NT domain, previous times, new times, and changed times are added to the System Time Changes active list, and a notification is sent to the SOC Operators team. By default, the notification is disabled. This rule is not designed to be activated on NTP time changes.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/

Resource	Description	Type	URI
Critical Service Request Start	This rule looks for critical Windows services sent a start control. You can define which services are considered critical in your environment by editing the Critical Services active list or filter. On every event, the service, host, and user information is added to the "Critical Services Started or Stopped" active list, the device and agent severities are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled. This rule requires collecting the Service Control Manager logs. By default, this rule is not enabled. This rule should be enabled when the Critical Services active list is populated.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Unable to Log Events	This rule looks for events that indicate Windows is unable to write events to the security event log. If this behavior is detected on a high-value computer, investigate immediately. On the first event, the agent and device severity values are set to High and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Critical Service Stopped	This rule looks for critical Windows services stopping. You can define which services are considered critical in your environment by editing the Critical Services active list or filter. On every event, the service, host, and user information are added to the Critical Services Started or Stopped active list, the device and agent severity values are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled. This rule requires collecting the Service Control Manager logs. By default, this rule is not enabled. This rule should be enabled when the Critical Services active list is populated.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/

Resource	Description	Type	URI
Install Service Attempt	This rule looks for the installation of services which should be a rare event and not an everyday action. You should investigate all successes and failures for this event. On every event, the agent and device severities are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
CrashOnAuditFail Modified	This rule looks for changes to the Windows 2008 family CrashOnAuditFail setting. On every event, the agent and device severity values are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled. This setting controls whether the host will shut down if it fails to write audit logs.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Windows Security Audit Log Cleared	This rule looks for Windows audit logs being cleared. On every event, the device and agent severity values are set to Medium, the user and host information are added to the Audit Logs Cleared active list, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Critical Service Request Stop	This rule looks for critical Windows services sent a stop control. You can define which services are considered critical in your environment by editing the Critical Services active list or filter. On every event, the service, host, and user information is added to the "Critical Services Started or Stopped" active list, the device and agent severities are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled. This rule requires collecting the Service Control Manager logs. By default, this rule is not enabled. This rule should be enabled when the Critical Services active list is populated.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/

Resource	Description	Type	URI
Critical Service Started	This rule looks for critical Windows services starting. You can define which services are considered critical in your environment by editing the Critical Services active list or filter. On every event, the service, host, and user information is added to the Critical Services Started or Stopped active list, the device and agent severities are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled. This rule requires collecting the Service Control Manager logs. By default, this rule is not enabled. This rule should be enabled when the Critical Services active list is populated.	Rule	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Library Resources			
System Time Changes	This active list stores the user name, NT domain, host name, previous time, new times, and changed time when a Windows host's system time changes. By default, the TTL is 7 days.	Active List	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Critical Services Started or Stopped	This active list stores the user name, domain, host, and service information when a critical Windows system service is started or stopped. By default, the TTL is 1 day.	Active List	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Windows - Systems Starting Up	This active list stores Windows systems that are starting up. It is used to reduce false positives in the System Audit Policy Changed rule, because many policy change events are generated by Windows when systems are starting. By default, the TTL is 10 minutes.	Active List	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/

Resource	Description	Type	URI
Critical Services	This active list stores the service name for critical Windows services that require alerting upon starting or stopping. It needs to be configured to correspond to the critical Windows services in your environment. The service name stored in this list must match the Service Control Manager:7035 or Service Control Manager:7036 events from your Windows System logs (the service name in the list must match the Target service name field of the base event). Once you populate this list with the services that are critical for your environment, enable the following rules: Critical Service Request Start Critical Service Request Stop Critical Service Stopped Critical Service Started.	Active List	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Audit Logs Cleared	This active list stores the user name, domain, host name, and timestamp when a Windows audit log is cleared. By default, the TTL is 1 day.	Active List	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Windows System Services and Auditing Violations	This data monitor displays the last 20 Windows events related to audit violations. It shows the priority, user name, domain, host name, end time, and the event name.	Data Monitor	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
admin	This destination is pre-defined for SOX operators. Customize this destination for your environment; for example, specify an email address.	Destination	SOC Operators/Level 1
Target_HostName	This variable displays the Target Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_User	This variable displays the Target User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_NTDomain	This variable displays the Target NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_NTDomain	This variable displays the Attacker NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_User	This variable displays the Attacker User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/

Resource	Description	Type	URI
Attacker_Host Name	This variable displays the Attacker Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_NTDomain	This variable displays the Device NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_HostName	This variable displays the Device Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
CrashOnAuditFail is True	This filter is designed for a conditional evaluation, and returns only events where the Windows CrashOnAuditFail value is set to true. It is used in a conditional variable by the CrashOnAuditFail Modified rule. This filter is applicable only to Windows 2008 family events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Audit Log Cleared - pre-Win2k8	This filter is designed to provide only Windows audit log cleared events. Specifically, it is filtering for classic Windows 2003 family events, and is used in a conditional variable by the Windows Security Audit Log Cleared rule.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
System Services and Auditing Violations	This filter is designed to provide only correlation events resulting from changes to Windows system services or auditing violations.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Service Stopped Action Count is NULL	This filter is designed for conditional expression variables. It checks the Action Count value in the "Critical Services Started or Stopped" active list for Service Stopped is NULL.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
Windows Events	This filter is designed to provide only Windows events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/
Critical Services	This filter stores the service name for critical Windows services that require alerting upon starting or stopping. It needs to be configured to correspond to the critical Windows services in your environment.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Target User with Domain Information	This filter is designed for conditional expression variables. It passes events where the target user name contains the Domain information.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/

Resource	Description	Type	URI
Service Started Action Count is NULL	This filter is designed for conditional expression variables. It checks the Action Count value in the "Critical Services Started or Stopped" active list for Service Started is NULL.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
Critical Services Started or Stopped - Table	This query looks for critical Windows services starting or stopping. It selects the service, user, and host information related to the service starting or stopping.	Query	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
System Time Changes - Table	This query looks for Windows system time-changed events. It selects the user name, NT domain, host name, new system time, previous system time, and the time at which the system time was changed.	Query	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Audit Logs Cleared - Chart	This query looks for Windows audit log cleared events. It selects the domain and the number of times the logs were cleared.	Query	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
System Time Changes - Chart	This query looks for Windows system time-changed events. It selects the NT domain, host name, and the number of times the time was changed.	Query	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Audit Logs Cleared - Table	This query looks for Windows audit log cleared events. It selects the user, domain, host, and time that the log was cleared.	Query	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Critical Services Started or Stopped - Chart	This query looks for critical Windows services starting or stopping. It selects the service name and the number of times the service was started or stopped.	Query	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/

Appendix A

Events by Use Case

The following table outlines the events used by each use case in the Microsoft Windows Monitoring content.

Account Management

Windows 2003 family:	Windows 2008 family:
• Security:528	• Microsoft-Windows-Security-Auditing:4624
• Security:540	• Microsoft-Windows-Security-Auditing:4720
• Security:624	• Microsoft-Windows-Security-Auditing:4722
• Security:626	• Microsoft-Windows-Security-Auditing:4723
• Security:627	• Microsoft-Windows-Security-Auditing:4724
• Security:628	• Microsoft-Windows-Security-Auditing:4725
• Security:629	• Microsoft-Windows-Security-Auditing:4726
• Security:630	• Microsoft-Windows-Security-Auditing:4728
• Security:632	• Microsoft-Windows-Security-Auditing:4729
• Security:633	• Microsoft-Windows-Security-Auditing:4732
• Security:636	• Microsoft-Windows-Security-Auditing:4733
• Security:637	• Microsoft-Windows-Security-Auditing:4738
• Security:642	• Microsoft-Windows-Security-Auditing:4740
• Security:644	• Microsoft-Windows-Security-Auditing:4741
• Security:645	• Microsoft-Windows-Security-Auditing:4742
• Security:646	• Microsoft-Windows-Security-Auditing:4743
• Security:647	• Microsoft-Windows-Security-Auditing:4756
• Security:660	• Microsoft-Windows-Security-Auditing:4757
• Security:661	• Microsoft-Windows-Security-Auditing:4767
• Security:671	• Microsoft-Windows-Security-Auditing:6279
	• SAM:12294

Authentication

Windows 2003 family:	Windows 2008 family:
• Security:529 • Security:530 • Security:531 • Security:532 • Security:533 • Security:534 • Security:535 • Security:536 • Security:537 • Security:539 • Security:672 • Security:673 • Security:675 • Security:676 • Security:677 • Security:680 • Security:681	• Microsoft-Windows-Security-Auditing:4625 • Microsoft-Windows-Security-Auditing:4768 • Microsoft-Windows-Security-Auditing:4769 • Microsoft-Windows-Security-Auditing:4771 • Microsoft-Windows-Security-Auditing:4772 • Microsoft-Windows-Security-Auditing:4773 • Microsoft-Windows-Security-Auditing:4776

Policy Changes

Windows 2003 family:	Windows 2008 family:
• Security:612 • Security:643	• Microsoft-Windows-Security-Auditing:4719 • Microsoft-Windows-Security-Auditing:4739

System Services and Auditing

Windows 2003 family:	Windows 2008 family:
• Security:512 • Security:516 • Security:517 • Security:520 • Security:521 • Security:601	• Microsoft-Windows-Eventlog:1102 • Microsoft-Windows-Security-Auditing:4608 • Microsoft-Windows-Security-Auditing:4612 • Microsoft-Windows-Security-Auditing:4616 • Microsoft-Windows-Security-Auditing:4617 • Microsoft-Windows-Security-Auditing:4697 • Microsoft-Windows-Security-Auditing:4906 • Service Control Manager:7035 • Service Control Manager:7036

Index

E

F

G

H

I

L

M

N

P

Q

R