



# **Micro Focus Security ArcSight Connectors**

## **SmartConnector for Microsoft Exchange PowerShell**

### **Configuration Guide**

**June, 2018**

## Configuration Guide

### SmartConnector for Microsoft Exchange PowerShell

June, 2018

Copyright © 2012 – 2017; 2018 Micro Focus and its affiliates and licensors.

### Warranty

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

### Restricted Rights Legend

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

### Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated. Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation. UNIX® is a registered trademark of The Open Group.

### Revision History

Date	Description
10/17/2017	Added support for 2016 Access Auditing events. Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
11/17/2015	Expanded Troubleshooting information.
03/31/2015	Added support for Admin Audit 2013.
06/28/2013	Added GA support for 2010 and 2013 Exchange events.
11/15/2012	First edition of this guide.

## SmartConnector for Microsoft Exchange PowerShell

---

This guide provides information for installing the SmartConnector for Microsoft Exchange PowerShell and configuring the device for event collection. This connector is based upon Microsoft's PowerShell technology and is supported for installation on Windows platforms only. This connector remotely retrieves:

- Microsoft Exchange Server 2010 SP2 and 2013 Mailbox Audit and Admin Audit logs
- Microsoft Exchange Server 2016 Access Auditing logs

### Product Overview

The Exchange Management Shell is built on Windows PowerShell technology. It provides a powerful command-line interface for Microsoft Exchange Server 2010 and 2013 that enables automation of administrative tasks. With the Shell, you can manage every aspect of Exchange, including enabling new e-mail accounts, configuring SMTP connectors, storing database properties, storing transport agents, and more. The Shell can perform every task that can be performed by the Exchange Management Console and the Exchange Web interface, in addition to tasks that cannot be performed in those interfaces.

### Configuration

You need to be assigned permissions before you can enable mailbox audit logging. You must log in as a domain user to install and run the connector. To see what permissions you need, see the "Mailbox audit logging" entry in the **Messaging Policy and Compliance Permissions** topic in the Microsoft Exchange TechNet Library.

For 2010, see "Understanding Mailbox Audit Logging" at [https://technet.microsoft.com/en-us/library/ff459237\(v=exchg.141\).aspx](https://technet.microsoft.com/en-us/library/ff459237(v=exchg.141).aspx).

For 2013, see "Mailbox audit logging" at [https://technet.microsoft.com/en-us/library/ff459237\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/ff459237(v=exchg.150).aspx).

For 2016, see "Mailbox auditing in Exchange 2016" at [https://technet.microsoft.com/en-us/library/ff459237\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/ff459237(v=exchg.160).aspx).

You can use administrator audit logging in Microsoft Exchange Server 2013 to log when a user or administrator makes a change in your organization. By keeping a log of the changes, you can trace changes to the person who made the change, augment your change logs with detailed records of the change as it was implemented, comply with regulatory requirements and requests for discovery, and more. For more information about audit logs, see the Administrator Audit Logging topic in the Microsoft Exchange TechNet Library.

For 2010, see "Administrator Audit Logging" at [https://technet.microsoft.com/en-us/library/dd335144\(v=exchg.141\).aspx](https://technet.microsoft.com/en-us/library/dd335144(v=exchg.141).aspx).

For 2013, see "Administrator audit logging" at [https://technet.microsoft.com/en-us/library/dd335144\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dd335144(v=exchg.150).aspx).

For 2016, see "Administrator audit logging in Exchange 2016" at [https://technet.microsoft.com/en-us/library/dd335144\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/dd335144(v=exchg.160).aspx).

## Mailbox Audit Logs

Mailbox audit logs are generated for each mailbox that has mailbox audit logging enabled. Log entries are stored in the **Audits** subfolder of the audited mailbox **Recoverable Items** folder. This ensures that all audit logs are available from a single location, regardless of which client access method was used to access the mailbox or which server or workstation an administrator used to access the mailbox audit log.

By default, mailbox audit log entries are retained in the mailbox for 90 days. You can modify this retention period by using the [AuditLogAgeLimit](#) parameter together with the **Set-Mailbox** cmdlet.

## Enable Mailbox Audit Logging

By using mailbox audit logging, you can track logons to a mailbox, and also track what actions are taken while the user is logged on. When you enable mailbox audit logging, some actions performed by administrators and delegates are logged by default. None of the actions performed by the mailbox owner are logged.

You can specify which user actions (for example, accessing, moving, or deleting a message) should be logged for a logon type (administrator, delegate user, or owner). See "Use the Shell to Specify Logging Settings." The following table lists the actions logged by mailbox audit logging, including the logon types for which the action is logged.

Action	Description	Administrator	Delegate	Owner
Copy	An item is copied to another folder.	Yes	Not applicable	Not applicable
Create	An item is created in the mailbox (for example, a message is sent or received). Note: Folder creation is not audited.	Yes*	Yes*	Yes
FolderBind	A mailbox folder is accessed.	Yes*	Yes**	Yes
HardDelete	An item is deleted permanently from the Recoverable Items folder.	Yes*	Yes*	Yes
MailboxLogin	The user signed in to their mailbox.	No	No	Yes***
MessageBind	An item is accessed in the reading pane or opened.	Yes	Not applicable	Not applicable
Move	An item is moved to another folder.	Yes*	Yes	Yes

Action	Description	Administrator	Delegate	Owner
MoveToDeletedItems	An item is moved to the Deleted Items folder.	Yes*	Yes	Yes
SendAs	A message is sent using Send As permissions.	Yes*	Yes*	Not applicable
SendOnBehalf	A message is sent using Send on Behalf permissions.	Yes*	Yes	Not applicable
SoftDelete	An item is deleted from the Deleted Items folder.	Yes*	Yes*	Yes
Update	An item's properties are updated.	Yes*	Yes*	Yes

### Use the Shell to Enable Mailbox Audit Logging

This example enables mailbox audit logging for Ben Smith's mailbox.

```
Set-Mailbox -Identity "Ben Smith" -AuditEnabled $true
```

For detailed syntax and parameter information, see Set-Mailbox in the Microsoft Exchange TechNet Library (<http://technet.microsoft.com/en-us/library/bb123981.aspx>).

### Use the Shell to Specify Mailbox Audit Logging Settings

Use the shell to specify logging settings for Administrator, Delegate, and Owner access.

This example specifies that the **SendAs** or **SendOnBehalf** actions performed by delegate users will be logged for Ben Smith's mailbox.

```
Set-Mailbox -Identity "Ben Smith" -AuditDelegate  
SendAs,SendOnBehalf -AuditEnabled $true
```

This example specifies that the **MessageBind** and **FolderBind** actions performed by administrators will be logged for Ben Smith's mailbox.

```
Set-Mailbox -Identity "Ben Smith" -AuditAdmin  
MessageBind,FolderBind -AuditEnabled $true
```

This example specifies that the **HardDelete** action performed by the mailbox owner will be logged for Ben Smith's mailbox.

```
Set-Mailbox -Identity "Ben Smith" -AuditOwner HardDelete -  
AuditEnabled $true
```

## Administrator Audit Logs

Administrator audit logs contain a record of all the cmdlets and parameters that have been run in the Exchange Management Shell and by the Exchange Administration Center (EAC). They are created on-demand when you run the Administrator audit log report in the EAC, or when you run the **New-AdminAuditLogSearch** cmdlet in the Shell.

By default, audit logging is configured to store audit log entries for 90 days. After 90 days, the audit log entry is deleted. You can change the audit log age limit using the **AdminAuditLogAgeLimit** parameter. You can specify the number of days, hours, minutes, and seconds that audit log entries should be kept. To specify a value, use the format **dd.hh:mm:ss** where the following applies:

- **dd** - The number of days to keep the audit log entry.
- **hh** - The number of hours to keep the audit log entry.
- **mm** - The number of minutes to keep the audit log entry.
- **ss** - The number of seconds to keep the audit log entry.

To specify multiple years, use the **dd** field. For example, 365 days equals one year; 730 days equals two years; 913 days equals two years and six months. For example, to set the audit log age limit to two years and six months, use the syntax **913.00:00:00**.

## Enable Administrator Audit Logging

Each audit log entry contains the information described in the following table. The audit log contains one or more audit log entries. The number of audit log entries is controlled by the audit log age limit specified using the **Set-AdminAuditLogConfig** cmdlet. Any audit log entry that exceeds the age limit is deleted. See "Use the Shell to Specify Administrator Logging Settings." The following table lists the actions logged by administrator audit log entry fields.

Field	Description
RunspaceId	This field is used internally by Exchange.
ObjectModified	This field contains the object that was modified by the cmdlet specified in the 'CmdletName' field.
CmdletName	This field contains the name of the cmdlet that was run by the user in the Caller field.
CmdletParameters	This field contains the parameters that were specified when the cmdlet in the CmdletName field was run. Also stored in this field, but not visible in the default output, is the value specified with the parameter, if any.
ModifiedProperties	This field contains the properties that were modified on the object in the ObjectModified field. Also stored in this field, but not visible in the default output, are the old value of the property and the new value that was stored. NOTE: This field is only populated if the LogLevel parameter on the "Set-AdminAuditLogConfig" cmdlet is set to 'Verbose'.
Caller	This field contains the user account of the user who ran the cmdlet in the CmdletName field.
Succeeded	This field specifies whether the cmdlet in the CmdletName field ran successfully. The value is either True or False.
Error	This field contains the error message generated if the cmdlet in the CmdletName field failed to complete successfully.
RunDate	This field contains the date and time when the cmdlet in the CmdletName field was run. The date and time are stored in Coordinated Universal Time (UTC) format.

Field	Description
OriginatingServer	This field indicates the server on which the cmdlet specified in the CmdletName field was run.
Identity	This field is used internally by Exchange.
IsValid	This field is used internally by Exchange.
ObjectState	This field is used internally by Exchange.

### Use the Shell to Enable Administrator Audit Logging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Administrator audit logging" entry in the "Exchange and Shell Infrastructure Permissions" topic ([https://technet.microsoft.com/en-us/library/dd638114\(v=exchg.141\).aspx](https://technet.microsoft.com/en-us/library/dd638114(v=exchg.141).aspx)).

To enable administrator audit logging, use the following command:

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $True
```

### Use the Shell to Specify Administrator Logging Settings

Use the shell to specify logging settings for Administrator, Delegate, and Owner access.

This example enables administrator audit logging for every cmdlet and every parameter in the organization, with the exception of Get cmdlets.

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -
AdminAuditLogCmdlets * -AdminAuditLogParameters *
```

This example enables administrator audit logging for specific cmdlets run in the organization. Any parameter used on the specified cmdlets is logged. Every time a specified cmdlet is run, a log entry is added to the audit log.

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -
AdminAuditLogCmdlets *Mailbox, *Management*,
*TransportRule* -AdminAuditLogParameters *
```

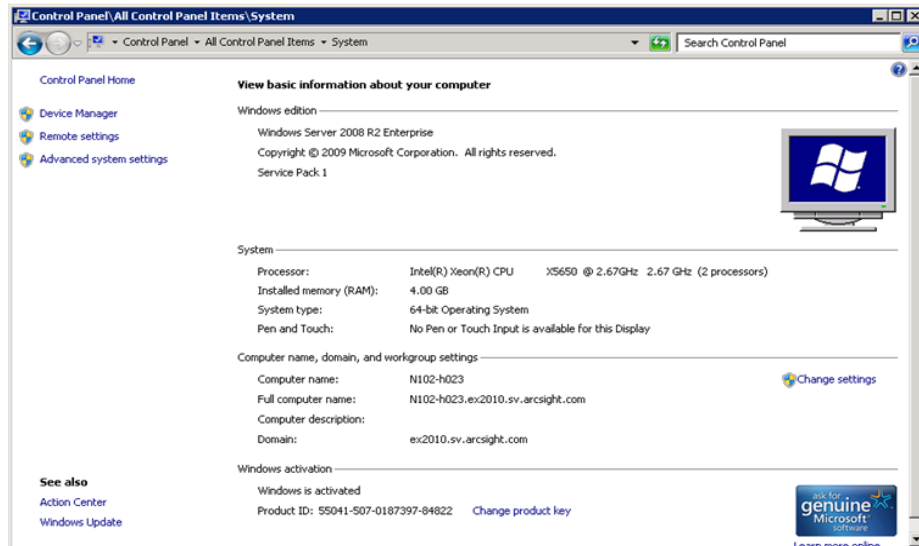
This example enables administrator audit logging only for specific parameters that are specified when running specific cmdlets. The parameter name and the cmdlet name must match the strings specified with the "AdminAuditLogCmdlets" and "AdminAuditLogParameters" parameters. For example, a log entry is generated only when a parameter with the string "Address" in the name is run on a cmdlet with the string "Mailbox" in its name.

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -
AdminAuditLogCmdlets *Mailbox* -AdminAuditLogParameters
*Address*
```

## Locate the Fully Qualified Domain Name

To fill in appropriate connector parameters to retrieve events from the correct source, you will need to know the Fully Qualified Domain Name (FQDN) of the Microsoft Exchange Server.

To find the FQDN, go to **Start -> Control Panel -> System**. Under **Computer name, domain, and workgroup settings**, find the **Full computer name**.



## Install the SmartConnector

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

### Prepare to Install Connector

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

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

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

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



## Install Core Software

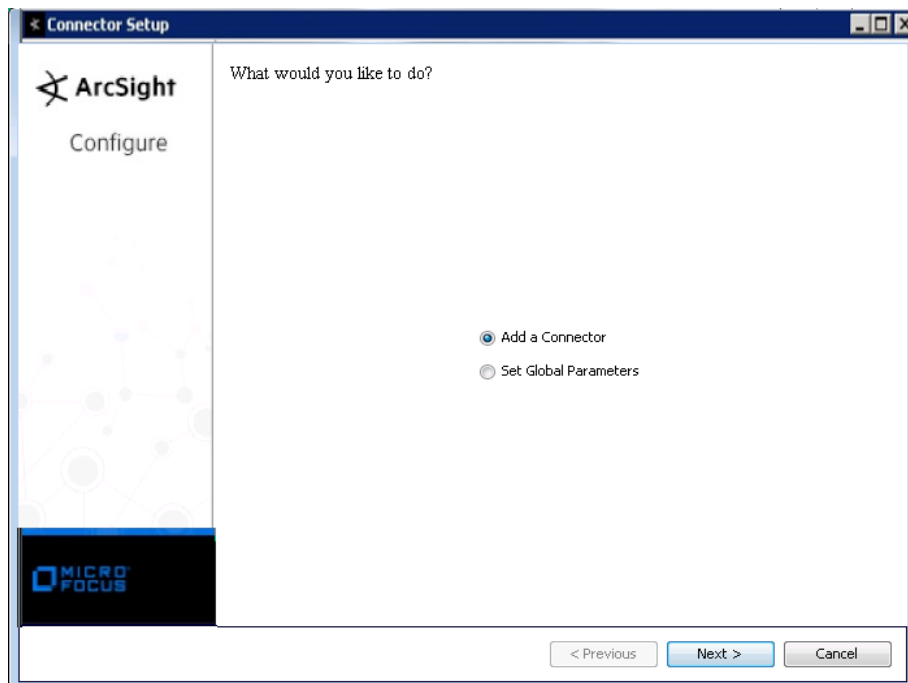
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

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

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

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

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



## Set Global Parameters (optional)

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

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

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

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

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

## Select Connector and Add Parameter Information

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

< Connector Setup

ArcSight  
Configure

Enter the parameter details

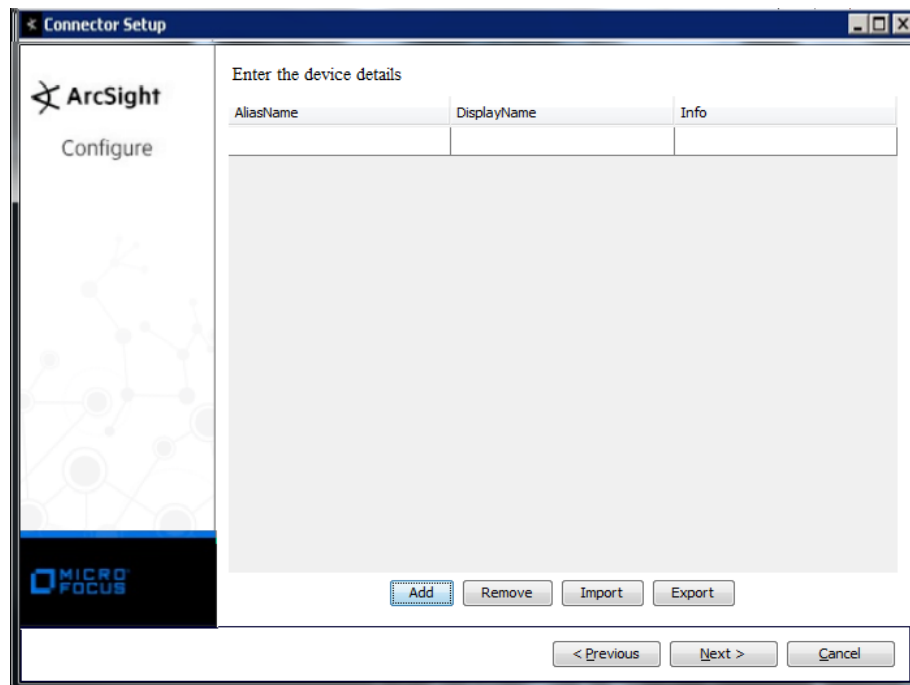
Server FQDN

PowerShell Path

Frequency (seconds)

MICRO FOCUS

< Previous   Next >   Cancel



Parameter	Description
Server FQDN	Specify the fully qualified domain name to the Exchange Server.
PowerShell Path	Enter the path to the directory where the PowerShell application is located. The default location is 'C:\Windows\System32\WindowsPowerShell\V1.0'.
Frequency (seconds)	Enter the frequency at which each mailbox audit log is to be retrieved, in seconds. The default value is 600 seconds.
AliasName	Enter the alias name of the mailbox user.
DisplayName	Enter the display name of the mailbox user.
Info	Add any pertinent information.

You can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. The connector automatically runs a script to create a CSV file containing the mailboxes for the server whose FQDN you specify during configuration. This file is located at \$ARCSIGHT\_HOME\user\agent\agentdata and has a file name of the format 'Mailboxes-yyyy\_mm\_dd-HH\_MM.csv'. You can click the 'Export' button to export the mailbox data you have entered into the table into a CSV file.

## Select a Destination

- 1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.
- 2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

- 3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.
- 4 If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

## Complete Installation and Configuration

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

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

## Run the SmartConnector

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

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

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

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

## Device Event Mapping to ArcSight Fields

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

### Microsoft Exchange PowerShell Mappings

ArcSight ESM Field	Device-Specific Field
Destination User ID	One of (DestMailboxOwnerSid, MailboxOwnerSid)
Destination User Name	One of (DestMailboxOwnerUPN, MailboxOwnerUPN)
Device Action	One of (Operation, CmdletName)
Device Custom String 1	One of (LogonType, ObjectModified)
Device Custom String 2	One of (SourceItemSubjectsList, CmdletParameters)
Device Custom String 3	One of (ItemSubject, ModifiedProperties)
Device Custom String 4	One of (ClientInfoString, ObjectState)
Device Custom String 5	MailboxResolvedOwnerName
Device Custom String 6	ExternalAccess
Device Event Class ID	One of (Operation, CmdletName)
Device Host Name	OriginatingServer
Device Process Name	ClientProcessName
Device Product	'Exchange Server'
Device Receipt Time	One of (LastAccessed, RunDate)
Device Vendor	'Microsoft'
Event Outcome	One of (OperationResult and Status(Succeeded,"True";Succeeded","Failed"))
External ID	Identity
File Path	DestFolderPathName
Name	One of (Operation, CmdletName)
Old File Name	SourceItemAttachmentsList
Old File Path	FolderPathName
Old File Size	SourceItemAttachmentsList
Source Address	ClientIPAddress
Source Host Name	ClientMachineName
Source User ID	LogonUserSid
Source User Name	One of (DelegateUserDisplayName, LogonUserDisplayName, Caller)

## Troubleshooting

### Execute PowerShell Scripts

This connector executes ArcSight Windows PowerShell scripts to retrieve information about mailboxes and events/logs from the Microsoft Exchange Server. Be sure you have turned on the execution policy for PowerShell through the Local Policy Editor to allow execution of these scripts. If other security measures block execution of these scripts, you can attempt to run the scripts directly.

When connection to the Exchange Server fails during configuration, search [agent.log](#) for information and execute a script directly from a PowerShell command line window.

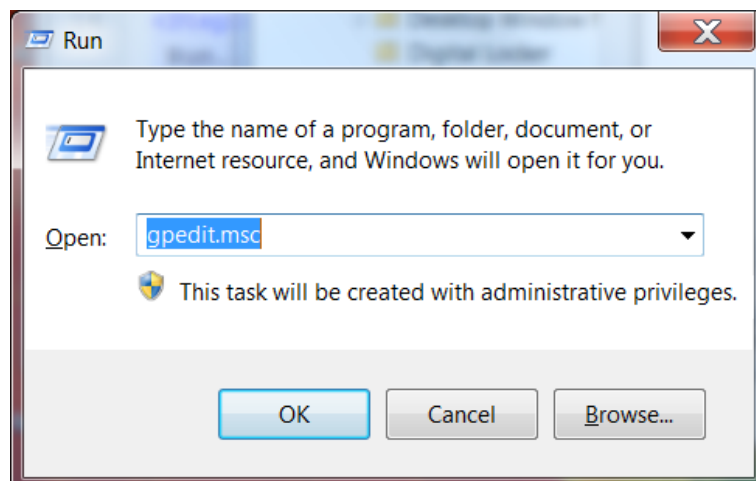
For example, from the box where the SmartConnector is installed, open a Windows command window and run the script [collectMailboxes.ps1](#) against the Exchange Server to retrieve mailbox information.

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell" -
file
"C:\$ARCSIGHT_HOME\current\bin\agent\microsoft\exchange\col
lectMailboxes.ps1" "<Exchange Server FQDN Hostname>"
"C:\$ARCSIGHT_HOME\current\user\agent\agentdata" "" ""
```

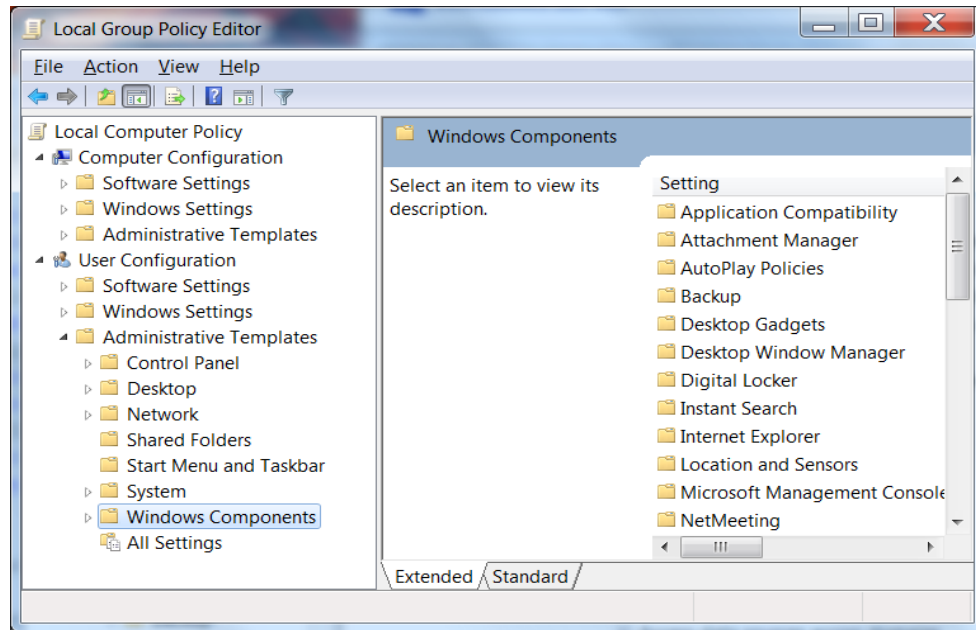
### Turn on Execution Policy for PowerShell

Turn on the execution policy for PowerShell through the Local Policy Editor:

- 1 To open the Local Group Policy Editor from the command line, click **Start -> Run...**, enter [gpedit.msc](#) in the **Open:** box and click **OK**.

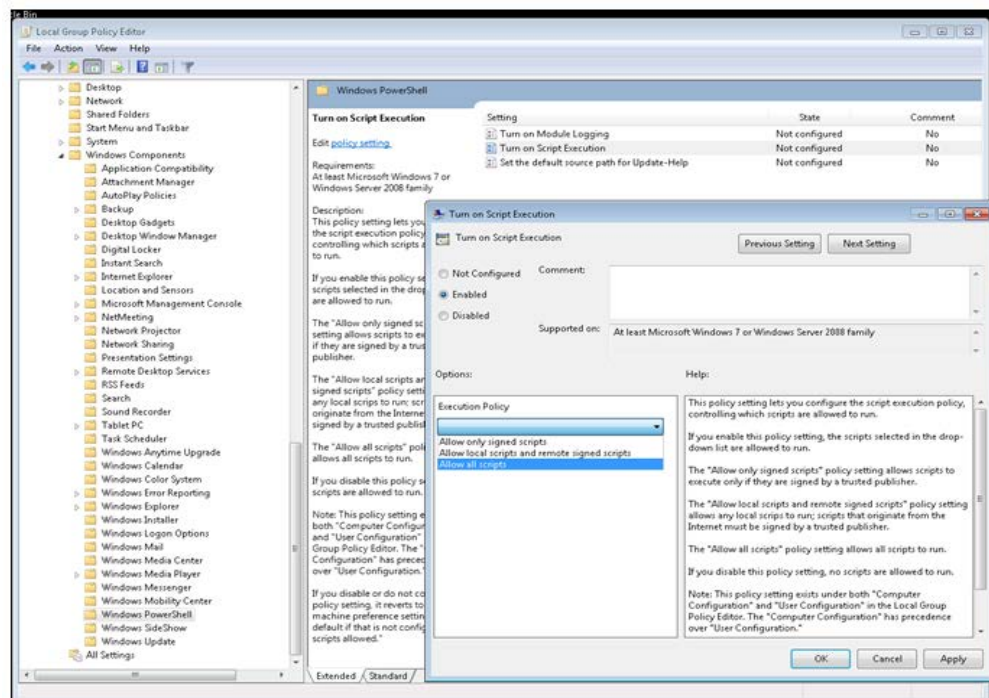


- 2 From the left pane, select **User Configuration -> Windows Components -> Microsoft PowerShell**.



If you do not see the PowerShell component, you will need to install Windows Management Framework. See "Install Windows Management Framework 3.0 RC."

- 3 With the Windows PowerShell component selected, check **Turn on Script Execution**.

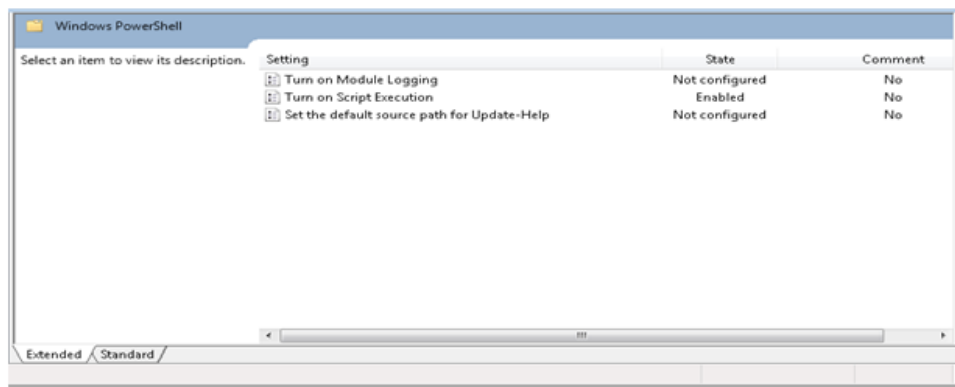


- 4 Under **Options, Execution Policy**, select **Allow all scripts**.

- 5 Click **OK**.



The **Turn on Script Execution** setting's state now shows **Enabled**.



## Install Windows Management Framework 3.0 RC

- 1 Download the correct package for your operating system and architecture.
  - ◆ Windows 7 Service Pack 1
  - ◆ 64-bit versions: WINDOWS6.1-KB2506143-x64.MSU
- 2 Close all Windows PowerShell windows.
- 3 Uninstall any other versions of Windows Management Framework 3.0.
- 4 Run the MSU file you downloaded.

For more information about scripting, see the [Group Policy Script Center](#).