Micro Focus Security ArcSight ESM

Software Version: 7.5

Actor Model Import Connector for Microsoft Active Directory Configuration Guide

Document Release Date: May 2021

Software Release Date: May 2021

MICRO FOCUS®

Legal Notices

Copyright Notice

© Copyright 2001-2021 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services 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.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

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.

Support

Contact Information

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

Contents

ESM

This guide describes installing the ESM and configuring the device for data collection.

Microsoft's Active Directory allows IT administrators to centrally manage objects in an enterprise. These objects include resources (such as printers), users (such as individual users and user groups), and services (such as e-mail).

The ESM extracts the user identity information (or Actor data) from the Active Directory LDAP, then uses that data to populate ArcSight ESM with resources. The Actor resource is populated dynamically, meaning that, as the identity data changes in Active Directory, the resource data in ESM is automatically updated.

> **Note:** The connector only supports queries on the same domain as the user accounts. The connector does not support queries across domains.
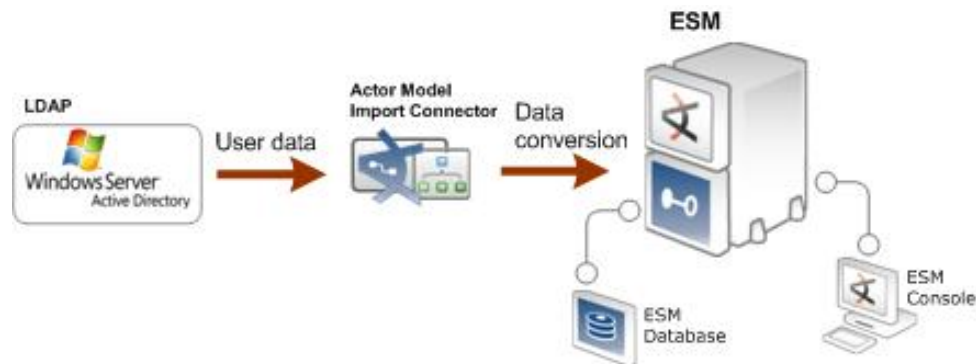
Active Directory Support

The ESM supports the following versions of Microsoft Active Directory:

- Active Directory on Microsoft Windows Server 2008

Importing the CA Certificate

To enable SSL support for the connector's LDAP connection to the Active Directory, you must have exported a CA certificate from Microsoft Certificate Services. The CA certificate will be imported into the connector's certificate store. The CA certificate must be exported in one of the following formats:

- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)

To import the CA certificate to the connector's certificate store:

1. From `$ARCSIGHT_HOME\current\bin`, execute the keytool application to import the CA certificate. Enter this keytool command on a single line:

   `jre\bin\keytool -keystore jre\lib\security\cacerts -storepass changeit -importcert –file <>`

   where the path to the certificate could be, for example:

   `"C:\MIC\AD Actor MIC\AD.cer"`

2. When prompted **Trust this certificate?**, click **Yes**.

3. Verify the imported certificate by entering this command from `$ARCSIGHT_HOME\current\bin`:

   `arcsight agent keytool -list -store clientcerts`

   The new certificate is listed.

Installing the Actor Model Import Connector

Before you install a connector, make sure that ArcSight ESM has already been installed correctly. For a successful installation of ArcSight ESM, install the components in the following order:

1. Ensure that the ArcSight Manager and Console are installed correctly.

2. Run the ArcSight Console. Though not necessary, it is helpful to have the ArcSight Console running when installing the connector to verify a successful installation.

3. Run the ArcSight Manager; the Manager command prompt window or terminal box displays a **Ready** message when the Manager starts. You can also monitor the `server.std.log` file located in `$ARCSIGHT_HOME\logs\default`.

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

- Local access to the machine where the connector is to be installed
- Administrator passwords
- Administrator user name and password for Active Directory access

> **Note:** For read and access privileges for the connector, a basic AD user ID will work.

Connector Installation

> **Note:** Use a non-root account to install the Active Directory Model Import Connector.

To install the connector, do the following.

1. Using the log-in credentials provided, download the ArcSight executable for your operating system from the Software Support Site.

2. Start the connector installer by running the executable.

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

   - Introduction

   - Choose Install Folder

   - Choose Shortcut Folder

   - Pre-Installation Summary

   - Installing...

   When the installation of connector core component software is finished, the Select Connector to Configure screen displays.

   > **Note**: The options for FIPS and remote management are not applicable at this time when "Set Global Parameters" is selected for this connector.

3. On Protect 724, under ArcSight Product Documentation, see chapter 4 "Modifying Connector Settings," in the SmartConnector User Guide for setting **preferred IP version**.

4. Select **Actor Model Import Connector for Microsoft Active Directory**. Click **Next**.

5. On the parameter details screen, enter values for the following parameters:

   Parameter Details

Parameter	Description
Active Directory machine host name or IP	Enter the host name or an IP address of the Active Directory server.
Security protocol	Select ssl (encrypted) or non-ssl (default, non-encrypted). Also, select an Active Directory port.
Active Directory port	Enter the port; 636 for SSL security protocol, or 389 for non-SSL security protocol.

Parameter Details, continued

Parameter	Description
Administrator user for Active Directory	Enter the name of a user from the Domain Admins group that the SmartConnector can use to access Active Directory data.
AD administrator's password	Enter the password for the user you specified as the Administrator user for the previous parameter.
AD query paused	Leave the default value of 'true.' After the connector is started from the ESM Console, this value changes to 'false' automatically so that the AD query continues automatically whenever the connector restarts.
AD query interval (in minutes)	Enter the time interval after which the SmartConnector polls the Active Directory server for updates. The default value is 10. The minimum value that can be specified is 1.
AD search base	Enter the search base of the Active Directory domain; for example, DC=company, DC=com.
IDM Identifier	Enter a name of your choosing to identify the IDM system from which the connector is carrying data. (e.g., "**company-dc.company.com**")

Click **Enter**.

6. On the type of destination screen, verify that **ArcSight Manager (encrypted)** is selected and then click **Next**.

7. On the destination parameters screen, enter or select values for the parameters and click **Next**. The connector details screen displays.

8. Enter the details for your connector. Click **Next** and complete the installation wizard.

> ✓ **Tip:** After completing the SmartConnector installation wizard, be sure to manually configure the connector for the type of SSL certificate your ArcSight Manager is using. See the *ArcSight ESM Administrator's Guide* for complete information.

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

> ⚠ **Caution:** Save any work on your computer or desktop and shut down any other running applications (including the Command Center, if it is running), then shut down the system.

Changing the Connector Heap Size

> ⚠️ **Caution:** If your deployment exceeds 10K actors with an average of five groups per user, we recommend modifying your minimum heap setting to 2GB. The maximum heap size should be 6GB.

MIC Installed As a Service

If you are going to import a large number of actors, it is recommended that you increase the heap size of the connector. The default heap size is 256 MB. If you are going to run the connector as a service, set the heap size in the following file:
`../current/user/agent.wrapper.conf`

Set the following parameters:

```
#Initial Java Heap Size (in MB)
wrapper.java.initmemory=2048

#Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=6144
```

MIC Installed As Standalone

If the connector runs in standalone mode, the default heap size is 256 MB. For proper operation of the connector with a large number of actors, Micro Focus recommends that you modify the heap size setting to 6 GB. Increase the memory for the connector by creating one of the following commands:

- For Linux - create the following shell script:
  `~/ARCSIGHT_HOME/current/user/agent/setmem.sh`
  with the following content:
  `ARCSIGHT_MEMORY_OPTIONS="-Xms2048m -Xmx6144m"`
- For Windows - create the following batch file:
  `$ARCSIGHT_HOME\current\user\agent\setmem.bat`
  with the following content:
  `SET ARCSIGHT_MEM_OPTIONS= -Xms2048m -Xmx6144m`

  > 📋 **Note:** Additional installation points:
  > - `ARCSIGHT_HOME` represents the directory where the connector is installed.
  > - Use regular double quote characters in the commands.

To uninstall the connector, or for connector upgrade instructions, see the SmartConnector User's Guide.

Optional Optimization of Data Transfer

For medium to large deployments, the connector processes data optimally. The default for batching *time* is 1 minute and batching *size* is 2500 users (or Actors). For a smaller deployment, you may want to reduce these parameters.

> **Note:** For more information about Actors, including the maximum number of actor models supported in ArcSight ESM, see the *Command Center online help.*

To change the Actor batching time or size, you can add the following properties to `agent.properties` (located at `$ARCSIGHT_HOME\current\user\agent`).

- `buildmodeldelay` controls the batching time. This dictates how long in milliseconds the wait before sending a batch of Actors to ESM.
- `maxeventsbeforebuild` controls the batching size. This dictates how many Actors can be received before sending a batch of Actors to ESM.

For example, the following properties set the batching time to 10 seconds and the batching size to 2500 Actors:

`agent.component[35].buildmodeldelay=10000`

`agent.component[35].maxeventsbeforebuild=2500`

The trigger for sending user (or Actor) data to ESM can be controlled through either a **counter** (the indicator of batch size) or **timer** (the indicator of elapsed time between batches). Priority is given to the first satisfied condition. For example, if the batch size achieves the maximum number of Actors allowed before the default time is exceeded, the Actor data is sent based on batch size. Conversely, if the defined time is reached before the defined buffer size is achieved, the data is sent to ESM based on the allotted time. After the batch is sent to ESM, the timer and counter revert back to zero in preparation for the next batch.

> **Caution:** If your deployment exceeds 10K actors with an average of 5 groups per user, we recommend modifying your minimum heap setting to 2GB. The maximum heap size should be 6GB, depending on available memory.

Run the Connector

Connectors can be installed and run in standalone mode, as a Windows service, or as a UNIX daemon. If installed standalone, the connector must be started manually, and is not

automatically active when a host is re-started. If installed as a UNIX daemon, the connector runs automatically when the host is re-started. For information about connectors running as Windows services or UNIX daemons, see the ArcSight SmartConnector User's Guide.

For connectors installed standalone, to run all installed connectors on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run:

`arcsight agents`

When you run the connector, it is started in Pause mode; it does not continue until you instruct it to do so through the ArcSight Console. Before doing so, set up a user for the connector, as described in the next section.

To view the connector log, read the file:

`$ARCSIGHT_HOME\current\logs\agent.log`

To stop all connectors, enter `Ctrl+C` in the command window.

> ✅ **Tip:** On Windows platforms, connectors can also be run using shortcuts and optional Start menu entries.

Importing Actor Data

You can set up the actor model import user, optional filter settings, and the initial import of actor data, as detailed in the following sections.

## Set up the Actor Model Import User in ESM

After installing and starting the connector, use the ArcSight Console to configure the connector with administrative privileges for the Model Import User.

1. From the ArcSight Console, go to the **Navigator** panel and choose the **Resources** tab.
2. Under **Resources**, choose the **Connectors** resource.
3. Under **All Connectors**, navigate to your **ESM**.
4. Right click on the connector and select **Configure**.
5. On the **Inspect/Edit** panel, choose the **Connector** tab.
6. Under the **Connector** tab, go to the **Model Import User** and select a user from the **Administrators** group.
7. Click **OK**.

Optional Configuration of Filter Settings

Setting up filtering conditions is optional, but recommended for use with a large number of users. Note that, when filtering by group type or group name, it is the group membership that is filtered; the users imported are not affected.

1. Configure filtering conditions by group name by entering each group name separated by the OR operator. Right-click the connector name, then **Configure**, **Default**, and **Filters**. Match the group name in the filtering condition to the group name found in Device Custom String 3, as shown in the following examples, which show filtering OUT by Name.
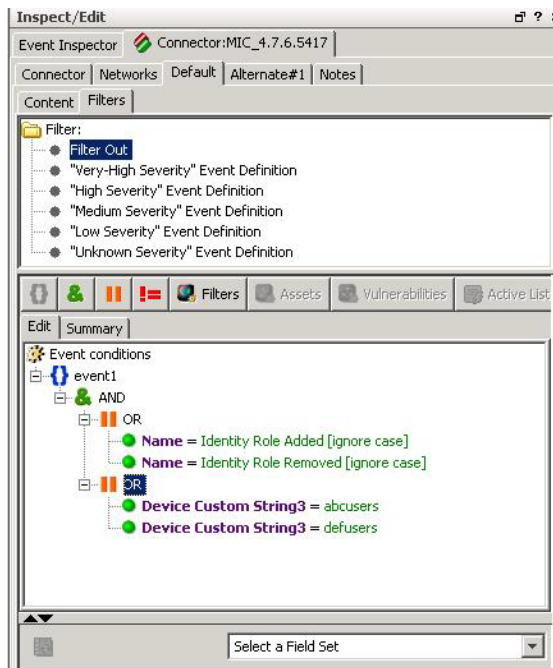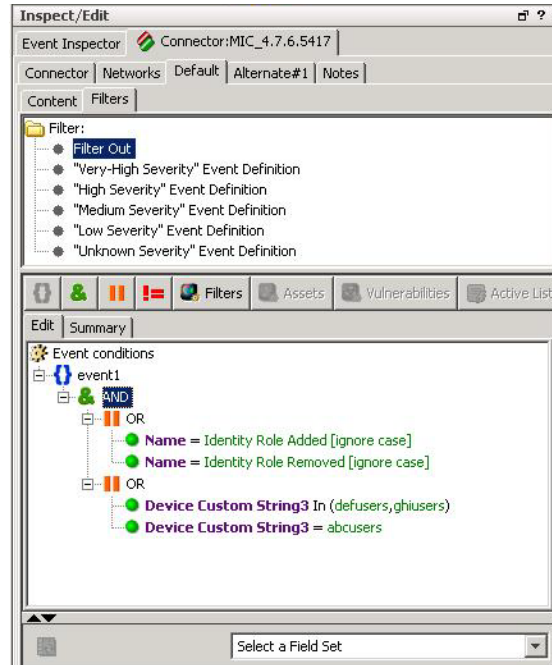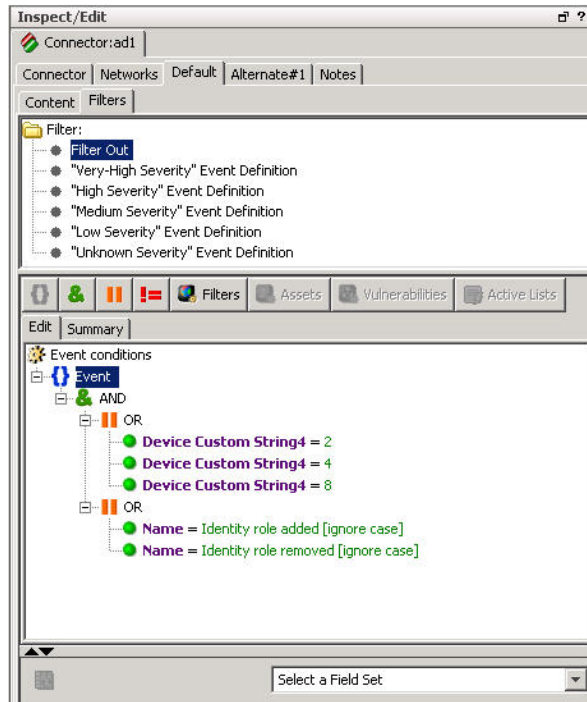
The following is an example of filtering IN groups by group Name.
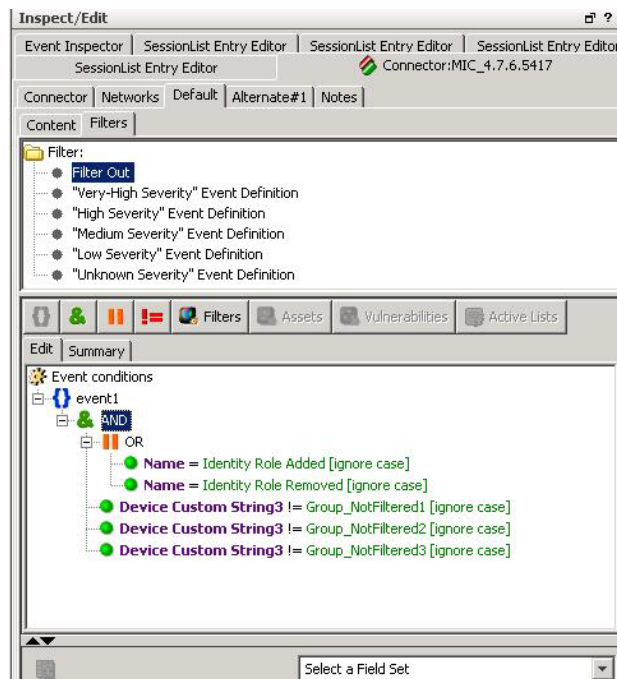
2. Configure filtering conditions by group type by entering each group type separated by the OR operator. Right-click the connector name, then **Configure**, **Default**, and **Filters**.

   The following is an example of filtering OUT groups by group Type. By default, the connector does not filter OUT groups by type.

Group types are as follows:

Type	Name
-2147483646	Global Security Group
-2147483644	Local Security Group
-2147483643	BuiltIn Group
-2147483640	Universal Security Group
2	Global Distribution Group
4	Local Distribution Group
8	Universal Distribution Group

Initial Import of Actor Data

The first time you import a large deployment of actors, run the server with no load, stop all the feeds and make sure that the EPS is zero.

To start the initial import of Actor data, start the Actor Model Import Connector from the console.

1. From the ArcSight Console, go to the **Navigator** panel and choose the **Resources** tab.
2. Under **Resources**, choose the **Connector** tab.
3. Navigate to the connector you wish to start from under the **All Connector** directory.

4. Right-click the connector and choose **Send Commands** -> **Model Import Connector**-> **Start Import**.

    The initial import begins.

    > **Note**: This initial import of data cannot be stopped until the transfer is complete. If you discover a configuration error mid-process, stop the connector, make your configuration changes, then reload the Active Directory information. See "Reloading Active Directory Information" on page 17 for detailed instructions.

5. After the import completes, configure the authenticators mapping table in ArcSight Console with the list of authenticators used in your environment. For detailed instructions, see the "Configuring Actors (for Administrators)" section of the ArcSight Console online help.

Advanced Parameter Tuning

You can tune the parameters used during account imports by modifying the account specifier and the authenticator properties. The following sections provide information about each property.

Account Specifier

The account specifier, for Active Directory accounts, has the following default values:

- sAMAccountName
- mail
- distinguishedName
- userPrincipalName

You can add or remove attributes by modifying the `accountspecifier` property. To add or delete attributes, the `accountspecifier` property is added to `agent.properties` (located at `$ARCSIGHT_HOME\current\user\agent`). For example:

```
agents[0].accountspecifier=givenName,title
```

If used, this property should be specified before the initial import since account import behavior is affected by the `accountspecifier` property. It is not advisable to add or delete attributes unless you are certain about why you are making the changes. A typical use case would be if your LDAP domain has a limitation needing a set of attributes other than the default attributes to identify an account.

Authenticator

The authenticator, for Active Directory accounts, can be controlled by the `authenticator` property. The default value is derived from the DC components of the search base, but it can be modified with the `authenticator` property.

To change the account authenticator, add the `authenticator` property to `agent.properties` (located at $ARCSIGHT_HOME\current\user\agent). For example:

`agents[0].authenticator=mf.net.local`

If used, this property should be specified before the initial import since account import behavior is affected by the `authenticator` property. It is not advisable to add the property unless you are certain about why you are adding the property. A typical use case would be to have one authenticator across multiple domains.

Accessing Advanced Parameters

Change the value for the properties in the agent.properties file located in the $ARCSIGHT_ HOME/current/user/agent directory after connector installation.

For Windows, the path starts with %ARCSIGHT_HOME% and uses back slashes. For example:

- Linux: $ARCSIGHT_HOME/current/user/agent/agent.properties
- Windows: %ARCSIGHT_HOME%\current\user\agent\agent.properties

The `agent.properties` file is a plain text file. Use the appropriate editor for your operating system to edit the content. For example, use Notepad for Windows and vi for Linux. Any modifications to the `agent.properties` file should be performed very carefully with knowledge of how parameters operate. This way, you would avoid inadvertently altering the behavior of the SmartConnector.

Access Attribute Fields

After connector installation, all the supported attributes are preselected. These attributes can be accessed using the Options menu, as described above.

> ⚠️ **Caution:** If you wish to re-add an attribute that you did not import initially, you must re-import the entire set. See "Reloading Active Directory Information" on page 17 for detailed instructions.

Locate the `attributelist` parameter to remove any unneeded attribute fields. Do not remove a required attribute (the first 15 attributes of the following list), as they are the minimum required for the system to properly operate.
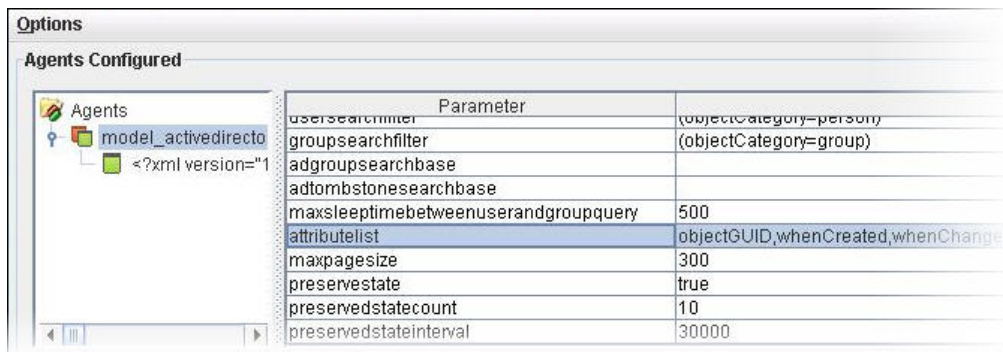
objectGUID

whenCreated

whenChanged

memberof: Member of

member: Member

sAMAccountName: User ID

mail: Email Address

distinguishedName: Distinguished Name

userPrincipalName: User Principal Name

cn: Full Name

givenName: First Name

sn: Last Name

department: Department

userAccountControl: Status

employeeType: Employee Type

> ✓ **Tip:** The employeeType attribute is not available in the native Microsoft Management Console. To use the resources based upon Employee Type, the attribute must be set using a tool such as ADSI edit. ADSI Edit is an MMC snap-in that acts as a low-level editor for Active Directory. This tool is included when you install Microsoft Windows Server Support Tools from the product CD or from the Microsoft Download Center (**http://go.microsoft.com/fwlink/?LinkId=100114**). For information about how to install Windows Support Tools from the product CD, see Install Windows Support Tools at **http://go.microsoft.com/fwlink/?LinkId=62270**.

The following attributes are optional and may be deleted.

> ⚠️ **Caution:** If you wish to re-add an attribute you mistakenly deleted, you must re-import the entire set. See "Reloading Active Directory Information" below for detailed instructions.

```
initials: Middle Initial

title: Title

company: Company

manager: Manager

physicalDeliveryOfficeName: Office

telephoneNumber: Business Phone

mobile: Mobile Phone

facsimileTelephoneNumber: Fax

pager: Pager

streetAddress: Address

l: City

st: State

postalCode: Zip Code

co: Country or Region
```

Role attributes are mapped as follows:

```
groupName: Role Name
resourceName: Resource Name
groupTypeName: Role Type
```

The group name will be a number and the groupTypeName will be this translation:

```
groupTypeName groupName
Built-In -2147483643
Domain Local Security -2147483644
Global Security -2147483646
Universal Security -2147483640
Domain Local Distribution 2
Global Distribution 4
Universal Distribution 8
```

Reloading Active Directory Information

To reload all Active Directory information:

1. If active, stop the Actor Model Import Connector.

2. From the Command Center, go to the **Navigator** panel and choose the **Resources** tab.

3. Under **Resources**, choose the **Actors** tab.

4. Under **All Actors**, go to the top level directory (This should be the connector's domain name related to Active Directory. Do not choose any subdirectories). Right-click from this top level and choose **Delete Group** from the shortcut menu, as shown below
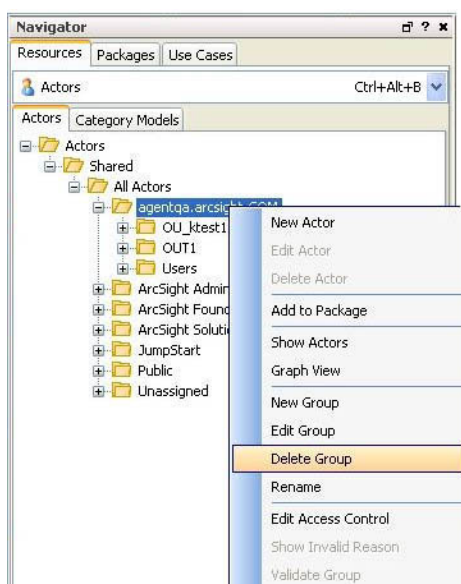
> ⚠ **Caution:** Do not delete Actors outside of this top level directory. If you are deleting a large number of actors, see "Best Practices for Deleting a Large Number of Actors" below.
>
> **Caution:** Performing this action **does not** remove all the Actor data and history.

5. From the following directory, delete all files starting with **ps.user** and **ps.group**:

    $ARCSIGHT_HOME/user/agent/agentdata

6. From this same directory ($ARCSIGHT_HOME/user/agent/agentdata), delete the {connector_id}.status.init.import file.

7. Restart the connector.

Best Practices for Deleting a Large Number of Actors

Deleting an entire actor group from the ArcSight Console can take an extended period of time, locks the console, and might never complete. You can delete actors manually to avoid these issues.

1. SSH to the ArcSight Manager as *arcsight* user.

2. Add the following line to `server.properties` in `/opt/arcsight/manager/config`:

   `dbconmanager.provider.logger.pool.maxcheckout=36000`

3. In the ArcSight Console, stop the Actor Model Import Connector for Microsoft Active Directory. Right-click the connector and choose `Send Commands > Model Import Connector > Stop`.

4. Stop the ArcSight Manager.

5. Delete the actor data from the database. Run the following command in `/opt/arcsight/logger/current/arcsight/bin`:

   `./mysql -u<username> -p<password>`

   Where `<username>` and `<password>` are the database user name and password that were set when you configured the database. Per MySQL conventions, omit the space between `-p` and the password.

   In the resulting MySQL prompt, enter the following MySQL instructions:

   ```
   use <ESM database name>;
   delete from arc_actor;
   delete from arc_resource where resource_type=56;
   delete from arc_sld_res56B_DN;
   delete from arc_sld_res56B_UUID;
   delete from arc_sld_res56D_BASE;
   delete from arc_sld_res56D_ROLES;equalespn
   delete from arc_sld_res56B_ACCTS;
   delete from arc_sld_res56D_ACCTS;
   commit;
   quit;
   ```

   If any of the delete commands fail with the SQL message `ERROR 1205 (HY000): Lock wait timeout exceeded; try restarting transaction`, retry the delete command after a few seconds.

6. Start the ArcSight Manager.

7. From the ArcSight Console, delete any remaining actors from the Actor group.

8. On the machine where the Actor Model Import Connector for Microsoft Active Directory is installed, delete the following files from `/user/agent/agentdata`:

   `*ps` files
   `*status.init` files

9. Restart the Actor Model Import Connector for Microsoft Active Directory.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Actor Model Import Connector for Microsoft Active Directory Configuration Guide (ESM 7.5)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!