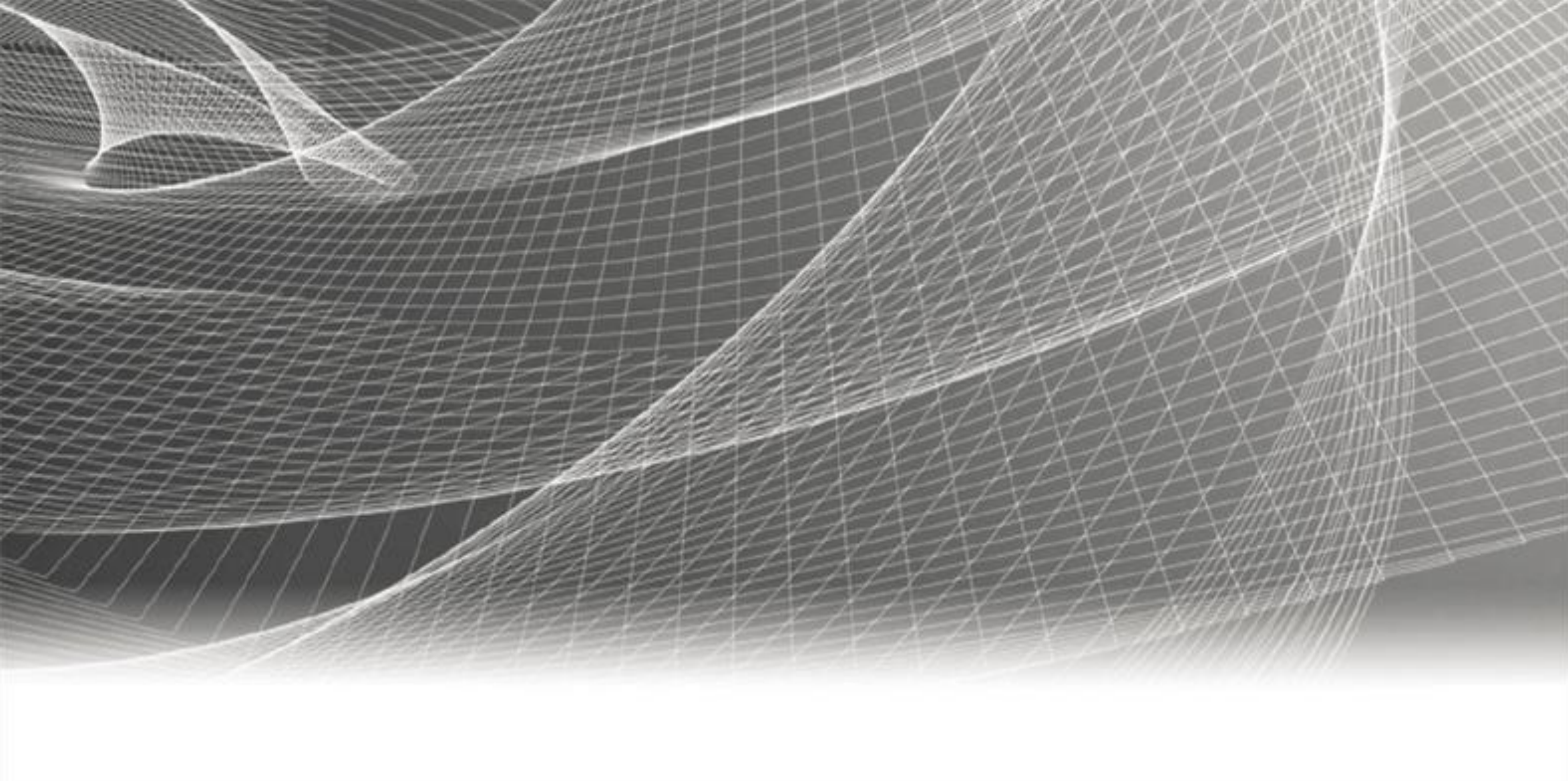


RSA | Identity Governance and Lifecycle

Active Directory Application Guide

Version 1.9 | May 2020

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

Dell, RSA, the RSA Logo, EMC and other trademarks, are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporationtrademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell Inc. or its subsidiaries, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell Inc.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed by launching the RSA Identity Governance and Lifecycle product and selecting the About menu. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any Dell software described in this publication requires an applicable software license.

Dell Inc. believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Contents

Revision History

Revision Number	Description
Version 1.0	Active directory
Version 1.1	Added instructions for configuring connection and read timeouts to collector
Version 1.2	Added instructions for configuring the password vault with RSA Identity Governance and Lifecycle Active Directory Connector
Version 1.3	Added instructions for configuring the password vault with RSA Identity Governance and Lifecycle Active Directory Account Data Collector
Version 1.4	Added instructions for configuring the password vault with RSA Identity Governance and Lifecycle Active Directory Identity Data Collector and Entitlement Data Collector
Version 1.5	Added instructions for configuring ‘Last login date’ and ‘Expiration date’ attributes with Active Directory Account Data Collector
Version 1.6	Added details for configuring the password vault with RSA Identity Governance and Lifecycle Active Directory Wizard
Version 1.7	Updated the information related to UAC PASSWD_CANT_CHANGE Under Appendix in section UAC Values
Version 1.8	Added information regarding limitations for using global catalog port while collection
Version 1.9	Updated the support version

Preface

This guide provides an overview of Out-Of-The-Box (OOTB) Connectors and Collectors for the Microsoft Active Directory (AD). This guide describes the required configurations, parameters and attributes mapping between the Connector and Collectors, and how to use the Application Wizard.

Audience

This guide is for RSA Identity Governance and Lifecycle users, including security administrators, Active Directory (AD) owners, and system configuration administrators.

Supported RSA Identity Governance and Lifecycle versions:

- RSA Identity Governance & Lifecycle version 7.0.0 and later

Supported Active Directory versions:

- Microsoft Window Server 2008 R2 SP1 Enterprise Edition and later

What is covered in the Guide

- **Overview** describes how Connectors and Collectors can help integrate RSA Identity Governance and Lifecycle with Active Directory.
- **Using the Active Directory Application Wizard** describes how to use the Active Directory wizard to create a Connector and Collectors for Active Directory.
- **Creating an Active Directory Connector and Collectors** describes how to configure or change the Collectors and Connector settings, if required.
- **Appendix** describes details of Active Directory configurations with RSA Identity Governance and Lifecycle viz. Domain configuration, SSL configuration, User Access Control configuration.
- **Troubleshooting** provides details on possible errors and their solutions.

Overview

Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services.

In RSA Identity Governance and Lifecycle, a Directory is an object that represents the data sources in the organization. You can create and manage a directory in order to collect identities of users, accounts, and entitlements.

These directories also serve as the managed entity for the data contained in them, which means directory owners can be designated as participants in the review process and in approval and fulfillment phases for change request workflows.

RSA Identity Governance and Lifecycle has the capacity to provision and de-provision entities using its Active Directory Connector, which can create new users, modify groups assignments, and modify User Account Control (UAC) parameters.

Using the Active Directory Application Wizard to Configure Collectors and Connector

RSA Identity Governance and Lifecycle provides an Application Wizard which simplifies the process of setting up Active Directory Connector and Collectors. Use the Application Wizard to set up Active Directory Connector and Collectors. If you need to modify these Connectors/Collectors later, then refer to next section(s).

Prerequisites

Manage Endpoint Credentials Using a Password Vault

To use a third-party password vault to manage the endpoint credentials, perform the following steps. RSA Identity Governance and Lifecycle currently supports the password vault.

1. Configure the password vault according to the third-party provider's instructions.

2. Create a new password vault profile in RSA Identity Governance and Lifecycle for retrieving the Active Directory password from the vault. See the RSA Identity Governance and Lifecycle Help for more information about creating a password vault profile.

3. Ensure that an Active Directory account has been created at the configured password vault for storing the password.

Configuring Active Directory as an identity source and creating its Collectors and Connector

1) From the main menu, click Resources > Directories.
2) Click Create Directory.
3) Select Active Directory (AD), and then click Next.
4) On the Remote Application Setup page, read through the content to better understand how to prepare a list of required parameters.
5) Click Next.
6) On the Connect page, configure the parameters. See the table for the description of the fields.

Refer to *Manage Endpoint Credentials Using a Password Vault* in the prerequisites section for using static or dynamic passwords during wizard configuration.

Field	Description
Directory	Choose a name for this directory
Domain Controller Host Name	The Setup page mentioned in step 4 above describes how to get this parameter from the server.
Domain Controller LDAP Port	Port number to the server (Default Non-SSL- 389 and SSL – 636) **Note:** To collect users/accounts from AD sub-domain from forests, use Global Catalog port, i.e. Non-SSL-3268

	and SSL-3269. (Refer to the Global catalog limitations for details)
Windows Domain Name	Windows Domain name for which the Domain controller is configured.
Domain Account Name	Admin account name to use for the collection and provisioning activities
Static Password	Select this option to provide the password manually. Fill in the value of password for the AD administrator in the area provided.
Dynamic Password	Select this option to use a configured password vault to manage the endpoint credentials. After you select this option, either select a previously configured password vault profile from the drop-down menu, or click Create Profile to add a new password vault profile to use with this connector. RSA Identity Governance and Lifecycle uses this profile to retrieve the appropriate credentials from the password vault during connector deployment and connection tests.
Connection Timeout	The time in milliseconds a collector waits to complete the initial TCP connection handshake before the connection attempt is aborted. It should be greater than zero.
Read Timeout	The time in milliseconds a collector waits to read data after the previous read before the read attempt is aborted. It should be greater than zero.
Use SSL	Choose whether to use Secure Sockets Layer (SSL) to connect. By default, traffic is transmitted unsecured. You can make traffic confidential and secure by using SSL. Before you configure SSL, you must first make sure that AD over SSL is enabled on your Active Directory server. Note: RSA Identity Governance and Lifecycle 7.0.1 and higher require TLS1.0 or later for SSL communication. Active Directory must be enabled with TLS1.0 or above. RSA Identity Governance and Lifecycle supports TLS1.0, TLS1.1, and TLS1.2. RSA Identity Governance and Lifecycle versions 7.0.1 and higher do not support SSLv3.
Skip Certificate Validation (If SSL is selected)	This is available if Use-SSL is selected. Not recommended for production, but can be used for testing. This option lets the AD server and RSA Identity Governance and Lifecycle communicate without validating the security certificates. **WARNING: This skips SSL certificate validation. RSA does NOT recommend using this option.**

Select Certificate	This is available if Use-SSL is selected. From a list of valid certificates retrieved from the AD server for a given host-port, select one for SSL communication
Certificate	This is available if Use-SSL is selected. And where certificate contents can be copied. Note: SSL Certificate Configuration is explained in the Appendix.
AFX Server	Select AFX server in case AD Connector needs to be configured.

7) Click Next.
8) On the Accounts page, select the Collect Accounts checkbox to enable user collection from Active Directory.
   a. Fill out the form fields to configure the Account Data Collector (ADC) for Active Directory. The following table describes each field.

Field	Description
Search DN	The DN from where the user accounts are to be collected
Page Size	Page size to collect records in paginated form
Search Filter	Default value is: (&(objectCategory=person)(objectClass=user)(sAMAccountName=*)) This can be changed as needed for users environment.
ObjectSID (Optional)	If checked, collects ObjectSID, an account attribute for groups' foreign security principle member resolution.

   b. Click Test Search to make sure that the connection and search parameters are correct.
   c. Select a way to link the accounts to users. The following table describes each option.

Option	Description
Collect Accounts as Users	Accounts from AD server is treated as Users of RSA Identity Governance and Lifecycle
Map Accounts to Users using Account Name	Account name is used as User name
Map Accounts to Users using Email Address	Account's Email ID is used as User Name
Do not map Accounts to Users	Selecting this option does not link any user to any collected Account.

9) Click Next.
10) On the Groups page, select the Collect Groups checkbox to enable the group collection from the Active Directory. The following table describes each field.

Field	Description

Search DN	The DN from where the groups are to be collected
Search Filter	Default value is: (objectClass=group) This can be changed as needed for users environment
ObjectSID (Optional)	If checked, collects ObjectSID, an account attribute for groups' foreign security principle member resolution
Collect Primary Group Members (Optional)	If checked, it collects the primary group members.
Collect Dynamic Group Members (Optional)	If checked, collects the members who are dynamically part of group based on the filter defined for each group.

Click Test Search to make sure that the provided connection and search parameters are correct.

11) Click Next.
12) On the Authentication page, select the Use for Authentication checkbox to enable the Active Directory to work as an authentication source.
    i. Select how you want to configure the Authentication source. The following table describes each option.

Option	Description
Authenticate users with Active Directory through the agent	Login to RSA Identity Governance and Lifecycle is authenticated against the configured AD.
Authenticate users via SAML	SAML Authentication is used where SAML standard parameters need to be configured.

Note: Authentication source configured for secured communication must have its SSL certificates configured using the default trust-store approach described in Appendix.

13) Click Next.
14) On the Connector page, select the Configure Connector for Provisioning checkbox to configure a Connector for the Active Database.

    a. Select the Configure Accounts checkbox to configure account related parameters. The following table describes each option.

Field	Description
Account Base DN	The base DN where the user accounts are created.
Account DN Prefix	Attribute as prefix to base DN that forms a complete account distinguishedName.

	Default value : CN
User Object Classes	List of objectClasses to create an account. Default values : 'top','person','organizationalPerson','user'

a. Select the Configure Groups checkbox to configure group related parameters. The following table describes each option.

Field	Description
Group Base DN	The base DN where the groups are to be created.
Group DN Prefix	Attribute as prefix to base DN that forms a complete group distinguishedName. Default value : CN
Group Object Classes	List of objectClasses to create a group Default values : 'top','group'

15) Click Verify to make sure that the provided connection and search parameters are correct.
16) Click Next.
17) On the Confirm Changes page, confirm all of the parameters provided. Click Back if you need to update the parameters.
18) Click Next.
19) On the Change Summary page, review all of the configured components to make sure the directory was created.
20) Click Close.

A new Active Directory is listed on the Directories page.

To edit any of the configurations, click on Directory name from the list and choose the component to be reconfigured.

Creating an Active Directory Connector (Optional)

The Application Wizard provides guidance for creating the RSA Active Directory Connector. Use this section only if you need to create a new RSA Active Directory Connector, which can be configured later with some Application. Use the Application Wizard to get the Application-Connector binding and Account template configurations created.

Prerequisites

You need to add required certificates to the default trust-store. Refer to the SSL certificate configuration section in the Appendix and follow the default trust-store approach for configuring certificates.

Refer to *Manage Endpoint Credentials Using a Password Vault* for the prerequisites of using static or dynamic passwords during collector creation and in the configuration wizard.

Configuration

1) From the main menu, click AFX > Connectors.
2) Click Create Connector.
3) Configure the General tab fields. The following table describes each field.

Field	**Description**
Name	Active Directory Connector
Description	Active Directory Connector
Server	AFX Server
Connector Template	Active Directory
State	Test
Export As Template	Provide name to export Connector Template (Optional)

4) From the Connector Template drop-down list, select Active Directory.
5) Configure the Settings tab fields. The following table describes each field.

Field	Description
Host	Domain controller host name
Port	Port number to the server (Default Non-SSL- 389 and SSL – 636) Note: Connector needs to be configured to use SSL port (default - 636), because it needs write access to AD.
Use SSL	Choose whether to use Secure Sockets Layer (SSL) to connect. By default, traffic is transmitted unsecured. You can make traffic confidential and secure by using SSL. Before you configure SSL, you must first make sure that AD over SSL is enabled on your Active Directory server.

	Note: RSA Identity Governance and Lifecycle 7.0.1 and higher require TLS1.0 or later for SSL communication. Active Directory must be enabled with TLS1.0 or above. RSA Identity Governance and Lifecycle supports TLS1.0, TLS1.1, and TLS1.2. RSA Identity Governance and Lifecycle versions 7.0.1 and higher do not support SSLv3.
Skip Certificate Validation	This is available if Use-SSL is selected. Not recommended for production, but can be used for testing. This option lets the AD server and RSA Identity Governance and Lifecycle communicate without validating the security. **WARNING: This skips SSL certificate validation. RSA does NOT recommend using this option.**
Login Distinguished Name	Administrator login- id with write permission on required tree scope
Static Password	Select this option, if you want to provide the password statically/manually. Fill in the value of password for the AD administrator in the area provided.
Dynamic Password	Select this option to use a configured password vault to manage the endpoint credentials. After you select this option, either select a previously configured password vault profile from the drop-down menu, or click Create Profile to add a new password vault profile to use with this connector. RSA Identity Governance and Lifecycle uses this profile to retrieve the appropriate credentials from the password vault during connector deployment and connection tests.
Account DN Suffix	The base DN where the user accounts are to be created
Group DN Prefix	Attribute as prefix for base DN that forms a complete group distinguishedName Default value : CN
Group DN Suffix	The base DN where the groups are to be created
DN Suffix Mappings	DN Suffix Mappings
LDAP object classes to create account	List of objectClasses to create an account Default values : 'top','person','organizationalPerson','user'

LDAP object classes to create group	List of objectClasses to create a group Default values : 'top','group'
User membership attribute for Group	Attribute that defines the account-group membership Default value : member
Account Lockout Threshold attribute value	A numeric value, security setting that determines the number of failed logon attempts that causes a user account to be locked
Dependent Exchange Connector	Dependent Exchange Connector to provision and de-provision for this configurations If you select the active exchange connector then create an additional AFX input parameter named '`Exchange_Database`' and provide appropriate value.

6) Configure capabilities.
   Note: The Active Directory Connector template has the capabilities set to the Microsoft Active Directory standards. You can modify these settings as required. To modify these settings, seethe mappings provide in the tables below.
7) Save the Connector.
   To test this connector, please wait until the connector status changes to "Running" and then check any capability using the Test Connector Capability button.

The Active Directory Connector supports the following commands:

- Account
  - Create Account on AD server
  - Delete Account from AD server
  - Reset Account's password
  - Add Account to AD Group
  - Remove Account from AD Group
  - Enable Account
  - Disable Account
  - Update Account
  - Move Account
  - Lock Account
  - Unlock Account

- Group
  - Create Group on AD server

- Delete Group from AD server
- Update Group

Create Account on AD server

The following table lists the parameters on the Create an Account screen:

Field Name	Value
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${AccountTemplate.AccountName}
Description	Full DN of account or login name

Field Name	Value
Parameter Name	sAMAccountName.
Type	STRING
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	sAMAccountName
Mapping	${AccountTemplate.sAMAccountName}
Description	Logon name used to support clients and servers running earlier versions of the operating system, such as Windows NT 4.0, Windows 95, Windows 98, and LAN Manager

Field Name	Value
Parameter Name	CN
Type	STRING
Default Value	-

Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Common Name
Mapping	${AccountTemplate.CN}
Description	Name that represents an object. It is used to perform searches

Field Name	**Value**
Parameter Name	sn
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Last Name
Mapping	${AccountTemplate.sn}
Description	Surname of a person

Field Name	**Value**
Parameter Name	givenName
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	First Name
Mapping	${ AccountTemplate.First_Name}
Description	given name of a person

Field Name	**Value**
Parameter Name	mail
Type	STRING
Default Value	-
Is the parameter required?	Yes

Is the parameter encrypted?	No
Display Name	Email address
Mapping	${ AccountTemplate.Email}
Description	simple SMTP address of a person

Field Name	Value
Parameter Name	Password
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	Yes
Display Name	Initial password to set
Mapping	${AccountTemplate.Password}
Description	password which is required for login

Field Name	Value
Parameter Name	UserAccountControl
Type	STRING
Default Value	-
Is the parameter required?	No
Is the parameter encrypted?	Yes
Display Name	User Account Control(UAC) Value
Mapping	${AccountTemplate.userAccountControl}
Description	UAC description

Delete Account from AD server

The following table lists the parameters on the Delete an Account screen:

Field Name	Value
Parameter Name	Account
Type	STRING
Default Value	-

Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.External_Id}
Description	Full DN of account or login name

Reset Account's Password

The following table lists the parameters on the Reset Password screen:

Field Name	Value
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.External_Id}
Description	Full DN of account or login name

Field Name	Value
Parameter Name	Password
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	Yes
Display Name	Initial password to reset to
Mapping	${AccountPassword}
Description	New password to reset an old password

Add Account to Group

The following table lists the parameters on the Add Account to Group screen:

Field Name	Value
Parameter Name	Account
Type	STRING

Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.External_Id}
Description	Full DN of account or login name

Field Name	**Value**
Parameter Name	Group
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group DN or Group Name
Mapping	${Group.External_Id}
Description	Full DN of group or group name

Remove Account from Group

The following table lists the parameters on the Remove Account from Group screen:

Field Name	**Value**
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.External_Id}
Description	Full DN of account or login name

Field Name	**Value**
Parameter Name	Group
Type	STRING
Default Value	-
Is the parameter required?	Yes

Is the parameter encrypted?	No
Display Name	Group DN or Group Name
Mapping	${Group.External_Id}
Description	Full DN of group or group name

Enable Account

The following table lists the parameters on the Enable an Account screen:

Field Name	Value
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.External_Id}
Description	Full DN of account or login name

Disable Account

The following table lists the parameters on the Disable an Account screen:

Field Name	Value
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.External_Id}
Description	Full DN of account or login name

Update Account

The following table lists the parameters on the Update an Account screen:

Field Name	Value

Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.External_Id}
Description	Full DN of account or login name

Field Name	**Value**
Parameter Name	userAccountControl
Type	STRING
Default Value	NA
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	User Account Control(UAC) Value
Mapping	N/A
Description	User Account Control (UAC) Value. Please refer to table UAC values mentioned in Appendix. Provide appropriate string or combinations from table, such as 1. ACCOUNTDISABLE can be provided to disable an account, 2.“NORMAL_ACCOUNT,DONT_EXPIRE_PASSWORD” can be provided to enable an account which is in disabled state and to set flag as password never expires

Move Account

The following table lists the parameters on the Move an Account screen:

Field Name	**Value**
Parameter Name	Account
Type	STRING
Default Value	-

Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.External_Id}
Description	Full DN of account or login name

Field Name	**Value**
Parameter Name	NewParentDN
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	New Parent's DN
Mapping	Null
Description	DN of new account base or organizational unit

Lock an Account

The following table lists the parameters on the Lock an Account screen:

Field Name	**Value**
Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.External_Id}
Description	Full DN of account or login name

Unlock an Account

The following table lists the parameters on the Unlock an Account screen:

Field Name	**Value**

Parameter Name	Account
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.External_Id}
Description	Full DN of account or login name

Create a group

The following table lists the parameters on the Create a Group screen:

Field Name	**Value**
Parameter Name	Group
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	${AccountTemplate.GroupName}
Description	Full DN of group

Field Name	**Value**
Parameter Name	CN
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Common Name
Mapping	${AccountTemplate.GroupName}
Description	Name that represents an object. It is used to perform searches

Field Name	**Value**
Parameter Name	sAMAccountName.

Type	STRING
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	sAMAccountName
Mapping	${AccountTemplate.GroupName}
Description	Logon name used to support clients and servers running earlier versions of the operating system, such as Windows NT 4.0, Windows 95, Windows 98, and LAN Manager

Field Name	**Value**
Parameter Name	groupType
Type	STRING
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	GroupType
Mapping	${AccountTemplate.GroupType}
Description	Set of flags that define the type and scope of a group object

Delete a group

The following table lists the parameters on the Delete a Group screen:

Field Name	**Value**
Parameter Name	Group
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	${Group.External_Id}
Description	Full DN of group

Update a group

The following table lists the parameters on the Update a Group screen:

Field Name	**Value**
Parameter Name	Group
Type	STRING
Default Value	-
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	${Group.External_Id}
Description	Full DN of group

Note: For provisioning a user on Active Directory with the User Access Control (UAC) property, refer to the Characteristics of UAC attribute and UAC table in the Appendix.

Creating Active Directory Collectors

The Application Wizard provides guidance for creating the RSA Active Directory Collectors. Use this section only if you need to create a new RSA Active Directory Collector, which can be configured later with some Application. Use the Application Wizard to get the Application-Collectors-Connector binding and Account template configurations created.

RSA Identity Governance and Lifecycle supports the following collectors for the Active Directory

- Account Data Collector (ADC)
- Identity Data Collector (IDC)
- Entitlement Data Collector (EDC)
- Role Data Collector (RDC)

Configuring an Account Data Collector (ADC)

Manually configure Active Directory Collectors (ADC) without using the Application Wizard.

Refer to *Manage Endpoint Credentials Using a Password Vault* for the prerequisites of using static or dynamic passwords in collector creation and configuration wizard.

1) Log into RSA Identity Governance and Lifecycle instance.
2) Click Collectors > Account Collectors.
3) Click Create Account Collector.
4) On the Collector Description page, configure the parameters. The following table describes each parameter:

Field	Description
Collector Name	Provide unique Collector name
Description	Provide description for this Collector
Business Source	Select available business source to link this Collector with i.e. An application or directory
Data Source Type	Select “Active Directory” from the list
Agent	Select any available Agent
Status	Active or Inactive
Copy From	If there exists a configured Collector and all the parameters can be copied from the existing one, select the same from the list
Schedule	This parameter will help scheduling runs of this Collector instance. On selecting this option, Start and Frequency can be set

5) Click Next.
6) On the Connection page, provide the connection parameters. The following table describes each parameter:

Field	Description
Host	Host Name of machine where AD is installed
Port	Port number to the server (Default Non-SSL- 389 and SSL – 636)

	Note: To collect users/accounts from AD sub-domain from forests, use Global Catalog port i.e. Non-SSL-3268 and SSL-3269. (Refer to the Global catalog Limitations)
Bind DN	Distinguished Name of the user on AD permitted to search the directory within the defined search base. Such as Domain\Administrator
Static Password	Select this option, if you want to provide the password statically/manually. Fill in the value of password for the AD administrator in the area provided.
Dynamic Password	Select this option to use a configured password vault to manage the endpoint credentials. After you select this option, either select a previously configured password vault profile from the drop-down menu, or click Create Profile to add a new password vault profile to use with this connector. RSA Identity Governance and Lifecycle uses this profile to retrieve the appropriate credentials from the password vault during connector deployment and connection tests.
Connection Timeout	The time in milliseconds a collector waits to complete the initial TCP connection handshake before the connection attempt is aborted. It should be greater than zero.
Read Timeout	The time in milliseconds a collector waits to read data after the previous read before the read attempt is aborted. It should be greater than zero.
Page Size	Page size to collect records in paginated form. Default page size is 1000
Ignore Referral	Whether Referral should be ignored or not. If referral is ignored and if a sub-tree search is performed, the search will return all objects within the specified domain that meet the search criteria. The search will also return referrals to any subordinate domains that are direct descendants of the directory server domain. If referrals are not ignored and if a sub-tree search is performed, the underlying LDAP API will automatically attempt to bind to any referrals and add the search results to the result set. If the "Ignore Referral" Checkbox is checked then the RSA Identity Governance and Lifecycle server will NOT need access to the name servers downstream from the Active Directory server.
Use SSL	Choose whether to use Secure Sockets Layer (SSL) to connect. By default, traffic is transmitted unsecured. You can make traffic confidential and secure by using SSL. Before you configure SSL, you must first make sure that AD over SSL is enabled on your Active Directory server.

	Note: RSA Identity Governance and Lifecycle 7.0.1 and higher require TLS1.0 or later for SSL communication. Active Directory must be enabled with TLS1.0 or above. RSA Identity Governance and Lifecycle supports TLS1.0, TLS1.1, and TLS1.2. RSA Identity Governance and Lifecycle versions 7.0.1 and higher do not support SSLv3.
Skip Certificate Validation (if Use SSL is selected)	This is available if Use-SSL is selected. Not recommended for production, but can be used for testing. This option lets the AD server and RSA Identity Governance and Lifecycle communicate without validating the security. **WARNING: This skips SSL certificate validation. RSA does NOT recommend using this option.**
Select Certificate (If Use SSL is selected)	This is available on selecting Use-SSL option. **Recommended approach -** Add required certificates to the default trust-store. Refer the SSL certificate configuration in Appendix; follow the default trust-store approach for configuring certificates. Keep this field blank by not selecting any certificate from dropdown. **Not recommended approach -** A list of valid certificates retrieved from the AD server for given host-port, select one for SSL communication.
Certificate (If Use SSL is selected)	This is available on selecting Use-SSL option, where certificate contents can be copied. **Recommended approach -** Add required certificates to the default trust-store. Refer the SSL certificate configuration in Appendix; follow the default trust-store approach for configuring certificates. Keep this field **blank**.

7) On the Select types of account data to collect" page, select type of data to collect:

Option	Description
Accounts	If selected will collect additional account data described in further steps
User Account Mapping	if selected will collect and map user based on configuration described in further steps
Groups	If selected will collect group data based on configuration described in further steps

8) Click Next.
9) On the Search Configuration for Accounts page, provide the required parameters used to collect Accounts from the Active Directory:

Field	Description
Account Base DN	DN from where to search for accounts
Account Search Scope	Search scope for accounts (can be Subtree or One level)

Account Search Filter	Account Search Filter such as (&(objectCategory=person)(objectClass=user)(sAMAccountName=*))
Account ID	Account ID (such as sAMAccountName)

If you selected Accounts in step7, the following fields appear:

Field	Description
ObjectSID (Optional)	If checked collects ObjectSID, an account attribute for groups' foreign security principle member resolution
Account Disabled	True (Check this to collect disabled accounts. This property will be visible if at directory level 'Allow account disabling' property is set to 'true' i.e. when Business Source is configured appropriately)
Account Locked	True (Check this to collect locked accounts. This property will be visible if at directory level 'Allow account locking' property is set to 'true' i.e. when Business Source is configured appropriately)
Last Login Date (Optional)	lastLogon It collects the last time (mm/dd/yy hh:mm) the user logged on.
Expiration Date (Optional)	accountExpires It collects the date (mm/dd/yy hh:mm) when the account expires.
External ID (Custom Attribute)	distinguishedName
User Access Control	UserAccountControl It is a 4 bytes (32-bit) integer that represents a bitwise enumeration of various flags that controls the behavior of an object. For more information regarding the flags, refer the list of available property flags described in UAC values in Appendix

If you selected User attribute mapping in step7, the following fields appear

Field	Description
UserId	User Id (such as objectGUID)

10) Click Next.
11) If you selected Groups in step 7, the Group Data page appears.

Field	Description
Group Base DN	DN for group search
Group Search Scope	Search scope for groups (can be Sub-tree or One level)
Group Search Filter	Search filter enables you to define search criteria, provide the filter to search for groups effectively (for example: (objectClass=group))
Group ID/Name	Unique attribute to be collected (such as samAccountName)

ObjectSID (Optional)	If checked collects ObjectSID, an account attribute for groups' foreign security principle member resolution
Collect Primary Group Members (Optional)	If checked, it collects the primary group members.
Collect Dynamic Group Members (Optional)	If checked, collects the members which are dynamically part of group based on the filter defined for each group

The Attribute GUID (the global unique identifier which is used to identify any object uniquely in Active Directory) is collected along with previously mapped attributes.

If the attributes to be collected are not available in RSA Identity Governance and Lifecycle, you can add then custom attributes. To add a custom attribute:

a) Click "Admin" on the menu ribbon
b) Select "Attributes"
c) Select "Account/Group"
d) Click "Edit" and add the new attribute
e) Save the attribute

12) Click Next.
13) On the Edit User Resolution Rules page, map the user and the account being collected.

Field Name	Value
Target Collector	<Any created LDAP IDC. (Default: Users)>
User Attribute	<Unique attribute for mapping. (Default: Unique Id)>

Note: Modifying these reference resolution rules results in complete processing of data and the relationships. This is the user attribute of the users collected from the configured LDAP IDC and is used for mapping with accounts collected. Change this attribute results in new user-account mappings on the next collection run.

14) Click Next.
15) On the Edit Member Account Resolution Rules page, configure an unique attribute from Account to define membership:

Field Name	Value
Target Collector	<AD Account Data Collector>
Account Attribute	<Account Name> Default External_Id

Note: Modifying these reference resolution rules results in complete processing of data and the relationships. This is the account attribute for accounts to be collected from the ADC and is used for mapping with users collected from the IDC. Changing this attribute results in new user-account mappings on the next collection run.

16) Click Next.
17) On the Edit Sub-group Resolution Rules page, configure the sub-group resolution attributes to define the group membership with accounts collected:

Field Name	Value
Target Collector	<AD Account Data Collector>
Group Attribute	<Name> Default External_Id

Note: Modifying these reference resolution rules results in complete processing of data. This attribute defines the uniqueness and the membership in RSA Identity Governance and Lifecycle for groups. If you change this attribute, the membership is processed on the next collection run.

18) Click Finish to save all the settings.
19) Click Finish.

Configuring an Identity Data Collector (IDC)

Refer to *Manage Endpoint Credentials Using a Password Vault* for the prerequisites of using static or dynamic passwords during collector creation and in the configuration wizard.

1) Click Collectors > Identity Collectors.
2) Click on Create Identity Collector.
3) On the Collector Description page, configure parameters.

Field	Description
Collector Name	Provide unique Collector name
Description	Provide description for this Collector
Data Source Type	Select “Active Directory” from the list
Agent	Select any available Agent
Directory	Select configured Directory from the list
Status	Active or Inactive
Copy From	If there exists a configured Collector and all the parameters can be copied from the existing one, select the same from the list
Schedule	This parameter will help scheduling runs of this Collector instance. On selecting this option, Start and Frequency can be set

4) Click Next.
5) On the “Connection” page, provide connection parameters.

Field	Description
Host	Host Name of machine where AD is installed
Port	Port number to the server (Default Non-SSL- 389 and SSL – 636)

	Note: To collect users/accounts from AD sub-domain from forests, use Global Catalog port i.e. Non-SSL-3268 and SSL-3269. (Refer to the Global Catalog Limitations)
Bind DN	Distinguished Name of the user on AD permitted to search the directory within the defined search base such as Domain\Administrator
Static Password	Select this option to provide the password statically/manually. Enter the password for the AD administrator in the area provided.
Dynamic Password	Select this option to use a configured password vault to manage the endpoint credentials. After you select this option, either select a previously configured password vault profile from the drop-down menu, or click Create Profile to add a new password vault profile to use with this connector. RSA Identity Governance and Lifecycle uses this profile to retrieve the appropriate credentials from the password vault during connector deployment and connection tests.
Page Size	Page size to collect records in paginated form. Default Paging Size is 1000
Ignore Referral	Whether Referral should be ignored or not. If referral is ignored and if a sub-tree search is performed, the search returns all objects within the specified domain that meet the search criteria. The search also returns referrals to any subordinate domains that are direct descendants of the directory server domain. If referrals are not ignored and if a sub-tree search is performed, the underlying LDAP API automatically attempts to bind to any referrals and add the search results to the result set. If the "Ignore Referral" checkbox is checked then the RSA Identity Governance and Lifecycle server will NOT need access to the name servers downstream from the Active Directory server.
Use SSL	Choose whether to use Secure Sockets Layer (SSL) to connect. By default, traffic is transmitted unsecured. You can make traffic confidential and secure by using SSL. Before you configure SSL, you must first make sure that AD over SSL is enabled on your Active Directory server. Note: RSA Identity Governance and Lifecycle 7.0.1 and higher require TLS1.0 or later for SSL communication. Active Directory must be enabled with TLS1.0 or above. RSA Identity Governance and Lifecycle supports TLS1.0, TLS1.1, and TLS1.2. RSA Identity Governance and Lifecycle versions 7.0.1 and higher do not support SSLv3.

Skip Certificate Validation (If Use SSL is selected)	This is available if Use-SSL is selected. Not recommended for production, but can be used for testing. This option lets the AD server and RSA Identity Governance and Lifecycle communicate without validating the security. **WARNING: This skips SSL certificate validation. RSA does NOT recommend using this option.**
Select Certificate (If Use SSL is selected)	This is available on selecting Use-SSL option. **Recommended approach -** Add required certificates to the default trust-store. Refer the SSL certificate configuration in Appendix; follow the default trust-store approach for configuring certificates. Keep this field blank by not selecting any certificate from dropdown. **Not recommended approach -** A list of valid certificates retrieved from the AD server for given host-port, select one for SSL communication.
Certificate (If Use SSL is selected)	This is available on selecting Use-SSL option, where certificate contents can be copied. **Recommended approach -** Add required certificates to the default trust-store. Refer the SSL certificate configuration in Appendix; follow the default trust-store approach for configuring certificates. Keep this field **blank**.

6) Click Next.
7) On the Select types of identity data to collect page, select Users.
8) Click Next.
9) On the Mapping for user attributes” panel, enter the user data:

Field	Description
User Base DN	DN from where to search for users
User Search Scope	Search scope for accounts (can be Sub-tree or One level)
User Search Filter	Search filter enables you to define search criteria, provide the filter to search for users effectively (for example: (objectClass=inetOrgPerson))
User ID	User ID such as CN
Department	Department
Email Address	Mail
First Name	givenName
Title	Title
UniqueID	distinguishedName
Last Name	Sn
Supervisor	Manager

Note: If the custom attribute is not present in RSA Identity Governance and Lifecycle, custom attributes can be added.

To add custom attribute,

a. Click Admin on the menu ribbon.
b. Select Attributes.
c. Select Account/Group
d. Click Edit and add the new attribute.
e. Save the attribute.

10) Click Finish to save all the provided parameters.

Configuring an Entitlement Data Collector (EDC)

Refer to *Manage Endpoint Credentials Using a Password Vault* for the prerequisites of using static or dynamic passwords during collector creation and in the configuration wizard.

1) Click Collectors > Entitlement Collectors.
2) Click Create Entitlement Collector.
3) On the Collector Description panel, configure the parameters.

Field	Description
Collector Name	Provide unique Collector name
Description	Provide description for this Collector
Business Source	Select available business source to link this Collector with
Data Source Type	Select “Active Directory” from the list
Agent	Select any available Agent
Status	Active or Inactive
Copy From	If other Collectors are exists and all the parameters can be copied from the existing one then select Collector from the drop down
Schedule	This parameter will help scheduling runs of this Collector instance. On selecting this option, Start and Frequency can be set

4) Click Next.
5) On the Connection page, configure the connection parameters.

Field	Description
Host	Host Name of machine where AD is installed
Port	Port number to the server (Default Non-SSL- 389 and SSL – 636) Note: To collect users/accounts from AD sub-domain from forests, use Global Catalog port i.e. Non-SSL-3268 and SSL-3269. (Refer to the Global Catalog Limitations)
Bind DN	Distinguished Name of the user on AD permitted to search the directory within the defined search base
Static Password	Select this option to provide the password statically/manually. Enter the password for the AD administrator in the area provided.

Dynamic Password	Select this option to use a configured password vault to manage the endpoint credentials. After you select this option, either select a previously configured password vault profile from the drop-down menu, or click Create Profile to add a new password vault profile to use with this connector. RSA Identity Governance and Lifecycle uses this profile to retrieve the appropriate credentials from the password vault during connector deployment and connection tests.
Page Size	Page size to collect records in paginated form
Ignore Referral	Whether Referral should be ignored or not. If referral is ignored and if a sub-tree search is performed, the search returns all objects within the specified domain that meet the search criteria. The search also returns referrals to any subordinate domains that are direct descendants of the directory server domain. If referrals are not ignored and if a sub-tree search is performed, the underlying LDAP API automatically attempts to bind to any referrals and add the search results to the result set. If the "Ignore Referral" checkbox is checked then RSA Identity Governance and Lifecycle server will NOT need access to the name servers downstream from the Active Directory server.
Use SSL	Choose whether to use Secure Sockets Layer (SSL) to connect. By default, traffic is transmitted unsecured. You can make traffic confidential and secure by using SSL. Before you configure SSL, you must first make sure that AD over SSL is enabled on your Active Directory server. Note: RSA Identity Governance and Lifecycle 7.0.1 and higher require TLS1.0 or later for SSL communication. Active Directory must be enabled with TLS1.0 or above. RSA Identity Governance and Lifecycle supports TLS1.0, TLS1.1, and TLS1.2. RSA Identity Governance and Lifecycle versions 7.0.1 and higher do not support SSLv3.
Skip Certificate Validation (If Use SSL is selected)	This is available if Use-SSL is selected. Not recommended for production, but can be used for testing. This option lets the AD server and RSA Identity Governance and Lifecycle communicate without validating the security. **WARNING: This skips SSL certificate validation. RSA does NOT recommend using this option.**
Select Certificate	This is available on selecting Use-SSL option.

(if Use SSL is selected)	**Recommended approach -** Add required certificates to the default trust-store. Refer the SSL certificate configuration in Appendix; follow the default trust-store approach for configuring certificates. Keep this field blank by not selecting any certificate from dropdown. **Not recommended approach -** A list of valid certificates retrieved from the AD server for given host-port, select one for SSL communication.
Certificate (If Use SSL is selected)	This is available on selecting Use-SSL option, where certificate contents can be copied. **Recommended approach -** Add required certificates to the default trust-store. Refer the SSL certificate configuration in Appendix; follow the default trust-store approach for configuring certificates. Keep this field **blank**.

6) Click Next.
7) On the Select types of entitlement data to collect page, select what type of entitlement data to collect

Option	Description
Accounts	This is to collect entitlements and relate them to accounts
Collect Groups as Application Roles	This is to collect groups as application roles

8) Click Next.
9) On the Account Data page, configure Attribute Modeling Options.

Field Name	Value
Account Base DN	DN from where to search for accounts
Account Search Scope	Search scope for accounts (can be Sub-tree or One level)
Account Search Filter	Account Search Filter
Account ID	Account ID (such as sAMAccountName)
Collect attribute name values as resource-action pairs	Select this to collect attribute name values as resource action pairs. Specify comma separated attribute names to extract. Attribute Name will be collected as Resource and Corresponding value will be collected as Action.
Collect attribute value as resource	Select this to collect attribute value as resource. Specify comma separated attribute names to extract. Value of the attribute will be collected as Resource and action will be

	NULL. The attribute name will be stored in the custom attribute specified below.
Collect attribute value as application role	Select this to collect attribute value as application role. Specify comma separated attribute names to extract. Value of the attribute will be collected as Application Role. The attribute name will be stored in the custom attribute specified below.
Custom Attribute	Custom attributes created under 'User Entitlements' tab will be listed here.

10) Click Next.
11) If "Collect Groups as Application Roles" is selected in step 7, configure Group Data.

    On Group Data page, configure Mapping of Group Attributes.

Field Name	Mapping
Group Base DN	DN from where to search for groups
Group Search Scope	Search scope for groups (can be Sub-tree or One level)
Group Search Filter	Group Search Filter
Group Id/ Name	Group Id /Name (such as cn)
Member of group	Member of Group Attribute (such as member)

12) Click Finish.

Configuring a Role Data Collector (RDC)

1) Click Collectors > Role Collectors.
2) Click on Create Role Collector.
3) On the Collector Description page, complete the parameters.

Field	Description
Collector Name	Provide unique Collector name
Description	Provide description for this Collector
Role Set	Select available role set from the list
Data Source Type	Select "Active Directory" from the list
Agent	Select any available Agent
Status	Active or Inactive
Has Data	If true, the members of these roles will automatically get the entitlements of these roles
Schedule	This parameter will help scheduling runs of this Collector instance. On selecting this option, Start and Frequency can be set

4) Click Next.

5) On Connection page, configure the connection parameters.

Field	Description
Host	Host Name of machine where AD is installed
Port	Port number to the server (Default Non-SSL- 389 and SSL – 636) Note: To collect users/accounts from AD sub-domain from forests, use Global Catalog port i.e. Non-SSL-3268 and SSL-3269. (Refer to the Global catalog Limitations)
Bind DN	Distinguished Name of the user on AD permitted to search the directory within the defined search base. such as Domain\User
Bind Password	Password to authenticate the user
Connection Timeout	The time in milliseconds a collector waits to complete the initial TCP connection handshake before the connection attempt is aborted. It should be greater than zero.
Read Timeout	The time in milliseconds a collector waits to read data after the previous read before the read attempt is aborted. It should be greater than zero.
Use SSL	Choose whether to use Secure Sockets Layer (SSL) to connect. By default, traffic is transmitted unsecured. You can make traffic confidential and secure by using SSL. Before you configure SSL, you must first make sure that AD over SSL is enabled on your Active Directory server. Note: RSA Identity Governance and Lifecycle 7.0.1 and higher require TLS1.0 or later for SSL communication. Active Directory must be enabled with TLS1.0 or above. RSA Identity Governance and Lifecycle supports TLS1.0, TLS1.1, and TLS1.2. RSA Identity Governance and Lifecycle versions 7.0.1 and higher do not support SSLv3.
Certificate (If Use SSL is selected)	The valid server certificate in PEM format
KeyStore Location (If Use SSL is selected)	The server key-store path to import the above given certificate such as $JAVA_HOME/jre/lib/security/cacerts

6) Click Next.
7) Select the types of data to collect:

Option	Description
Roles	This data is collected by doing a look up on roles and collecting role attributes as users, sub roles and parent roles.
User To Role Membership	This data is collected by doing look up on users and collecting user attributes as roles.

Collect Roles in one of the followings ways.

Following are the steps enlisted for all types of role data collection:

- Role Filter

Parameters	Description
Role Base DN	DN to search for roles objects
Role Search Scope	Search scope to search for role objects
Role Search Filter	Search filter to search for role objects
Unique Role Attribute Name	Name of the attribute from role entry that stores the unique role name or role identifier. This is optional property. Set this property if the role name is to be retrieved from a different attribute in the role entry. If this property is not set, then the default behavior is to collect the role entry DN for the role name.

- Role Members

Parameters	Description
User DN Attributes	Comma separated list of attribute names from role entry that stores the user membership information in DN form. If invalid attribute names are specified, they would be ignored.
Unique User Name Attribute	Name of the attribute from user entry that stores the unique user name or user identifier. This is optional property. Set this property if the user name is to be retrieved from a different attribute in the user entry. If this property is not set, then the default behavior is to collect the given value in user membership attribute (assumed as DN) for the user name.
Unique user Object Classes	Comma separated list of object class names that identify an LDAP entry as a user entry. If any of the object class names is found in the LDAP entry, then it will be considered as a user entry.

- Role Definitions

Parameters	Description
Child Role DN Attributes	Comma separated list of attribute names from role entry that stores the child role membership information in DN form. If invalid attribute names are specified, they would be ignored.
Parent Role DN Attributes	Comma separated list of attribute names from role entry that stores the parent role membership information in DN form. If invalid attribute names are specified, they would be ignored.
Unique Role Object Classes	Comma separated list of object class names that identify an LDAP entry as a role entry. If any of the object class

	names is found in the LDAP entry, then it will be considered as a role entry.
MaxRoleObjectCacheLimit	A numeric value that indicates the max number of role objects that can be cached by this Collector before publishing them. This is an optional property. Default value assumed when this property is not set or set to an invalid value is 100.

- User Filter

Parameters	Description
User Base DN	DN to search for users
User Search Scope	Search Scope
User Search Filter	Search filter to search for users
Unique User Name Attribute	Name of the attribute from user entry that stores the unique user name or user identifier. This is optional property. Set this property if the user name is to be retrieved from a different attribute in the user entry. If this property is not set, then the default behavior is to collect the given value in user membership attribute (assumed as DN) for the user name.

- Roles

Parameters	Description
Role DN Attribute	Comma separated list of attribute names from user entry that stores the user to role membership information in DN form. If invalid attribute names are specified, they would be ignored.
Unique Role Name Attribute	Name of the attribute from role entry that stores the unique role name or role identifier. This is optional property. Set this property if the role name is to be retrieved from a different attribute in the role entry. If this property is not set, then the default behavior is to collect the role entry DN for the role name.
Unique Role Object Classes	Comma separated list of object class names that identify an LDAP entry as a role entry. If any of the object class names is found in the LDAP entry, then it will be considered as a role entry.

8) Click Next.
9) On the Map Collector Attributes to User Entitlement Attributes page, provide the attributes to collect as user entitlements. You can create and map custom attributes, if needed.

10) Click Next.
11) On the Edit User Resolution Rules page, configure the user attribute to resolve the Unique User Name Attribute (Step 7) for the users of the configured IDC.

Field Name	Value
Target Collector	<AD Identity Data Collector>
User Attribute	<User Id>

Note: Modifying these reference resolution rules results in complete processing of data and hence the relationships.

12) Click Finish.

Appendix

Characteristics of User Access Control (UAC) attribute

The UAC attribute defines the characteristics and behavior of the account in Active Directory (AD). Its value can be set by one or more property flags.

UAC values

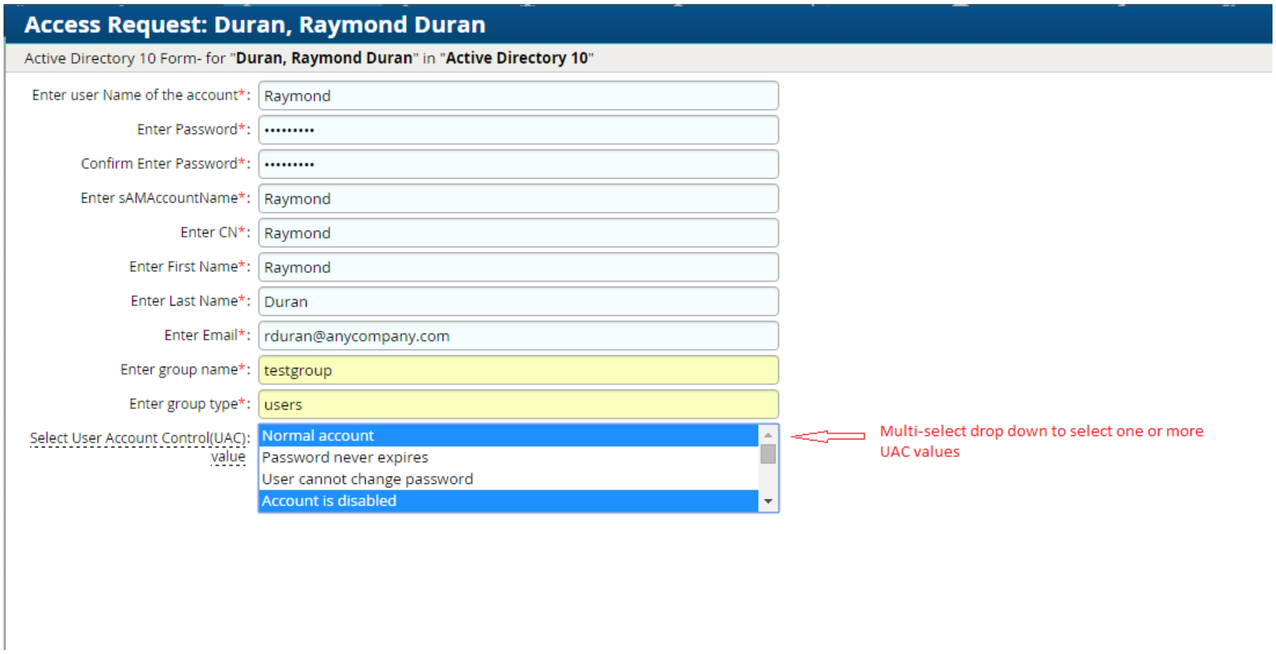
The following table lists the UAC flags along with their values:

Property display name	Property Flag
Account is disabled	ACCOUNTDISABLE
Normal account	NORMAL_ACCOUNT
User cannot change password	PASSWD_CANT_CHANGE
Password never expires	DONT_EXPIRE_PASSWORD
Home directory is required	HOMEDIR_REQUIRED
Store password using reversible encryption	ENCRYPTED_TEXT_PWD_ALLOWED
Smartcard required for logon	SMARTCARD_REQUIRED
Trusted for Kerberos delegation	TRUSTED_FOR_DELEGATION
Account is sensitive and cannot be delegated	NOT_DELEGATED
Use Kerberos DES encryption types for this account	USE_DES_KEY_ONLY
Kerberos pre-authentication not required	DONT_REQ_PREAUTH
Enabled for delegation	TRUSTED_TO_AUTH_FOR_DELEGATION

Note: These property flags are associated with the account options that can be enabled. For example, options like “User cannot change password”, “Password never expires”, and “Account is disabled” can be enabled for an account by providing the property flags to the “UAC” attribute.

In RSA Identity Governance and Lifecycle, when creating a user account on the Active Directory, you can select the enabled account options through a multi-select drop-down. To select the values for a UAC attribute:

1) Click Resources **>** Directories.
2) Select the Active Directory instance created through the Application Wizard.
3) Go to the Accounts tab.
4) Select Create Account to create a request to provision a user on AD.
5) The Access Request wizard shows the list of users. Select the user to provision.
6) Click Next.
7) Add the description, if any, for the selected user.
8) Click Next.
9) An Account template form appears shows the attributes needed for provisioning. It contains a multi-select dropdown for the UAC with display names for the property flags.



Access Request: Duran, Raymond Duran

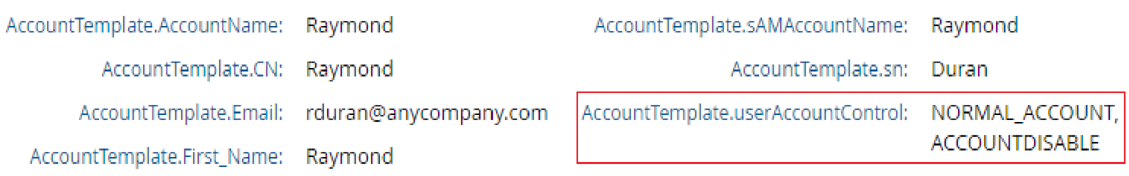
Active Directory 10 Form- for "**Duran, Raymond Duran**" in "**Active Directory 10**"

Enter user Name of the account*:	Raymond
Enter Password*:	•••••••••
Confirm Enter Password*:	•••••••••
Enter sAMAccountName*:	Raymond
Enter CN*:	Raymond
Enter First Name*:	Raymond
Enter Last Name*:	Duran
Enter Email*:	rduran@anycompany.com
Enter group name*:	testgroup
Enter group type*:	users
Select User Account Control(UAC): value	Normal account Password never expires User cannot change password Account is disabled

Multi-select drop down to select one or more UAC values

10) Click Finish.

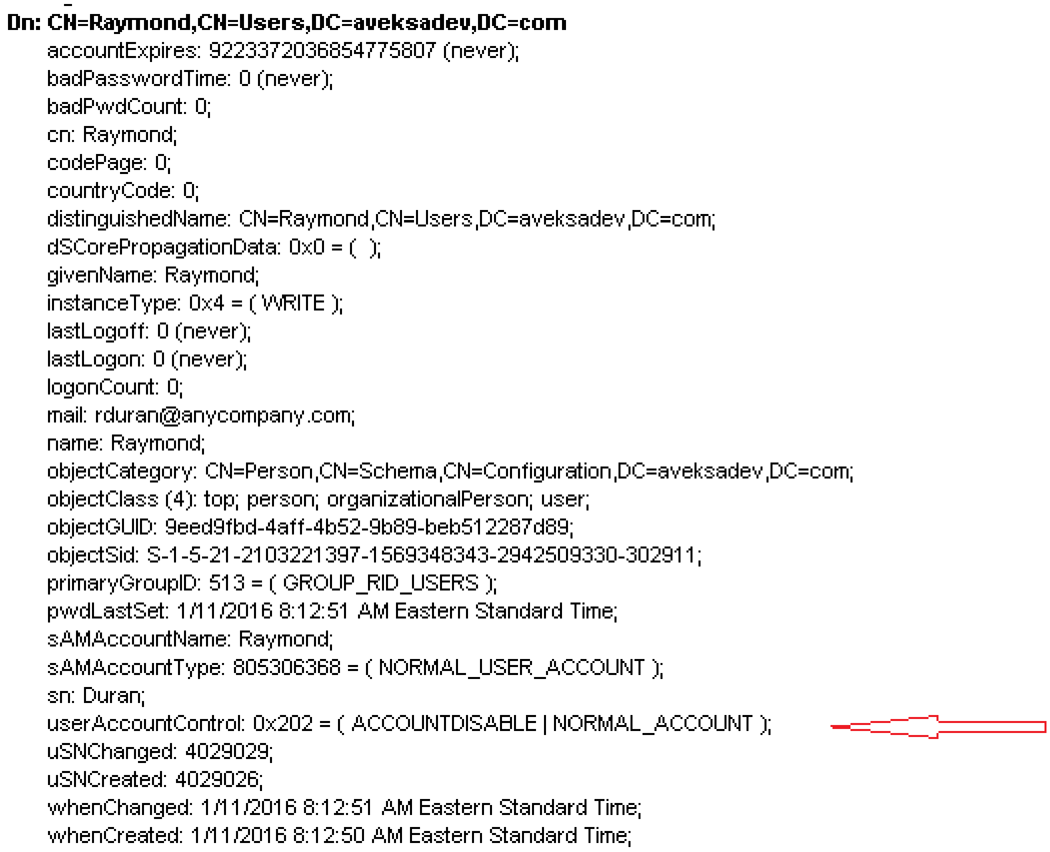
The request is initiated. To view the request details select the Requests > Requests tab. The UAC property values are shown in AccountTemplate.userAccountControl.



AccountTemplate.AccountName:	Raymond	AccountTemplate.sAMAccountName:	Raymond
AccountTemplate.CN:	Raymond	AccountTemplate.sn:	Duran
AccountTemplate.Email:	rduran@anycompany.com	AccountTemplate.userAccountControl:	NORMAL_ACCOUNT, ACCOUNTDISABLE
AccountTemplate.First_Name:	Raymond		

The AFX handler processes the request and creates a new user account in Active Directory.

The user account details obtained from AD are shown below.



```
Dn: CN=Raymond,CN=Users,DC=aveksadev,DC=com
    accountExpires: 9223372036854775807 (never);
    badPasswordTime: 0 (never);
    badPwdCount: 0;
    cn: Raymond;
    codePage: 0;
    countryCode: 0;
    distinguishedName: CN=Raymond,CN=Users,DC=aveksadev,DC=com;
    dSCorePropagationData: 0x0 = (  );
    givenName: Raymond;
    instanceType: 0x4 = ( WRITE );
    lastLogoff: 0 (never);
    lastLogon: 0 (never);
    logonCount: 0;
    mail: rduran@anycompany.com;
    name: Raymond;
    objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=aveksadev,DC=com;
    objectClass (4): top; person; organizationalPerson; user;
    objectGUID: 9eed9fbd-4aff-4b52-9b89-beb512287d89;
    objectSid: S-1-5-21-2103221397-1569348343-2942509330-302911;
    primaryGroupID: 513 = ( GROUP_RID_USERS );
    pwdLastSet: 1/11/2016 8:12:51 AM Eastern Standard Time;
    sAMAccountName: Raymond;
    sAMAccountType: 805306368 = ( NORMAL_USER_ACCOUNT );
    sn: Duran;
    userAccountControl: 0x202 = ( ACCOUNTDISABLE | NORMAL_ACCOUNT );
    uSNChanged: 4029029;
    uSNCreated: 4029026;
    whenChanged: 1/11/2016 8:12:51 AM Eastern Standard Time;
    whenCreated: 1/11/2016 8:12:50 AM Eastern Standard Time;
```

Note: Account data collection does not currently collect the PASSWD_CANT_CHANGE UAC due to a major performance impact.

SSL certificate configuration

For secure communication with Active Directory, the required certificates must be configured for RSA Identity Governance and Lifecycle. If there is a chain of certificates involved in the SSL handshake, the complete certificate chain (leaf up to the root) must be configured.

In RSA Identity Governance and Lifecycle, there are two approaches to configure the SSL certificate:

- Adding server certificates to default trust-store.
- Certificate provided in the CollectorApplicationwizard.

Adding server certificates to the default trust store

For java the default trust-store is either /lib/security/jssecacerts or /lib/security/cacerts (in the active java installation area). Complete the procedure for your application server, below:

WildFly

1. Download/retrieve ActiveDirectory and Certificate Authority (only if required) certificates in PEM format and save them at some location.
2. Add certificates in cacerts by using the keytool command:

```
keytool -import -file <certificate.pem> -alias <certificate_alias> -keystore
<JAVA_HOME>/jre/lib/security/cacerts –storepass changeit
```

3. To restart the server run these commands:
   afx stop
   acm stop
   acm start
   afx start

WebSphere

1. Log in to the WebSphere console using your host name:
   http://<HOST_NAME>:9060/ibm/console/login.do
2. In left panel, expand the Security menu.
3. Click SSL certificate and click key management.
4. Under Configuration Settings, click ‘Manage endpoint security configurations’.
5. Select Outbound properties for the appropriate node.
6. Click the appropriate node link to get the properties.
7. Under Related Items, click Key stores and certificates and click the NodeDefaultTrustStore.

   For a cluster, select the CellDefaultTrustStore instead of the particular NodeDefaulttrustStore.

8. Under Additional Properties, click Signer certificates and click Retrieve from Port.
9. In the Host field, enter: <your_active_directory_host_name>; in the Port field, enter the SSL port configured (default is 636), and in the Alias field, enter <active_directory_cert>.
10. Click Retrieve Signer Information.
11. Verify that the certificate information is for a certificate that you can trust.
12. Click Apply and click Save.
13. Log into the WebSphere machine using SSH (such as putty).
14. At command prompt, run: /home/oracle/AFX/afx stop.
15. At command prompt, run: /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1.
16. At command prompt, run: /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1.
17. At command prompt, run: /home/oracle/AFX/afx start.

WebLogic

1. Download/retrieve ActiveDirectory and Certificate Authority (only if required) certificates in PEM format and save them at some location.
2. Log in to WebLogic Administrative console. (http://<HOST_NAME>.aveksa.local:7001/console/login/LoginForm.jsp)
3. Under Domain Configuration, click the Servers link in the Environment.
4. Click Aveksa Server.
5. Click the SSL tab
6. Click Advanced.
7. Set HostName to 'Verification = None'
8. Save the settings.
9. Log into the WebLogic machine using SSH (such as putty).
10. Change directory: cd /home/oracle/
11. Add active_directory_certificate.pem and authority (such as emc.pem, only if required) certificates in the server.keystore by using keytool :
    keytool -import -file <certificate.pem> -alias <certificate_alias> -keystore server.keystore

12. Restart SSL on WebLogic Server:
    a. Go to Servers > controls tab
    b. Select/check aveksaServer(admin) and then click Restart SSL.
13. Restart the Server:
    a. /home/oracle/AFX/afx stop
    b. Run /path/to/weblogic/user_projects/domains/aveksaDomain/bin/stopWebLogic.sh
    c. Run /path/to/weblogic/user_projects/domains/aveksaDomain/bin/startWebLogic.sh
    d. /home/oracle/AFX/afx start

The trust-store location can be overridden by setting the javax.net.ssl.trustStore system property. Application servers might set this property (as part of an application installation) to redirect or override the trust-store location to one specific to an installed application. This allows the trust-store to be different for each application/jvm managed by the application server.

This is the recommended default trust-store option when configuring secure communication. When using this option, note of following:

- If the Collector Application Wizard has an option for providing certificate information, leave the certificate selection and text box content EMPTY. This forces use of the common default trust-store. In many cases, this default trust-store will contains the correct root/trusted certificates. If the collector does not have this option, follow the above steps to import the certificates to the trust-store for your application server.

- In the cases where the default trust-store does NOT yet contain all certificate information, then you must modify the default trust-store to add the missing certificates following the steps for your application server.

Notes:

1. The Active Directory connector must have its SSL certificates configured using this approach only.
2. Authentication source configured for secured communication must have its SSL certificates configured using this approach only.

Certificate provided in the Collector Application wizard

It is strongly recommended that option 1, the default trust-store setup option, always be used in all environments.

If this option must be used then be aware of the following:

- The certificate should be in PEM format.
- You can select the certificate from the Select Certificate list (which is in PEM format) or you can add its contents (in PEM format from external source) in the Certificate field. If the certificate box is left empty, then the default trust-store (option 1 above) is used; otherwise, a private trust-store using the certificate provided is used.
- You should select the root certificate from the drop-down and not the leaf/ end user certificate (if present). Selecting the root allows for more "flexible" validation. For example, if a leaf certificate changes on the server side (is updated for security reasons or expires, and so on):

  If you originally set up the collector using the leaf certificate (which has now been changed on the server), then any attempted link/ validation will fail as the new certificate is not trusted (new leaf certificate doesn't match old leaf certificate which is stored in the trust-store). You will have to reconfigure the collector to validate against the new certificate.

If you had originally set up the collector using the root certificate, the link/validation will succeed since the new leaf certificate can be validated "up the chain" to the root certificate. Choosing the root provides a better longer term validation solution.

Multi-Domain configuration

Domain

Domains are container objects. Domains are a collection of administratively defined objects that share a common directory database, security policies, and trust relationships with other domains. In this way, each domain is an administrative boundary for objects. A single domain can span multiple physical locations or sites and can contain millions of objects.

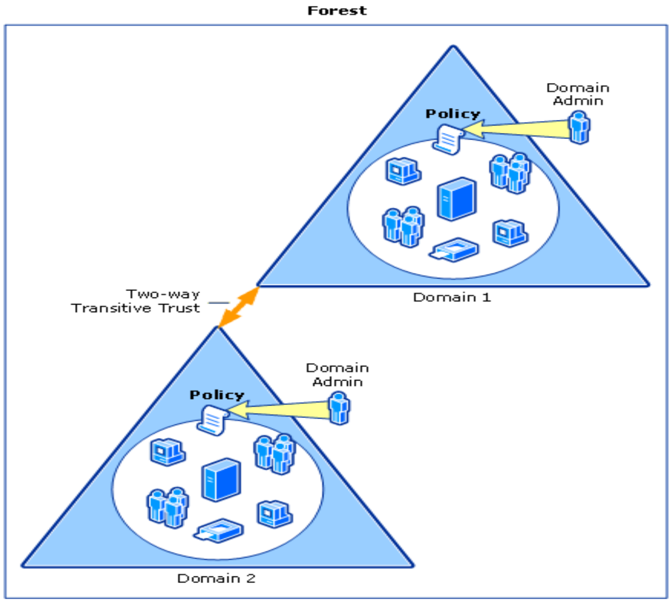
Domain Trees

Domain trees are collections of domains that are grouped together in hierarchical structures. When you add a domain to a tree, it becomes a child of the tree root domain. The domain to which a child domain is attached is called the parent domain.

Forest

A forest is a complete instance of Active Directory. Each forest acts as a top-level container in that it houses all domain containers for that particular Active Directory instance. A forest can contain one or more domain container objects, all of which share a common logical structure, global catalog, directory schema, and directory configuration, as well as automatic two-way transitive trust relationships. The first domain in the forest is called the forest root domain.

This diagram shows a forest configuration with two disjoint domains:



When a new domain tree is created in an existing Forest, a two-way, transitive tree root trust is established by default.

Limitations of using global catalog for AD forest search

a) The Global Catalog contains the partial replica of every naming context in the forest. It also contains the schema and configuration naming contexts. This means the Global Catalog holds a replica of every object in the directory but ***with only a small number of their attributes***.

   To identify the attributes which are marked for replication, the below query can be used:

   Consider, ‘dc=domain,dc=com’ is the domain controller that houses the Schema Master role for the forest.
   Basedn : CN=Schema,CN=Configuration,dc=domain,dc=com

Filter: (&(objectClass=attributeSchema)(isMemberOfPartialAttributeSet=TRUE))

To extend the replication schema (marking new attributes for replication) to global catalog, refer https://blogs.technet.microsoft.com/scotts-it-blog/2015/02/28/ad-ds-global-catalogs-and-the-partial-attribute-set/

b) Though the Global Catalog holds a partial copy of every group in the forest, the *member* attribute of a group is replicated to the global catalog for only ‘Universal group’ objects and not for global groups or domain local groups. Therefore, connecting to the global catalog always locates the user’s membership only in Universal groups.
However, connecting to the global catalog does not locate the user membership in global groups or domain local groups, unless the global catalog server happens to be an authoritative domain controller for the user’s domain.

Scenario

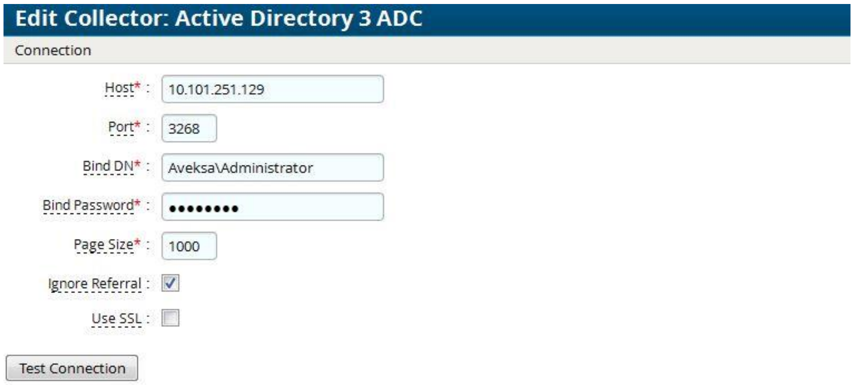
Now, when configuring the Active Directory Collector for one domain, like Domain1, the resources of Domain2 can be fetched and processed by specifying the Base DN of Domain2 in the search configuration.

Consider the following,

Let Domain1 be “aveksa.com”(DC=aveksa,DC=com) and Domain2 be “rsa.net” (DC=rsa,DC=net)

To configure RSA Identity Governance and Lifecycle ADC to collect data from Domain2 using the Domain1 administrator:

1. On the connection page, enter the connection parameters of Domain1, for example aveksa.com. Make sure the port used is the Global Catalog port, for example default non-SSL-3268 and SSL-3269.



Edit Collector: Active Directory 3 ADC

Connection

Host* : 10.101.251.129

Port* : 3268

Bind DN* : Aveksa\Administrator

Bind Password* : ••••••••

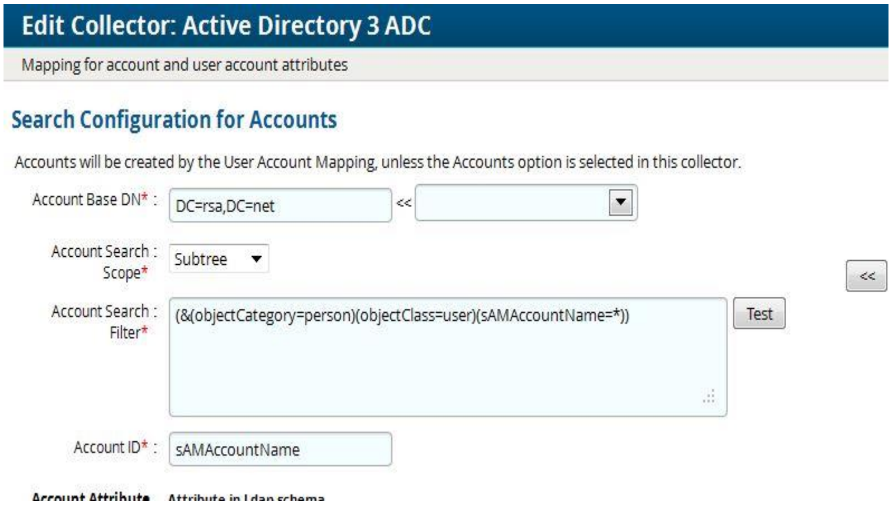
Page Size* : 1000

Ignore Referral : ☑

Use SSL : □

2. On the “Mapping for account and user account attributes” configuration page,

Under Accounts Base DN, enter the BaseDN or OU to search for the users of Domain2: rsa.net (DC=rsa,DC=net). For the rest of the configuration, use the default values or change as required.



Edit Collector: Active Directory 3 ADC

Mapping for account and user account attributes

Search Configuration for Accounts

Accounts will be created by the User Account Mapping, unless the Accounts option is selected in this collector.

Account Base DN* : DC=rsa,DC=net

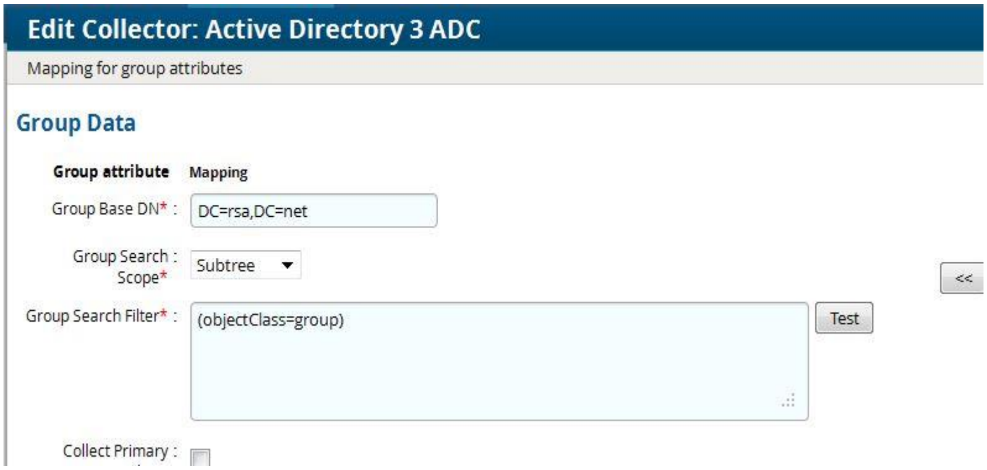
Account Search Scope* : Subtree

Account Search Filter* : (&(objectCategory=person)(objectClass=user)(sAMAccountName=*))

Account ID* : sAMAccountName

Account Attribute   Attribute in Ldap schema

3. On the “Mapping for group attributes” configuration page, under Group Base DN, enter the BaseDN or OU to search for groups of Domain2: rsa.net (DC=rsa,DC=net). For the rest of the configuration, use the default values or change as required.



Edit Collector: Active Directory 3 ADC

Mapping for group attributes

Group Data

Group attribute   Mapping

Group Base DN* : DC=rsa,DC=net

Group Search Scope* : Subtree

Group Search Filter* : (objectClass=group)

Collect Primary : □

This configured ADC collects accounts and groups data from Domain2: rsa.net

Note:

1. For disjoint domain resource collection, use the Global Catalog port. Default non-SSL-3268 and SSL-3269.

2. With the above configuration for data collection in the Active Directory forest, users/accounts/groups with limited attributes (which are marked for replication in schema) and memberships for only Universal groups (not global groups/domain local groups) will be collected.

Troubleshooting

This section describes common errors when configuring the RSA Identity Governance and Lifecycle components for Active Directory and solutions.

- Dynamic password is used on connector settings page and the connector is not getting deployed with error displayed as: *Password Vault Error*.

This may happen if there is an error in retrieving the password using the mentioned profile. You need to check if the values provided in the profile for password retrieval are valid and adequate permissions are present on the vault for fetching the password.

- java.net.UnknownHostException

The UnknownHostException occurs when: host name is incorrect, Active Directory server is not accessible from the RSA Identity Governance and Lifecycle instance, or network connectivity is not available.
To verify the host name, use the “ping <host name/IP>” command.

- SSLHandshakeException

javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target

If the certificate is not provided in the UI or selected when configuring the Active Directory wizard/Collectors with UseSSL, then the server certificate should be imported in the default trust-store depending on the JVM or application server.

Refer to the SSL Certificate configuration in the Appendix for more details.

- *com.aveksa.common.ConnectionException: There was an error establishing a connection with the LDAP directory. Please confirm the settings are correct.*

Analyze the aveksaServer.log and look for the following line:
java.security.cert.CertificateException: No subject alternative names matching xxxxxxxx found

The JRE has been upgraded to 1.8.0_181 in 7.1.1. By default, JRE versions 1.8.0_181 and greater enforce endpoint identification on LDAPS connections to improve the robustness of the connections. After upgrading, Active Directory collectors that use SSL that were previously able to connect might be unable to connect. If this occurs, ensure that the certificate of the host configured in the collector settings has the correct subject alternative name attributes available that match the hostname.

- Refer to the logs for troubleshooting,
  - For Connector logs, see mule_ee.log and mule.AFX-CONN-<Connector-Endpoint>.log at {AFX_HOME}/mule/logs.
  - For Collector logs, see aveksaServer.log at {WILD-FLY_HOME}/standalone/log

To enable additional connector debug logs, follow the below steps:

1. Modify the log4j.xml at {AFX_HOME}/mule/apps/AFX-CONN-<Connector-Endpoint>/classes/
2. Locate the following and change the level to **DEBUG** and save the changes

```
<logger name="org.mule">
    <level value="DEBUG"/>
  </logger>


  <logger name="org.mule.transport.ldapx">
    <level value="DEBUG"/>
  </logger>


  <logger name="com.novell.ldap">
    <level value="DEBUG"/>
        </logger>
```

1. Enable Logs enabled in mule.AFX-CONN-<Connector-Endpoint>.log at {AFX_HOME}/mule/logs.

- If you have configured Active Directory connector with dependent exchange connector and create account capability gets successful, but the account/mailbox is not created on the selected exchange instance.

  Refer dependent exchange connector logs for the detailed error message.

  - For connector logs, see esb.AFX-CONN-<Exchange-Connector-Name>.log at {AFX_HOME}/esb/logs.