



One Identity Active Roles 8.0 LTS

Solutions Guide

Copyright 2022 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC.

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

 **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

Active Roles Solutions Guide
Updated - October 2022
Version - 8.0 LTS

Contents

Active Roles Solutions Overview	8
Exchange Resource Forest Management	9
Configuration Transfer Wizard Solution	10
What's new in version 8.0 LTS	10
Solution components	10
Configuration Collection wizard	11
Configuration Deployment wizard	11
ARSconfig command-line tool	11
Installing the solution	11
Installation requirements	11
Installation procedure	12
Using the solution	12
General considerations	12
About dangling links	14
Using the Collection wizard and Deployment wizard	14
Using the ARSconfig command-line tool	15
Syntax	16
Parameters	16
Scenario: Transfer Active Roles configuration	18
Scenario: Rolling back the configuration changes	20
Known issues	21
Active RolesSPML Provider	24
Features	24
Use scenarios	25
Basic concepts and definitions	25
How SPML Provider works	26
System requirements	28
Hardware requirements	28
Software requirements	28
Web Server requirements	29

Configuring Active RolesSPML Provider	30
Configuration settings in SPML.Config	30
Sample configuration file	32
Extending the SPML Provider schema	33
Using Active RolesSPML Provider	33
Operation mode	34
Support for Active Roles controls	34
Sending controls to the Active Roles Administration Service	35
Specifying controls to return to the SPML Provider client	36
Sample SPML request	36
SPML request	37
SPML response	37
Supported Azure Features	39
Supported operations	42
Samples of use	44
Configuration settings in sample.config	44
Core Operation samples	45
Capability samples	51
Active RolesSPML Provider terminology	58
Troubleshooting SPML Provider	60
Cannot remove the specified item because it was not found in the specified Collec- tion	60
Resolution	60
Some of the specified attributes for the '<object class name>' object class are not defined in the schema	61
Resolution	61
What's new	62
Skype for Business Server Solution	63
Introducing Skype for Business Server User Management	63
Supported Active Directory topologies	64
Single forest	65
Multiple forests - Resource forest	65
Multiple forests - Central forest	65
User Management policy	66
User Management policy settings	67

Connection to Skype for Business Server	67
SIP user name generation rule	68
SIP domain restriction rule	69
Pool restriction rule	69
Telephony restriction rule	70
Master Account Management policy	70
Master Account Management policy settings	71
Skype for Business Server forest mode	71
Container for new shadow accounts	72
Default description for new shadow accounts	72
Attribute to store a reference to shadow account	72
Synchronized properties	72
Substituted properties	73
Back-synchronized properties	74
Master Account Management policy actions	74
Scheduled synchronization	76
Access Templates for Skype for Business Server	76
Deploying the Solution	79
Prerequisite conditions	79
Skype for Business Server deployment	79
Active Roles deployment	80
Deployment in a single-forest environment	81
Deployment in a multi-forest environment	82
Apply the Master Account Management policy	83
Apply the User Management policy	84
Upgrade from an earlier version	85
Managing Skype for Business Server Users	86
Enabling or disabling users for Skype for Business Server	87
Add and enable a new Skype for Business Server user	87
Disable or re-enable a user account for Skype for Business Server	87
Remove a user account from Skype for Business Server	88
Managing Skype for Business Server user properties	89
View or change Skype for Business Server user properties	89
Move a user to another server or pool in Skype for Business Server	91
Management Pack for SCOM	93

Features	93
Monitoring views	93
Getting started	94
Monitoring Active Roles Administration Service	94
General response - Script	95
General response - Alert	95
Replication monitoring - Script	95
Replication monitoring - Alert	96
Monitoring connection to configuration database	96
Connection to database has been lost - Alert	96
Connection to database has been restored - Alert	97
Monitoring of Dynamic Group-related operations	97
Dynamic Group - Rebuilding has been started - Alert	98
Failed to add object to Dynamic Group - Alert	98
Failed to remove object from Dynamic Group - Alert	98
Dynamic Group - Failed to process membership rule - Alert	99
Dynamic Group - Failed to update membership list - Alert	99
Dynamic Group - Failed to update membership list of nested group - Alert	99
Dynamic Group - Failed to update membership rule upon deletion of object - Alert	99
Dynamic Group - Failed to look up object when updating - Alert	100
Dynamic Group - Failed to retrieve information from domain - Alert	100
Dynamic Group - Membership rule domain unavailable - Alert	101
Dynamic Group - Membership rule failed - Alert	101
Monitoring of Group Family-related operations	101
Group Family - Cannot find configuration storage group - Alert	102
Group Family - Failed to retrieve configuration data - Alert	103
Group Family - Incorrect configuration data - Alert	103
Group Family - Failed to retrieve configuration data for controlled group - Alert	103
Group Family - Failed to retrieve data from container - Alert	103
Group Family - Failed to update configuration data - Alert	104
Group Family - Failed to update configuration data for controlled group - Alert	104
Group Family - Cannot find controlled group - Alert	104
Group Family - Failed to create controlled group - Alert	105
Group Family - Failed to update membership list of controlled group - Alert	105
Group Family - Failed to create run task - Alert	105

Group Family - Failed to modify run task - Alert	105
Group Family - Failed to delete run task - Alert	106
Group Family - Run task has been started manually - Alert	106
Group Family run has been completed - Alert	106
Internal error - Alert	106
Critical error on startup - Alert	106
License system failure - Alert	107
Monitoring Active Roles Web Interface	107
Availability - Script	107
Availability - Alert	107
Monitoring performance	108
AD changes processed/sec	108
Changes queue length (AD + Database)	108
Connected clients	108
Database changes processed/sec	109
LDAP operations in progress	109
LDAP operations/sec	109
Private bytes	109
Queued post-processing policies	109
Requests in progress	109
Requests/sec	110
Script module average execution time	110
Script modules executing	110
About us	111
Contacting us	111
Technical support resources	111

Active Roles Solutions Overview

One Identity Active Roles is highly configurable to meet different customer requirements. The add-on products available as part of Active Roles Solutions extend the Active Roles native capability to provide extensible solutions to the customer based on their requirement. For example, specific customer scenarios may involve the following:

- Multi-forest design environments.
- Transfer of Active Roles configuration between different environments.
- Exchange of user, resource, and service provisioning information between SPML-enabled enterprise applications and Active Directory.
- Administration of Skype for Business Server user accounts.
- Monitoring availability and health of the Active Roles Administration Service and its information store, Active Roles replication status, and availability of the Active Roles Web Interface.

Currently, Active Roles provides the following solutions to support customer requirements in specific environments:

- [Exchange Resource Forest Management](#)
- [Configuration Transfer Wizard Solution](#)
- [Active RolesSPML Provider](#)
- [Skype for Business Server Solution](#)
- [Management Pack for SCOM](#)

Active Roles solutions are available as part of the Active Roles package. However, the solutions can be installed on your system along with Active Roles based on the specific requirement.

Exchange Resource Forest Management

The Exchange Resource Forest Management (ERFM) feature of Active Roles allows you to automate mailbox provisioning for on-premises users in environments where the mailboxes and the user accounts are managed in different Active Directory (AD) forests. Such multi-forest environments are based on the resource forest model, and mailboxes provisioned in such environments are called linked mailboxes.

Multi-forest AD deployments have higher administrative and support costs. However, they offer the highest level of security isolation between AD objects and the Exchange service. As such, One Identity recommends configuring the resource forest model for use with Active Roles in organizations that:

- Aim for an extra layer of data security.
- Frequently experience organizational changes, for example buying companies, or consolidating and breaking off branch companies, departments and other business units.
- Abide by certain legal or regulatory requirements.

AD deployments following the resource forest model use two types of AD forests:

- **Account forests:** These AD forests store the user objects. Organizations can use one or more account forests in the resource forest model.
- **Resource forest:** This AD forest contains the Exchange server and stores the mailboxes of the user objects.

For more details on ERFM, see *Exchange Resource Forest Management* in the *Active Roles Feature Guide*.

For more information on the prerequisites and configuration of ERFM and linked mailboxes, see *Configuring linked mailboxes with Exchange Resource Forest Management* in the *Active Roles Administration Guide*.

Configuration Transfer Wizard Solution

For large enterprises which implement a complex administrative structure using Active Roles, one of the greatest challenges becomes exporting Active Roles configuration from a test environment to a production environment.

With Active Roles Configuration Transfer Wizard, you can export Active Roles configuration objects (such as Access Templates, Managed Units, Policy Objects, Policy Type objects, etc.) to an XML file and then import them from that file to populate another instance of Active Roles. The export and import operations provide a way to move configuration objects from a test environment to a production environment.

This document provides information on how to install and use Configuration Transfer Wizard.

What's new in version 8.0 LTS

Version 8.0 LTS of Configuration Transfer Wizard adds support for the latest Active Roles version, 8.0 LTS. Now you can use Configuration Transfer Wizard to move configuration data between Active Roles instances of version 6.7 or later, including version 8.0 LTS.

Solution components

Configuration Transfer Wizard includes the following components, which are installed during the solution setup:

- Configuration Collection wizard
- Configuration Deployment wizard
- ARSconfig command-line tool

Configuration Collection wizard

Configuration Collection Wizard is intended to collect the Active Roles configuration data in a source environment. During the collection process, the selected Active Roles configuration objects are packed into an XML file referred to as *configuration package*.

Configuration Deployment wizard

Configuration Deployment Wizard is designed to deploy a configuration package, earlier created with the Configuration Collection Wizard, in a destination Active Roles environment. When deploying the configuration data, the target Active Roles instance is populated with the configuration objects collected from the source Active Roles instance.

ARScfg command-line tool

The ARScfg command-line tool provides a script-based interface that enables automation of Active Roles configuration transfer. By using the command-line script, you can create or deploy an Active Roles configuration data package, or roll back changes made to a target Active Roles configuration during deployment of a configuration package.

For information on how to use the solution components, see [Using the solution](#) later in this document.

Installing the solution

This section explains how to install Configuration Transfer Wizard.

Installation requirements

The solution runs on top of Active Roles, and requires the Active Roles Administration Service to be deployed in your Active Directory environment prior to deploying the solution. The following versions of the Active Roles Administration Service are supported:

- 7.0.2
- 7.1
- 7.2
- 7.3
- 7.4.x

Before you install Configuration Transfer Wizard, ensure that you have any of following software components installed on the computer where you plan to install Configuration Transfer Wizard:

- Active Roles Administration Service
- Active Roles Console (MMC Interface)

Depending on whether you use the solution to collect Active Roles configuration data or to deploy a configuration package, Configuration Transfer Wizard must be installed on a computer from which you can connect to the Active Roles Administration Service in the source or destination environment. If the source and destination environments are physically separated, the solution must be installed in each environment.

Installation procedure

Assuming default security settings, the Domain Admins rights are sufficient to install the solution.

To install Configuration Transfer Wizard

1. Start the Installation Wizard by running **ConfigurationTransferWizard.msi** from the Active Roles distribution package.
2. Follow the instructions in the Installation Wizard.

Using the solution

This section explains how to use Configuration Transfer Wizard.

General considerations

To use this solution, you must have the necessary security permissions. It is sufficient to be a member of the Active Roles Admin account, in both the source and destination environments. The Active Roles Admin account is specified during installation of the Administration Service and defaults to the Administrators group on the computer running the Administration Service.

IMPORTANT: Before transferring the Active Roles configuration data, ensure that the Active Directory Organizational Unit (OU) structure in the destination environment is identical to the OU structure in the source environment.

These are the general steps required to transfer Active Roles configuration data by using this solution:

1. **Collect configuration data from a source Active Roles environment** In this step, you select the Active Roles configuration objects you want the configuration package to include, and then create a configuration package XML file. This step is performed in the source environment.
2. **Deploy the collected configuration data to a destination Active Roles environment** In this step, the target Active Roles instance is populated with configuration objects from an earlier created package. This step is performed in the destination environment.

NOTE: If an object to deploy already exists in the target configuration, then the properties of the object are updated during the deployment process.

To perform these steps, you can use either the Configuration Collection Wizard and Configuration Deployment Wizard, or the ARSconfig command-line tool. Both methods have the same effect and can be used interchangeably, depending on your requirements.

- You can use this solution to transfer Active Roles configuration objects of the following categories:
- Access Templates and containers that hold Access Templates
- Managed Units and containers that hold Managed Units
- Policy Objects and containers that hold Policy Objects
- Scheduled Task objects and containers that hold such objects
- Application objects and containers that hold such objects
- Script Modules and containers that hold Script Modules
- Virtual attributes
- Access Template Links (edsACE object type)
- Policy Object Links (edsPolicyObjectLink object type)
- Mail Configuration objects (edsMailConfiguration object type)
- Workflow definition objects (edsWorkflowDefinition object type)
- Automation Workflow definition objects (edsAutomationWorkflowDefinition object type)
- Policy Type objects (edsPolicyType object type)
- Entitlement Profile Specifier objects and containers (edsOneViewSpecifier or edsOneViewSpecifiersContainer object type) - requires Active Roles 6.7 or later
- Display specifiers and containers that hold display specifiers (displaySpecifier or edsDisplaySpecifierContainer object type)

The solution cannot be used to transfer configuration objects of the following categories:

- Built-in objects (the objects that have "built-in" as part of the name)
- Objects held in the Configuration/Application Configuration/Web Interface container (Web Interface configuration data)

If you need to roll back the changes made to the configuration of the target Active Roles instance, during the package deployment, you can do this by using the command-line tool

included with the solution. For step-by-step instructions, see [Scenario: Rolling back the configuration changes](#) later in this document.

About dangling links

When collecting Access Templates and Policy Objects, the solution analyzes their links and writes the links to the destination package. Every link record includes information about the directory object and, if applicable, the trustee to which the respective Access Template or Policy Object is applied. In the configuration package file, this information normally takes the form of the distinguished name (DN), whereas in the Active Roles environment the links refer to the objects by security identifier (SID) or globally unique identifier (GUID). The solution needs DN rather than SID or GUID to identify an object as in a different environment, the object SID or GUID differs from that in the original environment. By identifying the link reference objects by DN, the solution enables the delegation and policy settings to be properly transferred from the source environment to the destination environment.

To have the link records identify the link reference objects by DN, the solution has to look up object SID or GUID to object DN. If this process fails for a given link, the link record is created that identifies the link reference object by SID or GUID. Such a record is referred to as *dangling link*.

If any dangling links have been recorded to the destination package, the solution informs of this condition. Deploying a package that contains dangling links may create links in the destination environment that refer to non-existent objects. As a result, some delegation and policy settings configured by deploying the package may not match the settings found in the source environment from which the package was collected.

The ARSconfig tool provides the *danglingLinks* parameter that allows you to specify how you want the deployment process to handle dangling links. For more information, see [Using the ARSconfig command-line tool](#) later in this document.

Using the Collection wizard and Deployment wizard

To transfer Active Roles configuration, you can collect configuration objects from one Active Roles environment and then deploy them to another environment in the following way:

1. Create a configuration package file with the Configuration Collection Wizard.
2. Deploy the package with the Configuration Deployment Wizard.

To create a configuration package with the Configuration Collection wizard

1. Start the wizard by running the **Configuration Collection Wizard** application from the Start menu or Start page.

2. On the **Collect Active Roles Configuration Data** page, do the following:
 - a. Click **Connect** and using the **Connect to Administration Service** dialog that opens, select the Administration Service to which you want the wizard to connect.
 - b. Under **Select configuration objects to package**, select the objects you want to include in the configuration package, and specify whether you want to collect the child objects of the selected objects.
 - c. When finished, click **Create Package**.
3. On the **Specify a location for the configuration package** page, do the following:
 - a. Click **Browse** to specify a location and name for the configuration package file.
 - b. Under **Package description**, enter the package description (optionally).
 - c. To cause the wizard to collect Access Templates associated with selected objects, leave the **Do not collect associated Access Templates** check box cleared. Otherwise, select this check box.
 - d. To cause the wizard to collect Policy Objects associated with selected objects, leave the **Do not collect associated Policy Objects** check box cleared. Otherwise, select this check box.
4. On the **Verify the information you specified** page, click **Start**.

To deploy a configuration package with the Configuration Deployment wizard

1. Start the wizard by running the **Configuration Deployment Wizard** application from the Start menu or Start page.
2. On the **Deploy Active Roles Configuration Data** page, do the following:
 - a. Click **Browse** to select the configuration package file.
 - b. Optionally, select the **Ignore errors** check box for the wizard to ignore any errors during the configuration deployment.
 - c. Click **Deploy Package**.
3. On the **Connect to Administration Service** page, select the Administration Service to which you want the wizard to connect, and then click **Next**.
4. On the **Add Domain Name Mapping** page, if names of the managed domains differ in the test and production environments, add domain name mapping entries, and then click **Next**.
5. On the **Verify the information you specified** page, click **Start**.

Using the ARSconfig command-line tool

As an alternative to using the graphical user interface tools, you can use the ARSconfig command-line tool. The ARSconfig tool is the `arsconfig.wsf` Windows Script File (WSF) that defines the command line parameters and the required object references.

Using the ARSconfig tool requires two files to be pre-configured, before running the script. These are a file that lists the configuration objects that the package must include, and, if necessary, a file containing domain mapping entries.

To run the ARSconfig command-line tool

- From a command prompt, run the `arsconfig.wsf` script, specifying the required type of task and parameters. The script syntax is described in the section that follows.

Syntax

```
Cscript arsconfig.wsf [/?] /task:<'collect' | 'deploy' | 'rollback'>
[/selection:<"<filename.xml>">] [/package:<"<filename.xml>">] [/map:<"<filename.csv>">]
[/verbose] [/log:<"<filename>">] [/deletelog] [/server:<servername>] [/login:<username>]
[/password:<userpassword>] [/danglingLinks:<'Stop' | 'Skip' | 'Deploy'>]
[/ignoreLinks:<'0' | '1' | '2' | '3'>] [/ignoreErrors] [/upgrade]
```

Parameters

Table 1: Parameters

Parameter	Description
<i>task</i>	<p>This is a required parameter which defines the type of task you want to perform by using this script.</p> <p>Specify one of these parameter values:</p> <ul style="list-style-type: none">• 'collect' - Collects configuration data from the source Active Roles environment, and creates a configuration package file.• 'deploy' - Populates the target Active Roles instance with objects from a configuration package created earlier by Configuration Transfer Wizard.• 'rollback' - Reverts the configuration of the target Active Roles instance to the state it was in before deployment of the configuration package.
<i>selection</i>	<p>The path and name of the XML file containing a list of the source configuration objects to be included in the configuration package.</p> <p>This parameter is required when you use this script to create a configuration package. The XML file you specify in this parameter must be manually created before you run the script.</p>
<i>package</i>	<p>The full path to the configuration package XML file.</p> <p>Add this parameter is you want to specify a custom name and</p>

Parameter	Description
	location for the configuration package file. If you do not specify this parameter, the script assumes that the installation path, and the default package file name are used.
<i>map</i>	<p>The name of the domain mapping file.</p> <p>Add this parameter if you want the test domain names to be replaced with the production domain names, during configuration package deployment.</p> <p>You can add this parameter only when you use this script to deploy a configuration package. The CSV file you specify in this parameter must be manually created before you run the script.</p>
<i>verbose</i>	<p>Enables log trace output.</p> <p>If this parameter is not specified, then no information is displayed in the Command Prompt while the script is running.</p>
<i>log</i>	<p>Specifies the name of the trace output file. You can also specify a target location for the log file.</p> <p>Add this parameter to create a log file with diagnostic information.</p>
<i>deletelog</i>	<p>Deletes the trace output file upon successful completion.</p> <p>Add this parameter if you want the log file deleted if a task was completed with no errors.</p>
<i>server</i>	<p>The fully qualified domain name of the computer running the Administration Service to connect to.</p> <p>If this parameter is not specified, the script attempts a connection to any available Administration Service.</p>
<i>login</i>	The user logon name of the account with which you want to connect, in the form Domain\UserName, or in the form of a user principal name.
<i>password</i>	Password for the user logon name you specify in the <i>login</i> parameter.
<i>danglingLinks</i>	<p>This parameter takes effect if the <i>task</i> parameter value is set to 'deploy', and specifies whether to deploy Access Template or Policy Object links, if any found in the package, that refer to objects which may fail to be resolved in the destination environment (dangling links). The acceptable parameter values are:</p> <ul style="list-style-type: none"> 'Stop' - The deployment process is not started if any dangling links are detected (default setting)

Parameter	Description
	<ul style="list-style-type: none"> 'Skip' - The dangling links are not deployed in the destination environment 'Deploy' - Deployment of the dangling links is attempted based on the data found in the package
<i>ignoreLinks</i>	<p>Specifies whether to collect Access Template links and Policy Object links. This parameter can take any of the following values:</p> <ul style="list-style-type: none"> '0' - Collect all links (default setting). '1' - Do not collect Policy Object links. '2' - Do not collect Access Template links. '3' - Do not collect Policy Object and Access Template links.
<i>ignoreErrors</i>	If this parameter is specified, the solution ignores any errors that can be encountered during the configuration deployment.
<i>upgrade</i>	If supplied together with <code>/task:'deploy'</code> , preserves the existing links, policy parameters and scheduled task parameters. Without this parameter, the deployment of a configuration package replaces the existing links with the links found in the configuration package, and resets the policy and schedule task parameters to the default values.

Scenario: Transfer Active Roles configuration

This scenario explains how to use the ARSconfig command-line tool to transfer a set of configuration objects from a test Active Roles instance to a production instance.

Suppose you need to transfer the following configuration objects from a test Active Roles instance to a production Active Roles instance:

- The **Configuration/Access Templates/Common** container, including all child objects stored in this container.
- The **Configuration/Managed Units/Development** container, excluding the child objects stored in this container.
- All child objects stored in the **Script Modules/Corporate Policy/Priority Access** container, but excluding the container itself.

Also, assume that the names of the domains managed by the test (source) Active Roles instance are **test1.company.com** and **test2.company.com**, and the two corresponding domains managed by the production (target) Active Roles instance are **prod1.company.com** and **prod2.company.com**.

To implement this scenario, complete the following steps:

1. Create a list of the configuration objects to collect
2. Create configuration data package
3. Add domain mapping
4. Deploy the configuration data package

Step 1: Creating a list of the configuration objects to package

In this step, you create a list of the configuration objects that you want to collect into the configuration package, and define how you want to collect their child objects.

To do that, create the **selection.xml** file, and save that file to the solution installation folder: *<Active Roles installation folder>\Configuration Transfer Wizard\Scripts*.

To clarify the file format, consider the following sample file that illustrates how to collect Access Templates, Managed Units, and Script Modules residing within specified containers:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration>
  <include DN="CN=Common,CN=Access Templates,CN=Configuration" collectSelf="True"
collectChildren="True"/>
  <include DN="CN=Development,CN=Managed Units,CN=Configuration" collectSelf="True"
collectChildren="False"/>
  <include DN="CN=Priority Access,CN=Corporate Policy,CN=Script
Modules,CN=Configuration" collectSelf="False" collectChildren="True"/>
</Configuration>
```

Step 2: Creating configuration data package file

In this step, you use the ARSconfig command-line tool to create a configuration data package file using the data from the **selection.xml** file created in Step 1.

To create the configuration data package file

- At a command prompt, navigate to the Configuration Transfer Wizard installation folder, and enter the following syntax:

```
Cscript.exe arsconfig.wsf /task:collect /selection:selection.xml
```

As the result, the **package.xml** configuration data package file will be created in the following default location: *<Active Roles installation folder>\Configuration Transfer Wizard\Scripts*.

Step 3: Configuring domain mapping

If the names of the managed domains are different in the test and production environments, you must add domain mapping that defines the correspondence between the domain names. When the configuration package is deployed in the target environment, the domain names specified as a part of the objects' attributes are replaced with the names of the production domains, according to the name mapping entries.

In this step, you create the CSV domain name mapping file—**mapping.csv**, and then save that file to the solution installation folder: *<Active Roles installation folder>\Configuration Transfer Wizard\Scripts*. In this scenario, the **mapping.csv** file contains the following lines:

```
"DC=test1,DC=company,DC=com", "DC=prod1,DC=company,DC=com"
```

```
"DC=test2,DC=company,DC=com", "DC=prod2,DC=company,DC=com"
```

Step 4: Deploying the configuration data package

In this step, you use the ARSconfig command-line tool to deploy the **package.xml** configuration package in the production Active Roles environment. When running the `arsconfig.wsf` script, specify the package file to deploy (**package.xml**), and the domain name mapping file (**mapping.csv**) you have created in Step 3.

To deploy the package

- At a command prompt, navigate to the Configuration Transfer Wizard installation folder, and enter the following syntax:

```
Cscript.exe arsconfig.wsf /task:deploy /package:package.xml /map:mapping.csv
```

Scenario: Rolling back the configuration changes

This step may be required if you have encountered any errors when deploying a configuration package in the production environment. By rolling back changes in the target configuration, you bring it to the state it was in before the package was deployed. Use the following instruction to roll back the changes made by the deployment of the **package.xml** file described in the scenario outlined above.

To roll back configuration changes

- At the command prompt, navigate to the Configuration Transfer Wizard installation folder, and enter the following syntax:

```
Cscript.exe arsconfig.wsf /task:rollback /package:package.xml
```

Known issues

This section provides a list of the currently known issues that customers may experience with Configuration Transfer Wizard. For each issue, the list includes an ID number, which identifies the issue, a brief description of the problem, and a workaround, if any exists, for the problem.

TF00004281

In the target Active Roles configuration, the solution cannot restore the `edsvaDebuggingServer` and `edsvaDebuggingServerName` properties of Script Module objects: those attributes are always empty.

WORKAROUND

Manually specify those properties with the use of the Active Roles console.

TF00004581

Configuration Deployment Wizard fails to deploy some of Access Templates. The solution log file contains the error message similar to the following text:

"Error [4710]: Administrative Policy returned an error. The object <Object DN> not found."

This error occurs if the source configuration contains nested Access Templates.

WORKAROUND

On the **Collect Active Roles Configuration Data** page of the wizard, select all the nested Access Templates you want to collect. If you are using ARSconfig, ensure that the selection file includes the nested Access Templates into the configuration export package.

TF00004585

After transferring a Policy Object that includes the "User Account Relocation Deprovisioning" policy entry, the "Description" and the "Error message returned by this policy" text boxes available on the **User Account Relocation Policy Properties** dialog box contain invalid target domain name.

WORKAROUND

After deploying the target configuration, manually edit those text elements using the Active Roles console.

TF00010732

When collecting Script Modules, Configuration Transfer Wizard may not collect the library Script Modules that are used by the Script Modules being exported. As a result, the deployment of the exported Script Modules may cause an error condition in the destination environment.

WORKAROUND

On the **Collect Active Roles Configuration Data** page of the wizard, select all the

library Script Modules that are used by the Script Modules you want to collect. If you are using ARSconfig, ensure that the selection file includes the library Script Modules into the configuration export package.

TF00039803

When collecting Display Specifiers, Configuration Transfer Wizard may not collect the Active Roles virtual attributes for which the Display Specifiers are being exported. As a result, the deployment of the exported Display Specifiers may cause an error condition in the destination environment.

WORKAROUND

On the **Collect Active Roles Configuration Data** page of the wizard, select all the Active Roles virtual attributes for which the Display Specifiers are being exported. If you are using ARSConfig, ensure that the selection file includes the Active Roles virtual attributes into the configuration export package.

TF00050511

In a situation where an object to be exported does not exist in the source environment, Configuration Transfer Wizard stops the export process. As a result, the configuration export package may not include all objects that were selected for export.

WORKAROUND

Ensure that all objects you selected for export exist in the source environment.

TF00062463

Configuration Transfer Wizard does not provide the ability to export links that involve pre-defined or built-in objects, nor does it make possible to export pre-defined or built-in objects. As a result, you do not have the option to transfer, for example, the links of pre-defined Access Templates.

WORKAROUND

When transferring a configuration that includes any links of pre-defined or built-in objects, create the required links manually in the destination environment.

TF00125202

When using the Configuration Collection Wizard or Configuration Deployment Wizard, you may encounter an error message such as "A generic error occurred in GDI+."

WORKAROUND

Disregard the error message. Click **OK** to close the error message box.

TF00130489

When using ARSconfig with the 'rollback' task option, you may encounter an error: "This script module is in use, and cannot be deleted." This issue is most likely to occur with a PowerShell based Script Module containing a library script, and is due to the fact that the Script Module remains locked for a certain time period after all the Script Modules that use the library script have been deleted.

WORKAROUND

Run ARSconfig with the 'rollback' task option once more, or delete the Script Module manually, with the use of the Active Roles console.

TF00134074

With the display DPI setting of 'Large size (120 DPI)' you may encounter some minor visual defects on Configuration Transfer Wizard pages.

WORKAROUND

Use the display DPI setting of 'Normal size (96 DPI)'.

Active RolesSPML Provider

Active RolesSPML Provider is designed to exchange the user, resource, and service provisioning information between SPML-enabled enterprise applications and Active Directory.

Active RolesSPML Provider supports the Service Provisioning Markup Language Version 2 (SPML v2), an open standard approved by the Organization for the Advancement of Structured Information Standards (OASIS). SPML - is an XML-based provisioning request-and-response protocol that provides a means of representing provisioning requests and responses as SPML documents. The use of open standards provides the enterprise architects and administrators with the flexibility they need when performing user management and user provisioning in heterogeneous environments.

Features

The key features of Active RolesSPML Provider are as follows:

- **Support for two operation modes:** SPML Provider can be configured to operate in *proxy mode* or in *direct access mode*. In proxy mode, SPML Provider accesses Active Directory or Active Directory Lightweight Directory Services (AD LDS, formerly known as ADAM) through Active Roles used as a proxy service, while in direct access mode, SPML Provider directly accesses Active Directory or AD LDS.
- **Support for equivalent LDAP operations:** SPML Provider can perform equivalent LDAP operations such as `addRequest`, `modifyRequest`, `deleteRequest`, and `lookupRequest`.
- **Support for Azure AD, AD, and AD LDS data management:** SPML Provider enables SPML-conformant applications to read from and write to Azure AD, Active Directory (AD), and AD LDS.
- **Search Capability support:** SPML Provider allows SPML-enabled applications to search for relevant directory objects based on various search criteria.
- **Password Capability support:** SPML Provider allows SPML-enabled applications to perform basic password management tasks such as setting and expiring user passwords.

- **Suspend Capability support:** SPML Provider allows SPML-enabled applications to effectively enable, disable and deprovision user accounts in Active Directory.
- **Flexible Configuration options:** There is support for many different configuration options that enable the administrator to adjust the behavior and optimize the SPML Provider performance.
- **IIS Security Support:** SPML Provider supports all IIS security configurations, including integrated Windows authentication, basic authentication, and basic authentication over Secure Sockets Layer (SSL).
- **Support for using Active Roles controls:** In proxy mode, you can send Active Roles controls to the Active Roles Administration Service with an SPML request to perform an administrative operation. In your request, you can also define the Active Roles controls that the Administration Service must return in the SPML response.

Use scenarios

SPML Provider can be used for a variety of purposes. Some common scenarios for using SPML Provider are as follows:

- **Non-Windows applications:** The systems running non-Windows applications that need to communicate with Active Directory can do this through SPML Provider. For example, with SPML Provider, Unix applications can manage Unix-enabled user accounts in Active Directory. In proxy mode, SPML Provider allows existing SPML-compatible provisioning systems, such as SUN Java System Identity Manager and IBM Tivoli Directory Integrator to take advantage of the functionality of Active Roles.
- **Web services:** The use of directories in Web services is growing rapidly. Additionally, XML is becoming the default language for use with Web services. SPML Provider fills the gap between XML documents and Active Directory services, enabling applications that must provide or use Web services to communicate with Active Directory.
- **Handheld and portable devices:** Data-enabled cell phones or PDAs that need an access to directory data may not contain a client for the ADSI LDAP Provider but might be able to use the SPML communication protocol to access Active Directory over the Internet.
- **Firewall access:** Certain firewalls cannot pass LDAP traffic because they cannot audit it, but these firewalls can pass XML. In such cases, applications can use SPML Provider to communicate with Active Directory across a firewall.

Basic concepts and definitions

Active RolesSPML Provider operates based on the concepts defined in SPML v2. This section introduces and describes these key concepts and definitions as applied to SPML Provider.

A **Client** (Requesting Authority or Requestor) is any SPML-compliant application that sends well-formed SPML requests to the Active RolesSPML Provider and receives responses from it. Clients can include various business applications, such as human resources (HR) databases or Identity Management systems. There is no direct contact between a client and the target (Active Roles or an Active Directory server).

Active RolesSPML Provider (Provisioning Service Provider or PSP) is a Web service that uses the Simple Object Access Protocol (SOAP) over HTTP for communications. SPML Provider can directly access Active Directory data or communicate with Active Directory using the Active Roles proxy service. SPML Provider acts as an intermediary between a client and the target (Active Directory domain controller or Active Roles).

In proxy mode, **Active Roles** represents the Provisioning Service Target (or Target) that is available for provisioning actions through SPML Provider. The target has a unique identifier (targetID) that is maintained by SPML Provider and is used in a request or a response.

AD Objects (Provisioning Service Objects or PSO) represent directory objects that SPML Provider manages. A client can add, delete, modify, or look up a directory object. Each object has a unique identifier (PSO ID). In SPML Provider, an object DN is used as a PSO ID.

NOTE: A Requestor, Provisioning Service Provider, Provisioning Service Target, and Provisioning Service Objects are key notions described in the official SPML v2 specification.

For detailed information on the concepts defined in SPML v2, see Section 2 "Concepts" of the OASIS SPML v2 specification, available for download at <http://www.oasis-open.org/specs/index.php#spmlv2.0>.

How SPML Provider works

With SPML Provider, applications can use SPML documents to look up, retrieve and update directory data in Active Directory, Azure AD, and AD LDS. SPML Provider converts XML elements and attributes into commands used to make changes to Active Directory and retrieve data from Active Directory. SPML Provider can also convert the response received from Active Roles or Active Directory to XML format. These conversions are based on and are in compliance with the OASIS SPML v2 - DSML v2 Profile specification.

SPML Provider runs as a Web application on a Web server running Microsoft Internet Information Services (IIS), and uses SOAP over HTTP to transmit and receive directory requests from client computers.

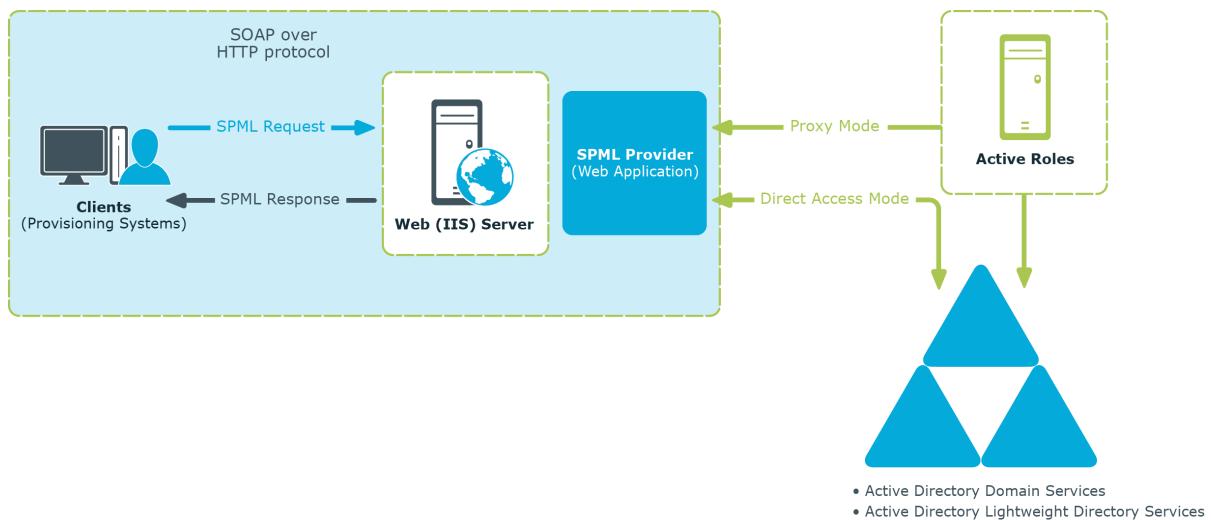
The SPML Provider environment includes the following components:

- **Clients that use SPML v2:** These clients are applications that manage directory objects (for example, user accounts). A client issues SPML requests that describe operations to be performed on the directory object and send these requests to SPML Provider.
- **SPML Provider:** Receives and processes client requests, and returns a response to the client.

- **Active Roles:** In proxy mode, this is the endpoint for provisioning requests and the actual software that manages directory objects.
- **Active Directory, Azure AD, or AD LDS:** In proxy mode, SPML Provider can access Active Directory or Azure AD domains and AD LDS instances that are registered with Active Roles as managed domains, Azure AD tenants, and managed AD LDS instances, respectively. In direct access mode, SPML Provider can access the domain controller or the AD LDS instance defined in the SPML.Config file. For more information, see "Configuring SPML Provider" later in this document.

The following diagram illustrates the flow of requests and responses through the SPML Provider environment components:

Figure 1: Flow of requests and responses through the SPML Provider environment components



As shown in the diagram, the client/SPML Provider communications are based on the simple request/response protocol.

In proxy mode, SPML Provider works in the following way:

1. A client issues a well-formed SPML request using the SOAP over HTTP protocol. This request goes to a server running IIS, where it is routed to SPML Provider.
2. SPML Provider examines the request for conformance to the SPML format.
3. If the request complies with the SPML format, the SPML Provider submits the request to Active Roles. Based on the client request, Active Roles retrieves or modifies data in Active Directory, Azure AD, or in AD LDS.
4. After performing the requested operation, Active Roles sends the result of the operation back to SPML Provider.
5. SPML Provider then processes this result data and sends the result of the performed operation back to the client in the form of an SPML response.

In direct access mode, SPML Provider works in the following way:

1. A client issues a well-formed SPML request using the SOAP over HTTP protocol. This request goes to a server running IIS, where it is routed to SPML Provider.
2. SPML Provider examines the request for conformance to the SPML format.
3. If the request conforms to the SPML format, SPML Provider retrieves or modifies the relevant data in Active Directory or in AD LDS (ADAM).
4. SPML Provider sends the result of the performed operation back to the client in the form of an SPML response.

If the client request does not conform to the SPML format, the client receives an SPML response that describes the encountered error.

System requirements

Before installing the Active RolesSPML Provider, ensure your system meets the following minimum hardware and software requirements.

Hardware requirements

Ensure that the following hardware requirements are met:

- 1 GHz or higher Intel Pentium-compatible CPU.
- At least 1 GB of RAM.
- At least 100 MB of free disk space.

Software requirements

Ensure that the following software requirements are met:

- Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, or Microsoft Windows Server 2019 operating system.
- Microsoft .NET Framework 4.7.2.
- Microsoft Internet Information Services (IIS). For proxy mode, the IIS server must be part of an Active Directory forest where Active Roles is deployed.
- For proxy mode, Active Roles Administration Service 7.4 is required.

TIP: If you choose the proxy mode, for performance reasons, we recommend that you install the Active RolesSPML Provider on the computer running the Active Roles Administration Service.

NOTE: SPML component cannot be installed on a System with TerminalServer roles and components enabled.

Web Server requirements

Windows Server 2012

On a Windows Server 2012 or Windows Server 2012 R2 based computer, ensure that the **Web Server (IIS)** sever role is installed, including:

- Web Server/Common HTTP Features/
 - Default Document
 - HTTP Errors
 - Static Content
 - HTTP Redirection
- Web Server/Security/
 - Request Filtering
 - Basic Authentication
 - Windows Authentication
- Web Server/Application Development/
 - .NET Extensibility 4.7.2
 - ASP
 - ASP.NET 4.7.2
 - ISAPI Extensions
 - ISAPI Filters
- Management Tools/IIS 6 Management Compatibility/
 - IIS 6 Metabase Compatibility

Windows Server 2016 and Windows Server 2019

On Windows Server 2016 and Windows Server 2019 based computer, ensure that the **Web Server (IIS)** sever role is installed, including:

- Web Server/Common HTTP Features/
 - Default Document
 - HTTP Errors
 - Static Content
 - HTTP Redirection
- Web Server/Security/
 - Request Filtering
 - Basic Authentication

- Windows Authentication
- Web Server/Application Development/
 - .NET Extensibility 4.7.2
 - ASP
 - ASP.NET 4.7.2
 - ISAPI Extensions
 - ISAPI Filters
- Management Tools/IIS 6 Management Compatibility/
 - IIS 6 Metabase Compatibility

Use Server Manager to add the required role, role services, and features.

Feature Delegation

Configure Internet Information Services (IIS) to provide **Read/Write** delegation for the following features:

- Handler Mappings
- Modules

Use **Feature Delegation** in Internet Information Services (IIS) Manager to verify that these features have delegation set to **Read/Write**.

Configuring Active RolesSPML Provider

Configuration settings allow the administrator to configure SPML Provider and its schema in order to adjust the SPML Provider behavior. Administrators can, for example, specify the required managed objects and attributes in the schema, or choose the type of execution (disabling or deprovisioning objects) for the Suspend operation.

Configuration settings in SPML.Config

The SPML Provider configuration settings can be found in the SPML.Config file located in the **Web** sub-folder of the SPML Provider installation folder. The SPML.Config file contains data in the XML format. You can open and edit the configuration file with a common text editor such as Notepad.

NOTE: After you modify configuration settings, the IIS application pool for the SPML Provider Web site must be restarted in order for the changes to take effect.

The following table describes the XML elements used in the SPML Provider configuration file.

Table 2: XML elements used in the SPML Provider configuration file

Element	Parent element	Description
service	configuration	In proxy mode, specifies the name of the computer running the Active Roles Administration Service. In direct access mode, specifies the name of the AD domain controller or AD LDS server. The name of the AD LDS server must be in the form <code><servername:portnumber></code> .
adsiProvider	configuration	Specifies the progID of the ADSI Provider. In proxy mode, the progID is EDMS. In direct access mode, the progID is LDAP.
schemaFile	configuration	Contains the name of the file that defines the DSML Profile schema for SPML Provider. By default, the file name is SPMLSchema.Config. The schema file must be located in the same folder as the SPML.Config file.
defaultMaxSelect	search	Specifies the maximum number of search results that SPML Provider can return without page splitting. The default value is 1000.
pageSize	search	Specifies the maximum number of search results per page. The default value is 25. NOTE: If pageSize is set to 0 , SPML Provider returns search results without page splitting.
class	password	Contains the LDAP display name of the schema class of objects on which SPML Provider is expected to perform the Password Capability-related operations such as setPassword and expirePassword .
class	suspend	Contains the LDAP display name of the schema class of objects on which SPML Provider is expected to perform the Suspend Capability-related operations such as suspend , resume , and active .
suspendAction	suspend	Possible values: disable or deprovision. The default value is disable. If suspendAction is set to disable , SPML Provider disables the specified user account on the target. If suspendAction is set to deprovision , SPML Provider deprovisions the specified user account in accordance with the deprovisioning policies defined by Active Roles.

Element	Parent element	Description
checkOutput	configuration	<p>Possible values: true or false. The default value is false.</p> <p>true causes SPML Provider to check the string attribute values retrieved from the underlying directory before adding them to a response. If an attribute value contains illegal characters that could break the XML parser on the client side, SPML Provider converts the attribute value to the base64binary format and then adds the result of the conversion to the response. Note that this option may result in performance degradation of SPML Provider as checking every attribute value is a resource-intensive operation.</p> <p>false causes SPML Provider not to check the string attribute values retrieved from the underlying directory. An attribute value is added to the response without any conversion even if the value contains illegal characters.</p> <p>NOTE: In accordance with the XML specification, the legal character range is as follows: #x9 #xA #xD [#x20-#xD7FF] [#xE000-#xFFFF] [#x10000-#x10FFFF]. With checkOutput set to true, SPML Provider ensures that attribute values in a response contain only characters from the legal character range.</p>

Sample configuration file

The following is an example of the configuration file for SPML Provider configured to operate in proxy mode. If SPML Provider and the Active Roles Administration service are installed on the same computer, the default configuration settings look as follows:

```
<?xml version="1.0"?>
<configuration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="urn:quest:names:SPMLProvider">
<service>localhost</service>
<adsiProvider>EDMS</adsiProvider>
<schemaFile>SPMLSchema.Config</schemaFile>
<capabilities>
<search>
<defaultMaxSelect>1000</defaultMaxSelect>
```



```

<pageSize>25</pageSize>
</search>
<password>
<appliesTo>
<class>user</class>
</appliesTo>
</password>
<suspend>
<appliesTo>
<class>user</class>
</appliesTo>
  <suspendAction>disable</suspendAction>
</suspend>
</capabilities>
<checkOutput>>false</checkOutput>
</configuration>

```

Extending the SPML Provider schema

The SPML Provider schema defines the XML structure of the objects and attributes that SPML Provider manages. You can modify the schema to manage new types of objects or object properties. Thus, you can add the class and attribute definitions to the schema in order to meet the needs of your organization.

NOTE: In proxy mode, you can add only those object classes and attributes that are valid according to the Active Roles schema.

The SPML Provider schema is stored in the SPMLSchema.Config file. The SPMLSchema.Config file is located in the **Web** sub-folder of the SPML Provider installation folder.

The schema format corresponds to the DSML Version 2 profile (DSMLv2). For detailed information on the DSML v2 profile, refer to the OASIS SPML v2 - DSML v2 Profile specification. The specification describes the use of the DSML protocol as a data model for SPML- based provisioning and can be accessed from the OASIS Web site at <http://www.oasis-open.org/specs/index.php#spmlv2.0>.

Using Active RolesSPML Provider

To access SPML Provider, use the following URL:

`http://<HostName>/ARServerSPML/SPMLProvider.asmx`

where the `<HostName>` stands for the name of the computer where SPML Provider is installed.

NOTE: The SPML Provider Web service is described by a Web Services Description Language (WSDL) file. To obtain a WSDL description of SPML Provider, navigate to `http://<HostName>/ARServerSPML/SPMLProvider.asmx?WSDL`.

Operation mode

SPML Provider can be configured to operate in:

- **Proxy mode** In this mode, SPML Provider accesses Active Directory, Azure AD, or AD LDS using the Active Roles proxy service. In proxy mode, SPML Provider extends Active Roles. Because SPML Provider uses open standards such as HTTP, XML, and SOAP, a greater level of interoperability with Active Roles is possible than is available with the Active Roles ADSI Provider.
- **Direct access mode** In this mode, SPML Provider directly accesses Active Directory, Azure AD, or AD LDS.

In proxy mode, SPML Provider can manage objects in Active Directory domains and AD LDS instances that are registered with Active Roles as managed domains and managed AD LDS instances, respectively. In direct access mode, SPML Provider can manage only objects in the domain or AD LDS instance to which SPML Provider is connected using the configuration setting such as the domain controller or AD LDS server.

TIP: To take advantages of the powerful functionality of Active Roles, we recommend that you use proxy mode whenever possible

Support for Active Roles controls

Active Roles implements special parameters called Active Roles controls (hereafter *controls*). The controls allow you to customize request processing.

In proxy mode, SPML Provider clients can send controls to the Active Roles Administration Service with an SPML request to perform an administrative operation. The Administration Service can process the controls. On the other hand, the Administration Service can return its own control to the SPML Provider client, and then the client can process that control. The controls a client sends to the Administration Service are referred to as *InControls* whereas the controls the Administration Service returns to the client are referred to as *OutControls*.

This section covers the following subjects:

- Sending the InControl-type controls to the Active Roles Administration Service with an SPML request.
- Specifying a set of the OutControl-type controls that the Active Roles Administration Service will return with an SPML response.

For more information about Active Roles controls and for the list of available built-in controls, see Active Roles SDK.

IMPORTANT: All elements described in this section must be defined at the beginning of your SPML request. For a sample of use, see later in this document.

Sending controls to the Active Roles Administration Service

This section covers the `controls` and `control` XML elements that your SPML request must include to send controls to the Active Roles Administration Service.

Element name: `controls`

Element description: Specifies a collection of InControl-type controls to send to Administration Service.

Child elements: `control`

Attributes:

Table 3: Controls attributes

attribute name	attribute description
<code>xmlns</code>	Declares the namespace for all child elements of the <code>controls</code> element. This attribute must be set to <code>quest:ars:SPML:2:0</code>

Element name: `control`

Element description: Describes a control to send to the Administration Service.

Parent elements: `controls`

Child elements: None

Attributes:

Table 4: Control attributes

attribute name	attribute description
<code>name</code>	Specifies the name of the control.

The control value in the `control` element body must be specified as follows:

```
<control name=%control name%>%control value%</control>
```

To send an empty control, use the following syntax:

```
<control name=%control name% />
```

Specifying controls to return to the SPML Provider client

This section covers the `controlsForOutput` and `control` XML elements that your SPML request must include to specify a set of controls to return to the SPML Provider client.

Element name: `controlsForOutput`

Element description: Specifies a collection of `OutControl`-type controls to return to SPML client.

Child elements: `control`

Attributes:

Table 5: Attributes for `controlsForOutput`

attribute name	attribute description
<code>xmlns</code>	Declares the namespace for all child elements of the <code>controls</code> element. This attribute must be set to <code>quest:ars:SPML:2:0</code>

Element name: `control`

Element description: Describes a control to return to SPML Provider client with an SPML response.

Parent elements: `controlsForOutput`

Child elements: None

Attributes:

Table 6: Attributes for `control`

attribute name	attribute description
<code>name</code>	Specifies the name of the control.

The `control` elements used to specify controls to return with SPML response must be defined as follows:

```
<control name=%control name% />
```

Sample SPML request

This section provides a sample SPML request and the SPML response that illustrate how to use Active Roles controls in your SPML requests.

This sample shows how an SPML Provider client can send a request to modify the specified user object. With this request, the client sends the `AllowApproval` built-in control set to `Confirm`, and the `CustomControl` control set to `MyCustomValue`. The request also contains the

controlsForOutput element, which specifies that Active Roles Administration service will return values of the OperationStatus and CustomControl controls in the SPML response.

TIP: For more information about the use of the AllowApproval and OperationStatus controls, refer to the Active Roles SDK.

NOTE: You need to modify the sample SPML request in order to adjust it to your environment. Before using this sample, set the ID attribute of the psoID element to the distinguished name of the user account you want to modify.

SPML request

```
<?xml version="1.0"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <spml:modifyRequest xmlns:spml="urn:oasis:names:tc:SPML:2:0">
      <controls xmlns="quest:ars:SPML:2:0">
        <control name="AllowApproval">Confirm</control>
        <control name="CustomControl">MyCustomValue</control>
      </controls>
      <controlsForOutput xmlns="quest:ars:SPML:2:0">
        <control name="OperationStatus"/>
        <control name="CustomControl"/>
      </controlsForOutput>
      <spml:psoID ID="CN=JDOE,OU=Users,DC=mycompany,DC=com"/>
      <spml:modification>
        <modification name="description" operation="replace"
xmlns="urn:oasis:names:tc:DSML:2:0:core">
          <value>New description</value>
        </modification>
      </spml:modification>
    </spml:modifyRequest>
  </soap:Body>
</soap:Envelope>
```

SPML response

```
<?xml version="1.0" encoding="UTF-16"?>
```

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <modifyResponse status="success" xmlns="urn:oasis:names:tc:SPML:2:0">
      <controls xmlns="quest:ars:SPML:2:0">
        <control name="OperationStatus">Completed</control>
        <control name="CustomControl">ReturnedValue</control>
      </controls>
      <pso>
        <psoID ID="CN=JDOE,OU=Users,DC=mycompany,DC=com"/>
        <data>
          <attr name="cn" xmlns="urn:oasis:names:tc:DSML:2:0:core">
            <value xsi:type="xsd:string">Admin1</value>
          </attr>
          <attr name="objectClass" xmlns="urn:oasis:names:tc:DSML:2:0:core">
            <value xsi:type="xsd:string">top</value>
            <value xsi:type="xsd:string">person</value>
            <value xsi:type="xsd:string">organizationalPerson</value>
            <value xsi:type="xsd:string">user</value>
          </attr>
          <attr name="objectCategory" xmlns="urn:oasis:names:tc:DSML:2:0:core">
            <value
xsi:type="xsd:string">CN=Person,CN=Schema,CN=Configuration,DC=dom,DC=lab,DC=local</val
ue>
          </attr>
          <attr name="objectGUID" xmlns="urn:oasis:names:tc:DSML:2:0:core">
            <value xsi:type="xsd:base64Binary">Aodvua6TAE+Ja903vnRntg==</value>
          </attr>
          <attr name="description" xmlns="urn:oasis:names:tc:DSML:2:0:core">
            <value xsi:type="xsd:string">New description</value>
          </attr>
        </data>
      </pso>
    </modifyResponse>
  </soap:Body>
</soap:Envelope>

```

Supported Azure Features

- Active Roles 7.4 SPML Provider supports Azure user, group, and contact creation.

NOTE: You must complete Azure AD configuration, before using SPML for user, group, and contact creation in Azure AD. For more information, see *Azure AD and Office 365 Management Administrator Guide*.

Sample SPML request for Azure user, group, and contact creation

Sample SPML request for Azure User Creation

```
<?xml version="1.0"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body>
<addRequest xmlns="urn:oasis:names:tc:SPML:2:0" returnData="everything">
<containerID ID="OU=AzureOU, DC=Sample,DC=local,DC=com"/>
<data>
<attr name="cn" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>AzureUser</value>
</attr>
<attr name="description" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>Azure test user</value>
</attr>
<attr name="sAMAccountName" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>AzureUser</value>
</attr>
<attr name="objectClass" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>user</value>
</attr>
<attr name="mail" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>AzureUser@ARStestdev.onmicrosoft.com</value>
</attr>
<attr name="otherHomePhone" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>12135555555</value>
<value>12134444444</value>
```

```

</attr>
<attr name="edsaPassword" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>P@ssw0rd123</value>
</attr>
<attr name="edsaAccountIsDisabled" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>FALSE</value>
</attr>
<attr name="userPrincipalName" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>AzureUser@ARStestdev.onmicrosoft.com</value>
</attr>
<attr name="edsaAzureOffice365Enabled" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>TRUE</value>
</attr>
<attr name="edsaAzureUserPrincipalName" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>AzureUser@ARStestdev.onmicrosoft.com</value>
</attr>
<attr name="edsaAzureUserAccountEnabled" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>TRUE</value>
</attr>
<attr name="edsaAzureUserDisplayName" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>AzureUser</value>
</attr>

</data>
</addRequest>
</soap:Body>
</soap:Envelope>

```

Sample SPML request for Azure Group Creation.

```

<?xml version="1.0"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body>
<addRequest xmlns="urn:oasis:names:tc:SPML:2:0" returnData="everything">
<psoID ID="CN=GroupName,OU=AzureOU,DC=Sample,DC=local,DC=com"/>
<data>

```



```

<attr name="objectClass" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>group</value>
</attr>
<attr name="description" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>My test group</value>
</attr>
<attr name="mailEnabled" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>false</value>
</attr>
<attr name="mail" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value> GroupName@company.com</value>
</attr>
<attr name="mailNickName" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value> GroupName</value>
</attr>
<attr name="edsvaAzureOffice365Enabled" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>TRUE</value>
</attr>
<attr name="edsaAzureGroupDisplayName" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value> GroupName</value>
</attr>
<attr name="edsaEstablishGroupEmail" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>false</value>
</attr>
<attr name="edsaAzureGroupType" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>-2147483646</value>
</attr>
</data>
</addRequest>
</soap:Body>
</soap:Envelope>

```

Sample SPML request for Azure Contact Creation

```

<?xml version="1.0"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

```

```

<soap:Body>
<addRequest xmlns="urn:oasis:names:tc:SPML:2:0" returnData="everything">
<containerID ID="OU=AzureOU,DC=Sample,DC=local,DC=com"/>
<data>
<attr name="cn" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>AzureContact</value>
</attr>
<attr name="description" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>AzureContact</value>
</attr>
<attr name="objectClass" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>Contact</value>
</attr>
<attr name="edsvaAzureOffice365Enabled" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>TRUE</value>
</attr>
<attr name="edsaAzureContactEmail" xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>AzureContact@test.com</value>
</attr>
</data>
</addRequest>
</soap:Body>
</soap:Envelope>

```

Supported operations

SPML Provider implements the SPML v2 core protocol and supports core operations that are required for conformance to the official SPML v2 specification. The following table lists the core operations supported by SPML Provider.

Table 7: Core operations supported by SPML Provider

Operation	Description
listTargets	Lists targets available for provisioning through SPML Provider and the SPML Provider's supported set of capabilities for targets.

Operation	Description
add	Creates a new object on the target.
modify	Changes the specified object on the target.
lookup	Obtains the XML that represents the specified object on the target.
delete	Removes the specified object from the target.

In addition to core operations required for conformance to the SPML v2 specification, SPML Provider supports a set of optional operations (Capabilities) that are functionally related. The following tables list the Capabilities supported by SPML Provider.

Search capability

Table 8: Capabilities supported by SPML Provider

Operation	Description
search	Obtains every object that matches the specified query.
iterate	Obtains the next set of objects from the result set selected for a search operation.
closeIterator	Informs SPML Provider that the client no longer intends to iterate the search result.

Suspend capability

Table 9: Suspend capability

Operation	Description
suspend	Disables/deprovisions the specified object on the target.
resume	Re-enables the specified object on the target.
active	Checks whether the specified object on the target has been suspended.

Password Capability

Table 10: Password capability

Operation	Description
setPassword	Specifies a new password for a user account.
expirePassword	Marks as invalid the current password for a user account.

For detailed information on the SPML v2 operations, refer to the "Operations" section in the official SPML v2 specification, available for download at <http://www.oasis-open.org/specs/index.php#spmlv2.0>.

Samples of use

SPML Provider implements the SPML v2 core protocol and supports the DSML v2 Profile for SPML operations. SPML Provider comes with a sample client that includes examples illustrating how to construct SOAP messages that contain SPML payloads to perform common directory operations.

To work with the examples in the SPML Provider sample client

1. From the **Start** menu on the computer on which SPML Provider is installed, select **Active RolesSPML Provider** to open the home page of the sample client in your Web browser.
2. On the **Samples of Use** home page, under **How do I**, click the example you want to examine.

For instance, you might click **Create new user** to view, modify, and perform the SPML v2 request that creates a user object.

3. On the page that opens, in the **SPMLv2 request** box, view the SOAP message that will be sent to SPML Provider.

You may need to modify the SOAP message in order to adjust it to your environment. Thus, with the **Create new user** example, you have to set the ID attribute of the <ContainerID> element to the distinguished name (DN) of the container where you want to create a new user.

4. Click the **Send Request** button to send the SOAP message to SPML Provider.
5. In the **SPMLv2 response** box, view the SOAP message returned by SPML Provider in response to your request.
6. To examine another example, return to the home page, and then click the desired example.

Configuration settings in sample.config

Support for configuration options enables administrators to set the SPML Provider sample client configuration in order to test the SPML Provider functionality under actual conditions. Administrators can, for example, specify the desired settings for the sample container object (OU) that will be used in sample SPML v.2 operations.

The configuration settings of the SPML Provider sample client can be found in the sample.config file located in the **Samples** sub-folder of the SPML Provider installation folder.

The sample.config file contains data in the XML format. You can open and edit the configuration file with a common text editor such as Notepad. The default configuration settings in the sample.config file look as follows:

```
<samples>
<server>localhost</server>
```

```

<url>ARServerSPML/spmlprovider.asmx</url>
<sampleContainerName>OU=MyOU,DC=Company,DC=com</sampleContainerName>
</samples>

```

The following table provides reference information for XML elements used in the sample.config. file.

Table 11: XML elements used in the sample.config. file

Element	Parent element	Description
server	samples	Specifies the name of the computer running SPML Provider.
url	samples	Specifies Web address of SPML Provider. The default address is ARServerSPML/spmlprovider.asmx.
sampleContainerName	samples	Specifies the distinguished name of the container (OU) used in the sample SPML v.2 requests.

Core Operation samples

The following table lists all examples included in the Core Operation samples.

Table 12: Core operation samples

Operation	Description
List targets available for provisioning with SPML Provider	<p>This example illustrates how to retrieve the targets available for provisioning with SPML Provider.</p> <p>To do this, SPML Provider performs the listTargets operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. The <listTargetsRequest> element asks SPML Provider to declare the set of targets that SPML Provider exposes for provisioning operations. <p>The response lists the supported targets, including the schema definitions for each target and the set of capabilities that SPML Provider supports for each target. The contents of the <listTargetsResponse> element conform to the OASIS SPML v2 specification.</p>

Operation	Description
Create new user	These examples illustrate how to create a user account object in two operation modes.
Create new user (using direct access mode)	<p>To create a new object, SPML Provider performs the add operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <addRequest> element asks SPML Provider to create a new object. • The <containerID> element specifies the distinguished name of the container in which to create the new object. • The <data> element encloses the elements that specify attribute values on the new object. Thus, in accordance with the objectClass attribute value, SPML Provider is requested to create a user account. <p>The operation response indicates whether the user account is successfully created.</p> <p>Note that in direct access mode, to provision a user account, you should complete the following steps:</p> <ul style="list-style-type: none"> • Issue a request to create a new user account (see above). • Issue a request to set the user password (see "Set user password" in "Password capability samples," later in this document). • Issue a request to enable the user account (see "Resume user account" in "Suspend capability samples," later in this document).
Create new user (approval aware)	<p>This example illustrates how to create a user account if this operation is subject to approval by designated approvers. For more information about approval activities and workflows, refer to Active Roles Help and Active Roles SDK.</p> <p>If the creation of user is subject to approval, to perform the operation, your SPML request <i>must</i> contain the AllowApproval built-in control. For information about how to use controls in SPML requests, see Support for Active Roles controls earlier in this document.</p> <p>To create a new object, SPML Provider performs the add</p>

Operation	Description
	<p>operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <addRequest> element asks SPML Provider to create a new object. • The <controls> element includes the child element <control> that sets the AllowApproval control to the Confirm value. • The <controlsForOutput> element includes the child element <control>, which specifies that the OperationStatus control will be returned with the SPML response. • The <containerID> element specifies the distinguished name of the container in which to create the new object. • The <data> element encloses the elements that specify attribute values on the new object. Thus, in accordance with the objectClass attribute value, SPML Provider is requested to create a user account. <p>The operation response contains the OperationStatus control value that indicates the creation operation status. For example, if the user creation operation is subject to approval, the OperationStatus control returns the Pending value. In this case, the operation is waiting for approval by designated approvers. For more information about possible values of the OperationStatus control, see Active Roles SDK.</p>
Create a user whose logon name is not in compliance with Active Roles policies	<p>This example illustrates an attempt to create a new user account whose logon name does not conform to the Active Roles policies.</p> <p>Because the user logon name does not conform to the Active Roles policies, the creation operation fails and the operation response includes an error message returned by Active Roles. For example, an attempt to set the sAMAccountName attribute to a string of more than 20 characters causes the user creation operation to fail, with the response containing a message that provides some details on the error condition.</p>
Create new group	This example illustrates how to create the group object

Operation	Description
	<p>SPMLGroup in the mycompany.com domain.</p> <p>To create a new object, SPML Provider performs the add operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <addRequest> element asks SPML Provider to create a new object. • The <psoID> element specifies the distinguished name of the object to be created. • The <data> element encloses the elements that specify attribute values on the new object. Thus, in accordance with the objectClass attribute value, SPML Provider is requested to create a group object.
Modify user attributes	<p>This example illustrates how to modify the description attribute of the John Smith user object in the mycompany.com domain.</p> <p>To modify the object attribute, SPML Provider performs the modify operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <modifyRequest> element asks SPML Provider to make changes to a specified object. • The <psoID> element specifies the distinguished name of the user account to be modified. • The <modification> element specifies the type of change as replace, causing the new values to replace the existing attribute values. • The <data> element encloses the elements that specify the new attribute values.
Modify Shared mailbox user permissions	<p>Modify or replace the edsaUserMailboxSecurityDescriptorSddl attribute of the Shared mailbox object.</p> <p>To modify the object attribute, SPML Provider performs the modify operation.</p> <p>The request message includes the following XML elements:</p>

Operation	Description
	<ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <modifyRequest> element asks SPML Provider to make changes to a specified object. • The <psoID> element specifies the distinguished name of the user account to be modified. • The <modification> element specifies the type of change as replace, causing the new values to replace the existing attribute values. • The <data> element encloses the elements that specify the new attribute values, in SDDL format along with the SID of the user specified. <p>For example, see Sample request to modify Shared mailbox user permissions.</p>
Add user to group	<p>This example illustrates how to add the John Smith user account to the SPMLGroup group object in the mycompany.com domain.</p> <p>To do this, SPML Provider preforms the modify operation.</p> <ul style="list-style-type: none"> • The request message includes the following XML elements: • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <modifyRequest> element asks SPML Provider to make changes to a specified object. • The <psoID> element specifies the distinguished name of the group object to be modified. • The <modification> element specifies the type of change as add, causing the new values to be appended to the existing attribute values. • The <data> element encloses the elements that specify the distinguished name of the user account to be appended to the existing values of the member attribute.
Look up user attributes	<p>This example illustrates how to get the XML representation of the John Smith user in the mycompany.com domain.</p> <p>To get the XML representation of an object, SPML Provider performs the lookup operation.</p> <p>The request message includes the following XML elements:</p>

Operation	Description
	<ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <lookupRequest> element asks SPML Provider to return the XML document that represents a specified object. • The <psoID> element specifies the distinguished name of the object. <p>The response contains the object identifier, the XML representation of the object and its attributes, and information about SPML Provider capabilities that are supported on the object (the capability-specific data that is associated with the object).</p>
Delete user	<p>This example illustrates how to delete the John Smith user account.</p> <p>To do this, SPML Provider performs the delete operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <deleteRequest> element asks SPML Provider to delete a specified object. • The <psoID> element specifies the distinguished name of the user account to delete.
Delete group	<p>This example illustrates how to delete the SPMLGroup group object in the mycompany.com domain.</p> <p>To do this, SPML Provider performs the delete operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <deleteRequest> element asks SPML Provider to delete a specified object. • The <psoID> element specifies the distinguished name of the group object to delete.

Sample request to modify Shared mailbox user permissions

This section provides a sample request that illustrate how to use Active Roles controls in your SPML requests to modify Shared mailbox user permissions.

Sample request to modify Shared mailbox user permissions

```

<?xml version="1.0"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body>
<spml:modifyRequest xmlns:spml="urn:oasis:names:tc:SPML:2:0">
<spml:psoID ID="CN=shmb1,OU=NOV_OU,DC=ars,DC=cork,DC=lab,DC=local"/>
<spml:modification>
<modification name="edsaUserMailboxSecurityDescriptorSddl" operation="replace"
xmlns="urn:oasis:names:tc:DSML:2:0:core">
<value>0:PSG:PSD:AI(A;CI;RC;;;S-1-5-21-2064067869-2662360268-1970296196-3772)
(A;CI;RC;;;S-1-5-21-2064067869-2662360268-1970296196-3773)
</value>
</modification>
</spml:modification>
</spml:modifyRequest>
</soap:Body>
</soap:Envelope>

```

Capability samples

The following tables list all examples included in the Capability samples, grouped by Capability.

Search Capability samples

Table 13: Search Capability samples

Operation	Description
Perform one-level search	<p>This example illustrates how to obtain a list of the child objects (direct descendants) of the Active Directory container object. In proxy mode, you can use this example to list the domains that are registered with Active Roles (managed domains).</p> <p>To do this, SPML Provider performs the search operation. The request message includes the following XML elements:</p> <ul style="list-style-type: none"> The <soap:Envelope> and <soap:Body> SOAP elements

Operation	Description
	<p>enclose the SPML payload.</p> <ul style="list-style-type: none"> • The <searchRequest> element asks SPML Provider to perform a search and return the identifiers of the objects found. • The <query> element determines that SPML Provider is to perform a one-level search (that is, to search only direct descendants of the object specified by <basePsoID>). • The <basePsoID> element specifies the distinguished name of the container object to search. <p>The response contains the identifiers (distinguished names) of the objects residing in the container object specified by the <basePsoID> element.</p>
Perform subtree search	<p>This example illustrates how to obtain a list of objects that reside below the Active Directory object in the directory tree. You can use this example to list the objects that reside in a given domain.</p> <p>To do this, SPML Provider performs the search operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <searchRequest> element asks SPML Provider to perform a search and return the identifiers of the objects found. • The <query> element determines that SPML Provider is to perform a subtree search (that is, to search any direct or indirect descendant of the object specified by <basePsoID>). • The <basePsoID> element specifies the distinguished name of the container object to search. For instance, this could be the distinguished name of a domain that is registered with Active Roles (managed domain). <p>The response contains the identifiers (distinguished names) of the objects that reside in the directory tree below the container object specified by the <basePsoID> element.</p>
Perform base search	<p>This example illustrates how to obtain an XML representation of the specific object.</p> <p>To do this, SPML Provider performs the search operation.</p> <p>The request message includes the following XML elements:</p>

Operation	Description
	<ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <searchRequest> element asks SPML Provider to perform a search and return the XML representation of the object found. • The <query> element determines that SPML Provider is to perform a base search (that is, to search only the object identified by <basePsoID>). • The <basePsoID> element specifies the distinguished name of the object to search. For instance, this could be the distinguished name of a user account. <p>The response contains the identifier of the object and the XML representation of the object (as defined in the schema of the target).</p>
Iterate search results	<p>This example illustrates how to obtain the next set of objects from the result set that SPML Provider selected for a search operation.</p> <p>In this case, SPML Provider performs the iterate operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <iterateRequest> element asks SPML Provider to return additional objects that matched a previous search request but that the Provider has not yet returned to the client. • The <iterator> element supplies the iterator ID found either in the original search response or in a subsequent iterate response.
Stop iterating search results	<p>This example illustrates how to tell SPML Provider that the client has no further need for the search results that a specific iterator represents.</p> <p>In this case, SPML Provider performs the closeIterator operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <closeIteratorRequest> element tells SPML Provider that the client no longer intends to iterate search results.

Operation	Description
	<ul style="list-style-type: none"> The <iterator> element specifies the ID of the iterator to close. This could be the iterator ID found in the original search response or in a subsequent iterate response.
Find inactive users	<p>This example illustrates how to get a list of inactive (disabled or deprovisioned) user accounts found within a specified container.</p> <p>To do this, SPML Provider performs the search operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. The <searchRequest> element asks SPML Provider to perform a search and return the identifiers of the objects found. The <query> element determines SPML Provider is to perform a subtree search. The <basePsoID> element specifies the distinguished name of the container object to search. For instance, this could be the distinguished name of a certain organizational unit. The <filter> element encloses the elements that direct SPML Provider to search for inactive user accounts. Thus, the <equalityMatch> elements are configured so as to limit the search to user accounts; the <isActive> element combined with the <not> element causes SPML Provider to select the user accounts that are inactive. The response contains the identifiers (distinguished names) of the inactive user accounts that exist in the directory tree below the container object specified by the <basePsoID> element.
Perform complex search	<p>This example illustrates how to have SPML Provider find all objects that meet certain search criteria and return the values of certain attributes of the objects found.</p> <p>In this case, SPML Provider performs the search operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. The <searchRequest> element asks SPML Provider to

Operation	Description
	<p>perform a search and return the identifiers and attribute values of the objects found.</p> <ul style="list-style-type: none"> • The <query> element determines the scope of the search. • The <basePsoID> element specifies the distinguished name of the container object to search. For instance, this could be the distinguished name of a certain organizational unit. • The <filter> element encloses the elements that specify the search criteria. • The <attributes> element specifies the object attributes to be included in the response. <p>The response contains the identifiers (distinguished names) of the objects found and, for each object, the values of the attributes specified by the <attributes> element in the search request.</p>
Find only security groups	<p>This example illustrates how to obtain a list of security groups found in a specified container.</p> <p>In this case, SPML Provider performs the search operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <searchRequest> element asks SPML Provider to perform a search and return the identifiers of the objects found. • The <query> element determines that SPML Provider is to perform a subtree search. • The <basePsoID> element specifies the distinguished name of the container object to search. For instance, this could be the distinguished name of a certain organizational unit. • The <filter> element encloses the elements that direct SPML Provider to search for security groups. Thus, the <equalityMatch> elements are configured so as to limit the search to group objects; the <extensibleMatch> element specifies a matching rule that is equivalent to the LDAP filter (groupType:1.2.840.113556.1.4.803:=2147483648) where 2147483648 is the decimal equivalent of the ADS_GROUP_TYPE_SECURITY_ENABLED flag (0x80000000).

Operation	Description
	The response contains the identifiers (distinguished names) of the security groups that exist in the directory tree below the container object specified by the <basePsoID> element.

Password Capability samples

Table 14: Password capability samples

Operation	Description
Set user password	<p>This example illustrates how to set a new password for the specific user account.</p> <p>To set a new password, SPML Provider performs the setPassword operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <setPasswordRequest> element asks SPML Provider to change to a specified value the password that is associated with a certain user account. • The <psoID> element specifies the distinguished name of the user account. • The <password> element specifies the new password to assign to the user account.
Expire user password	<p>This example illustrates how to force a given user to change the password at next logon.</p> <p>To do this, SPML Provider performs the expirePassword operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <expirePasswordRequest> element asks SPML Provider to mark expired the current password that is associated with a certain user account. The remainingLogins attribute is set to 1 so as to disallow grace logons once the expirePassword operation is completed, forcing the user to change the password at next logon. • The <psoID> element specifies the distinguished name of the user account.

Suspend Capability samples

Table 15: Suspend capability samples

Operation	Description
Suspend user account	<p>This example illustrates how to either disable or deprovision a specified user account, depending on the SPML Provider configuration (see the description of the <code><suspendAction></code> element in the "Configuring SPML Provider" section earlier in this document).</p> <p>To do this, SPML Provider performs the suspend operation.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none">• The <code><soap:Envelope></code> and <code><soap:Body></code> SOAP elements enclose the SPML payload.• The <code><suspendRequest></code> element asks SPML Provider to perform the suspend action on a certain user account (either disable or deprovision, depending on the configuration of SPML Provider).• The <code><psoID></code> element specifies the distinguished name of the user account to suspend.
Resume user account	<p>This example illustrates how to enable a disabled user account. This operation requires that the suspend action be set to disable in the SPML Provider configuration file (see the description of the <code><suspendAction></code> element in the "Configuring SPML Provider" section earlier in this document).</p> <p>In this case, SPML Provider performs the resume operation in order to enable a disabled user account.</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none">• The <code><soap:Envelope></code> and <code><soap:Body></code> SOAP elements enclose the SPML payload.• The <code><resumeRequest></code> element asks SPML Provider to re-enable a user account that has been disabled.• The <code><psoID></code> element specifies the distinguished name of the user account to re-enable.
Check whether user is active	<p>This example illustrates how to determine whether a specified user account is active, that is, has not been suspended. A user account is considered to be suspended if the suspend action was performed on that account. The suspend action can be either disable or deprovision, depending on the SPML Provider configuration (see the description of the <code><suspendAction></code> element in the</p>

Operation	Description
	<p>"Configuring SPML Provider" section earlier in this document).</p> <p>The request message includes the following XML elements:</p> <ul style="list-style-type: none"> • The <soap:Envelope> and <soap:Body> SOAP elements enclose the SPML payload. • The <activeRequest> element asks SPML Provider to check whether the suspend action has been performed on a given user account (either disable or deprovision, depending on the SPML Provider configuration). • The <psoID> element specifies the distinguished name of the user account to check. <p>The <activeResponse> element in the response message has the active attribute that indicates whether the specified user account is suspended. If the user account is suspended, the active attribute is set to false. Otherwise, the active attribute is set to true.</p>

Active RolesSPML Provider terminology

Direct Access Mode

In this mode, SPML Provider directly connects to the specified domain or AD LDS instance.

Capabilities

A set of optional, functionally related operations defined in SPML v2.

Core Operations

The minimum set of operations that a provider must implement to conform to the official SPML v2 specification.

Extensible Markup Language (XML)

A meta-markup language that provides a format for describing structured data. This facilitates more precise declarations of content and more meaningful search results across multiple platforms. In addition, XML enables a new generation of Web-based data viewing and manipulation applications.

Organization for the Advancement of Structured Information Standards (OASIS)

An international consortium that drives the development, convergence, and adoption of e-business and Web service standards.

Provider

See Provisioning Service Provider.

Provisioning Service Object (PSO)

Represents a data entity or an information object on a target.

Provisioning Service Provider (PSP)

A software component that listens for, processes, and returns the results for well-formed SPML requests from a known requestor.

Provisioning Service Target (PST)

Represents a destination or endpoint that a provider makes available for provisioning actions.

Proxy Mode

In proxy mode, SPML Provider accesses directory data using the Active Roles proxy service.

Requesting Authority (RA)

A software component that issues well-formed SPML requests to a Provisioning Service Provider.

Requestor

See Requesting Authority.

Simple Object Access Protocol (SOAP)

An XML/HTTP-based protocol for platform-independent access to objects and services on the Web. SOAP defines a message format in XML that travels over the Internet using HyperText Transfer Protocol (HTTP). By using existing Web protocols (HTTP) and languages (XML), SOAP runs over the existing Internet infrastructure without being tied to any operating system, language, or object model.

SPML

An XML-based framework for exchanging user, resource, and service provisioning information between cooperating organizations.

SPML v2

An OASIS standard that provides a means of representing provisioning requests and responses as SPML documents.

Target

See Provisioning Service Target.

Target Schema

Defines the XML structure of the objects (PSO) that the target may contain.

Troubleshooting SPML Provider

This section briefly discusses some error statements that you may encounter when using SPML Provider.

Cannot remove the specified item because it was not found in the specified Collection

When sending a request to remove a user from a group (see the example below), the requested operation fails with the error statement "Cannot remove the specified item because it was not found in the specified Collection."

Resolution

This error has one of the following causes:

- The <value> element of the <attr> element specifies a user account that is not a member of the group.
- The Distinguished Name fields, such as CN or OU, used in the distinguished name of the user account to be removed, have invalid spelling or case. The Distinguished Name fields must be in upper case. So the use of cn=Robert Smith instead of CN=Robert Smith generates this error.

Verify that the <value> element specifies the distinguished name of the user that is the group member. Make sure that the Distinguished Name fields are in upper case.

The following example illustrates how to create a request to remove user **Robert Smith** from the **Sales** group.

```
<?xml version="1.0"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <modifyRequest xmlns="urn:oasis:names:tc:SPML:2:0" returnData="everything">
      <psoID ID="CN=Sales,OU=SPML2,DC=Mycompany,DC=com"/>
      <modification modificationMode="delete">
        <data>
          <attr name="member" xmlns="urn:oasis:names:tc:DSML:2:0:core">
            <value>CN=Robert Smith,OU=Staff,DC=MyCompany,DC=com</value>
          </attr>
        </data>
      </modification>
    </modifyRequest>
  </soap:Body>
</soap:Envelope>
```

Some of the specified attributes for the '*<object class name>*' object class are not defined in the schema

When sending a request to change values of an object virtual attribute, the requested operation fails with the error statement "Some of the specified attributes for the '*<object class name>*' object class are not defined in the schema."

Resolution

This error has one of the following causes:

- The `spmlschema.config` configuration file has changed since you started SPML Provider.
- The Default Application Pool idle timeout period has ended.

To resolve this issue, recycle the Default Application Pool or change its settings using Internet Information Services (IIS) Manager.

What's new

This version of Active RolesSPML Provider has the same features and functions as the previous version, 1.4.0. The new version adds support for:

- Active Roles 7.4, allowing you to use the latest version of the Active Roles Administration Service.
- Adding users, groups, and contacts in Azure AD.

This version of Active RolesSPML Provider requires a 64-bit (x64) operating system, and cannot be installed on a 32-bit (x86) system (see [System requirements](#) earlier in this document).

Skype for Business Server Solution

The Skype for Business Server User Management solution enables Active Roles to administer Skype for Business Server user accounts. This solution provides built-in policies that synchronize user account information between Active Roles and Skype for Business Server, allowing Skype for Business Server user management tasks to be performed using Active Roles Web Interface.

- [Introducing Skype for Business Server User Management](#)
- [Supported Active Directory topologies](#)
- [User Management policy](#)
- [Master Account Management policy](#)
- [Access Templates for Skype for Business Server](#)

Introducing Skype for Business Server User Management

With Skype for Business Server User Management, you can use Active Roles to perform the following tasks:

- Add and enable new Skype for Business Server users
- View or change Skype for Business Server user properties and policy assignments
- Move Skype for Business Server users from one Skype for Business Server pool to another
- Disable or re-enable user accounts for Skype for Business Server
- Remove users from Skype for Business Server

Skype for Business Server User Management adds the following elements to Active Roles:

- Built-in Policy Object containing a policy that enables Active Roles to perform user management tasks on Skype for Business Server.

- Built-in Policy Object containing a supplementary policy that enables Active Roles to administer Skype for Business Server users in environments that involve multiple Active Directory forests.
- Commands and pages for managing Skype for Business Server users in the Active Roles Web Interface.
- Access Templates to delegate Skype for Business Server user management tasks.

The Skype for Business Server User Management policy allows you to control the following factors of Skype for Business Server user creation and administration:

- Rule for generating the SIP user name. When adding and enabling a new Skype for Business Server user, Active Roles can generate a SIP user name based on other properties of the user account.
- Rule for selecting a SIP domain. When configuring the SIP address for a Skype for Business Server user, Active Roles can restrict the list of selectable SIP domains and suggest which SIP domain to select by default.
- Rule for selecting a Telephony option. When configuring Telephony for a Skype for Business Server user, Active Roles can restrict the list of selectable Telephony options and suggest which option to select by default.
- Rule for selecting a Skype for Business Server pool. When adding and enabling a new Skype for Business Server user, Active Roles can restrict the list of selectable registrar pools and suggest which pool to select by default. This rule also applies to selection of the destination pool when moving a Skype for Business Server user from one pool to another.

Skype for Business Server User Management provides a number of Access Templates allowing you to delegate the following tasks in Active Roles:

- Add and enable new Skype for Business Server users
- View existing Skype for Business Server users
- View or change the SIP address for Skype for Business Server users
- View or change the Telephony option and related settings for Skype for Business Server users
- View or change Skype for Business Server user policy assignments
- Disable or re-enable user accounts for Skype for Business Server
- Move users from one Skype for Business Server pool to another
- Remove users from Skype for Business Server

Supported Active Directory topologies

Skype for Business Server User Management supports the same Active Directory Domain Services (AD DS) topologies as Microsoft Lync 2013. The following topologies are supported:

- Single forest with a single tree or multiple trees
- Multiple forests in a resource forest topology
- Multiple forests in a central forest topology

Single forest

The single forest topology assumes that the logon-enabled user accounts managed by Active Roles are defined in the Active Directory forest in which Skype for Business Server is deployed. To perform Skype for Business Server user management tasks on a given user account, Active Roles makes changes to the attributes of that user account, and then, based on the attribute changes, the Skype for Business Server User Management policy requests the Skype for Business Server remote shell to update the user account accordingly. For example, when creating a new Skype for Business Server user, Active Roles sets a virtual attribute on that user's account directing the policy to invoke the remote shell command for enabling the new user for Skype for Business Server. When making changes to an existing Skype for Business Server user, Active Roles populates the attributes of the user's account with the desired changes, causing the policy to apply those changes via the remote shell.

Multiple forests - Resource forest

The resource forest topology refers to a multi-forest environment where a separate forest—Skype for Business Server forest—hosts servers running Skype for Business Server but does not host any logon-enabled user accounts. Outside the Skype for Business Server forest, user forests host logon-enabled user accounts but no servers running Skype for Business Server. When creating a Skype for Business Server account for a user from an external forest, Active Roles creates a disabled user account in the Skype for Business Server forest, establishes a link between the user account in the user forest (master account) and the disabled user account in the Skype for Business Server forest (shadow account), and enables the shadow account for Skype for Business Server. The Master Account Management policy then ensures that the attributes of the shadow account are synchronized with the attributes of the master account, so that Skype for Business Server user properties can be administered on the master account via Active Roles. In the Skype for Business Server forest, the User Management policy detects the attribute changes replicated from the master account to the shadow account, and translates them to remote shell commands on Skype for Business Server, similarly to the [Single forest](#) case.

Multiple forests - Central forest

The central forest topology refers to a multi-forest environment where a separate forest—Skype for Business Server forest—hosts servers running Skype for Business Server and may also host logon-enabled accounts. Outside the Skype for Business Server forest, user

forests host logon-enabled user accounts but no servers running Skype for Business Server.

With the Skype for Business Server User Management policy applied to logon-enabled user accounts in the Skype for Business Server forest, Active Roles can enable and administer those user accounts for Skype for Business Server in the same way as in the [Single forest](#) case.

When creating a Skype for Business Server account for a user from an external forest, Active Roles creates a contact in the Skype for Business Server forest, establishes a link between the user account in the user forest (master account) and the contact in the Skype for Business Server forest (shadow account), and enables that contact for Skype for Business Server. The Master Account Management policy then ensures that the attributes of the contact are synchronized with the attributes of the user account, so that Skype for Business Server user properties can be administered on the user account via Active Roles. In the Skype for Business Server forest, the User Management policy detects the attribute changes replicated from the user account to the contact, and translates them to remote shell commands on Skype for Business Server, similarly to the [Single forest](#) case.

User Management policy

The User Management policy is intended for single-forest and multi-forest environments where logon-enabled accounts of Skype for Business Server users are defined in the Active Directory forest in which Skype for Business Server is deployed, as well as for multi-forest environments where logon-enabled master accounts of Skype for Business Server users are defined in external forests with each master account being represented by a shadow account (disabled user account or contact) in the Active Directory forest in which Skype for Business Server is deployed. The User Management policy enables Active Roles to perform user management tasks on Skype for Business Server.

The Policy Object that holds this policy is in the **Configuration/Policies/Administration/Builtin** container. The name of the Policy Object is **Built-in Policy - Skype for Business - User Management**. Depending upon your Active Directory topology, apply this Policy Object as follows to enable Skype for Business Server User Management in Active Roles.

Table 16: Applying the Built-in - Skype for Business - User Management Policy Object

Topology option	Where to apply the Policy Object
Single forest	Apply this Policy Object to Active Directory domains or containers that hold user accounts you want to administer by using Skype for Business Server User Management in Active Roles.
Multiple forests	Apply this Policy Object to

Topology option	Where to apply the Policy Object
- Resource forest	Active Directory domains or containers in the Skype for Business Server forest that hold shadow accounts (disabled user accounts) for users from external forests you want to administer by using Skype for Business Server User Management in Active Roles.
Multiple forests - Central forest	<p>Apply this Policy Object to</p> <p>Active Directory domains or containers in the Skype for Business Server forest that hold logon-enabled user accounts you want to administer by using Skype for Business Server User Management in Active Roles</p> <p>Active Directory domains or containers in the Skype for Business Server forest that hold shadow accounts (contacts) for users from external forests you want to administer by using Skype for Business Server User Management in Active Roles.</p>

User Management policy settings

The topics in this section cover the User Management policy settings.

Connection to Skype for Business Server

To administer Skype for Business Server users, Active Roles requires a connection to a computer running the following server role in your Skype for Business Server deployment: Front End Server (in case of Skype for Business Server Enterprise Edition) or Standard Edition Server. The computer must be from an Active Directory domain that is registered with Active Roles as a managed domain. By using the **Server** policy setting, you can specify how you want Active Roles to select a Skype for Business Server computer:

- **Connect to any available server** With this option, Active Roles attempts to connect to any Front End Server or Standard Edition Server that runs the Central Management Server in your Skype for Business Server deployment. If no Central Management Server role holders are available in the managed domains, then Active Roles attempts to connect to the first Front End Server or Standard Edition Server found in the managed domains.
- **Connect to these servers only** This option allows you to configure a list from which you want Active Roles to select a Skype for Business Server computer. You can:
 - Add or remove computers from the list. Active Roles searches the managed domains for computers running the appropriate Skype for Business Server role, allowing you to select the desired computers.

- Set the default computer. Active Roles first attempts to connect to that computer.
- Reorder the list. Active Roles first attempts to connect to computers that are higher in the list.

Note that at least one of your Active Directory domains that hold computers running the Front End Server or Standard Edition Server must be registered with Active Roles as a managed domain. Otherwise, Active Roles is unable to discover your Skype for Business Server deployment, so Skype for Business Server User Management functions are unavailable.

SIP user name generation rule

The **SIP User Name** policy setting allows you to configure a rule for generating the SIP user name based on other properties of the user account. When adding a new Skype for Business Server user, Active Roles uses that rule to generate the SIP user name on the Web Interface page for enabling users for Skype for Business Server. The rule has an effect if you select the SIP address option that provides for entering a SIP user name. On the page where you edit Skype for Business Server users, the rule performs a validation function, preventing changes to the SIP user name that violate the rule.

To configure a rule, you set up a value that acts as a template for the SIP user name. You can add one or more entries to the value, with each entry representing one of the following:

- **Text** A text string. You can type the desired text when adding the entry.
- **User Property** A particular property of the user account. You can choose the desired property and specify whether you want the entry to include the entire property or a part of the property.
- **Parent OU Property** A particular property of the Organizational Unit that holds the user account. You can choose the desired property and specify whether you want the entry to include the entire property or a part of the property.
- **Parent Domain Property** A particular property of the Active Directory domain that holds the user account. You can choose the desired property and specify whether you want the entry to include the entire property or a part of the property.

The rule sets the SIP user name to the string value obtained by calculating each entry and then concatenating the calculation results so that they form a single string value.

By default, the policy allows the generated name to be modified. The **SIP User Name** policy setting provides the option to prevent changing the generated name. If you select that option, the SIP user name is read-only on the Web Interface page for enabling users for Skype for Business Server.

SIP domain restriction rule

The **SIP Domain** policy setting allows you to configure a rule that restricts selection of a SIP domain for the user SIP address. When you add a new Skype for Business Server user or edit an existing Skype for Business Server user, this rule determines the list from which you can select a SIP domain for the user's SIP address. In case of adding a new Skype for Business Server user, the rule applies to any SIP address option that involves selecting a SIP domain from the list.

To configure a rule, you choose one of these policy options:

- **Allow selection of any SIP domain** With this option, the policy does not restrict the list of SIP domains.
- **Restrict selection to these SIP domains** This option allows you to configure a list of acceptable SIP domains. You can:
 - Add or remove SIP domains from the list. Active Roles identifies all SIP domains that exist in your Skype for Business Server deployment, allowing you to select the desired SIP domains.
 - Set the default SIP domain. When creating a SIP address, Active Roles selects the specified SIP domain by default.
 - Reorder the list. When prompting to select a SIP domain for a user's SIP address, Active Roles lists the SIP domain names in the order specified.

Pool restriction rule

The **Pool** policy setting allows you to configure a rule that restricts selection of an Enterprise Edition Front End pool or Standard Edition server to which Skype for Business Server users can be assigned. When you add a new Skype for Business Server user, this rule determines the list from which you can select a pool for the new user. When you move a Skype for Business Server user from one pool to another, this rule determines the list from which you can select the destination pool.

To configure a rule, you choose one of these policy options:

- **Allow selection of any pool** With this option, the policy does not restrict the list of pools.
- **Restrict selection to these pool** This option allows you to configure a list of acceptable pools. You can:
 - Add or remove pools from the list. Active Roles identifies all Front End pools and Standard Edition servers in your Skype for Business Server deployment, allowing you to select the desired pools or servers.
 - Set the default pool. When adding a new Skype for Business Server user or moving a user to another pool, Active Roles selects the specified pool by default.
 - Reorder the list. When prompting to select a pool, Active Roles lists the pools in the order specified.

Telephony restriction rule

The **Telephony** policy setting allows you to configure a rule that restricts selection of a Telephony option for Skype for Business Server users. When you add or edit a Skype for Business Server user, this rule determines the list from which you can select a Telephony option.

To configure a rule, you choose one of these policy options:

- **Allow selection of any option** With this option, the policy does not restrict the list of Telephony options.
- **Restrict selection to these options** This option allows you to configure a list of acceptable Telephony options. You can:
 - Add or remove Telephony options from the list.
 - Set the default Telephony option. When adding a new Skype for Business Server, Active Roles selects the specified Telephony option by default.
 - Reorder the list. When prompting to select a Telephony option, Active Roles lists the options in the order specified.

Master Account Management policy

The Master Account Management policy is intended for multi-forest environments where logon-enabled master accounts of Skype for Business Server users are defined in Active Directory forests in which Skype for Business Server isn't deployed, with each master account being represented by a shadow account (disabled user account or contact) in the Active Directory forest in which Skype for Business Server is deployed (see [Multiple forests - Resource forest](#) and [Multiple forests - Central forest](#) earlier in this document). The Master Account Management policy enables Active Roles to control master accounts of Skype for Business Server users, and operates in conjunction with the [User Management policy](#) that controls shadow accounts in the Skype for Business Server forest.

The Policy Object that holds this policy is in the **Configuration/Policies/Administration/Builtin** container. The name of the Policy Object is **Built-in Policy - Skype for Business - Master Account Management**. Depending upon your Active Directory topology, apply this Policy Object as follows to enable Skype for Business Server User Management in Active Roles.

Table 17: Applying the Built-in - Skype for Business - Master Account Management Policy Object

Topology option	How to apply the Policy Object
Single forest	Do not apply this Policy Object
Multiple forests	Configure the Forest Mode policy setting by selecting the Resource

Topology option	How to apply the Policy Object
- Resource forest	<p>forest option, and then apply this Policy Object to</p> <p>Active Directory domains or containers that hold logon-enabled user accounts in external forests (master accounts) you want to administer by using Skype for Business Server User Management in Active Roles.</p>
Multiple forests - Central forest	<p>Configure the Forest Mode policy setting by selecting the Central forest option, and then apply this Policy Object to</p> <p>Active Directory domains or containers that hold logon-enabled user accounts in external forests (master accounts) you want to administer by using Skype for Business Server User Management in Active Roles.</p>

Master Account Management policy settings

The topics in this section cover the Master Account Management policy settings.

Skype for Business Server forest mode

The Master Account Management policy is intended for multi-forest environments where the Skype for Business Server forest is used either as a resource forest or as a central forest. In the central forest mode, the Skype for Business Server forest may hold logon-enabled Skype for Business Server user accounts in addition to shadow accounts (contacts) for Skype for Business Server users from external forests. In the resource forest mode, the Skype for Business Server forest holds only shadow accounts (logon-disabled user accounts) for Skype for Business Server users from external forests. The **Forest Mode** policy setting allows you to choose the option that matches the Skype for Business Server forest mode in your Skype for Business Server deployment:

- **Resource forest** The policy creates and administers logon-disabled user accounts as shadow accounts for Skype for Business Server users from external forests. The user account from an external forest, referred to as a master account, is linked and synchronized with the shadow account that is enabled for Skype for Business Server in the Skype for Business Server forest.
- **Central forest** The policy creates and administers contact objects as shadow accounts for Skype for Business Server users from external forests. The user account from an external forest, referred to as a master account, is linked and synchronizes with the contact that is enabled for Skype for Business Server in the Skype for Business Server forest.

Container for new shadow accounts

The Master Account Management policy allows you to specify the container in which you want Active Roles to create shadow accounts when enabling master accounts for Skype for Business Server. You can select the desired organizational unit in the Skype for Business Server forest or you can let Active Roles choose the default container.

If you select a particular organizational unit, Active Roles creates shadow accounts in that organizational unit. You can select an organizational unit from any domain of the Skype for Business Server forest that is registered with Active Roles as a managed domain.

If you let Active Roles choose the default container for new shadow accounts, then Active Roles creates shadow accounts in the **Users** container in a particular domain of the Skype for Business Server forest. If the forest root domain of the Skype for Business Server forest is registered with Active Roles as a managed domain, then Active Roles creates shadow accounts in that domain. Otherwise, Active Roles creates shadow accounts in the domain that appears first in the ordered list of the managed domains from the Skype for Business Server forest. Note that Active Roles requires at least one domain of the Skype for Business Server forest to be registered with Active Roles as a managed domain.

Default description for new shadow accounts

The Master Account Management policy allows you to specify a text to use as the default description for new shadow accounts that Active Roles creates when enabling master accounts for Skype for Business Server. Active Roles writes that text to the **Description** property of every new shadow account.

Attribute to store a reference to shadow account

By default, the policy designates the **adminDescription** attribute of the master account for storing the GUID of the shadow account, and allows you to choose a different attribute for that purpose. Exchange Resource Forest Management uses this attribute to identify the shadow account (and, consequently, the linked mailbox) when managing a given master account. The policy causes Active Roles to set this attribute on the master account when creating the linked mailbox.

Synchronized properties

The Master Account Management policy defines a list of properties to copy from the master account to the shadow account. These properties are referred to as *synchronized properties*. When you use Active Roles to set or change a synchronized property of a master account, the policy causes Active Roles to set or change the value of that property on both the master account and shadow account.

In addition, Skype for Business Server User Management provides a scheduled task that copies synchronized properties from every managed master account to the corresponding shadow account. The task runs on a scheduled basis to ensure that each of the synchronized properties of the shadow account has the same value as the corresponding property of the master account. If a synchronized property of the shadow account has changed for whatever reason, Active Roles changes that property back to the value found on the master account. For further details, see [Scheduled synchronization](#) later in this document.

The following table provides the default list of synchronized properties. You can configure the policy to synchronize additional properties or remove individual properties from synchronization.

Table 18: Default list of synchronized properties

c (Country Abbreviation)	physicalDeliveryOfficeName (Office Location)
co (Country)	postalCode (ZIP/Postal Code)
company (Company)	postOfficeBox (Post Office Box)
countryCode (Country-Code)	sAMAccountName (Logon Name (pre-Windows 2000))
department (Department)	sn (Last Name)
displayName (Display Name)	st (State/Province)
givenName (First Name)	streetAddress (Street Address)
homePhone (Home Phone)	telephoneNumber (Telephone Number)
initials (Initials)	title (Job Title)
l (City)	url (Web Page Address (Others))
mobile (Mobile Number)	wWWHomePage (Web Page Address)
otherTelephone (Phone Number (Others))	

Substituted properties

The Master Account Management policy defines a list of properties that appear on the master account but reflect the properties of the shadow account. These properties are referred to as *substituted properties*. When you use Active Roles to view properties of a master account, the policy causes Active Roles to retrieve the values of the master account's substituted properties from the shadow account. When you use Active Roles to set or change a substituted property of a master account, the policy causes Active Roles to set or change the value of that property on the shadow account.

The policy does not allow you to narrow down the list of substituted properties. However, you can specify your custom list of substituted properties in addition to the default list. If you do so, the resulting list of substituted properties includes all properties from both the default list and your custom list.

Table 19: Default list of substituted properties

edsva-Skype for Business-AccountExists	edsva-Skype for Business-Move
edsva-Skype for Business-ArchivingPolicy	edsva-Skype for Business-MoveTargetRegistrarPool
edsva-Skype for Business-ClientPolicy	edsva-Skype for Business-PersistentChatPolicy
edsva-Skype for Business-ClientVersionPolicy	edsva-Skype for Business-PIN
edsva-Skype for Business-ConferencingPolicy	edsva-Skype for Business-PINPolicy
edsva-Skype for Business-DialPlanPolicy	edsva-Skype for Business-PrivateLine
edsva-Skype for Business-Disable	edsva-Skype for Business-ReEnable
edsva-Skype for Business-Enable	edsva-Skype for Business-RegistrarPool
edsva-Skype for Business-ExchangeArchivingPolicy	edsva-Skype for Business-SIPAddress
edsva-Skype for Business-ExternalAccessPolicy	edsva-Skype for Business-SIPAddressType
edsva-Skype for Business-HostedVoiceMail	edsva-Skype for Business-SIPDomain
edsva-Skype for Business-IsEnabled	edsva-Skype for Business-SIPUserName
edsva-Skype for Business-LineServerURI	edsva-Skype for Business-TasksAllowed
edsva-Skype for Business-LineURI	edsva-Skype for Business-TelephonyOption
edsva-Skype for Business-LocationPolicy	edsva-Skype for Business-TemporarilyDisable
edsva-Skype for Business-MasterAccount	edsva-Skype for Business-VoicePolicy
edsva-Skype for Business-MobilityPolicy	

Back-synchronized properties

The Master Account Management policy defines a list of properties to copy from the shadow account to the master account. By default, the list is empty. If you add a property to that list, the policy ensures that any changes to that property on the shadow account are replicated to the master account.

Master Account Management policy actions

The Master Account Management policy causes Active Roles to perform the following actions depending on the change request submitted to the Active Roles Administration Service.

Table 20: Policy Actions

Request	Actions
Enable an existing Active Directory user for Skype for Business Server	<p>Active Roles retrieves the properties of the existing user (in the external forest), and then performs the following actions:</p> <ul style="list-style-type: none"> • Create a shadow account in the Skype for Business Server forest, and populate its properties with the properties of the user from the external forest • Enable the shadow account for Skype for Business Server • Set the msRTCSIP-OriginatorSID attribute of the shadow account to the value of the objectSID attribute of the user from the external forest • Create a reference to the shadow account on the master account <p>If the user from the external forest already has a shadow account (for example, created by Exchange Resource Forest Management), then the policy re-uses the existing shadow account instead of creating a new one.</p> <p>When creating the shadow account, Active Roles executes all policies that are applied to the container that holds the shadow account.</p>
Modify Skype for Business Server user properties of a master account	<p>If the change request includes any changes to substituted properties, Active Roles first makes the requested changes to the substituted properties of the shadow account. Next, Active Roles makes the requested changes to the properties of the master account, and then updates the synchronized properties of the shadow account with the new property values found on the master account.</p>
Deprovision a master account	<p>Active Roles deprovisions the master account, and then temporarily disables the shadow account for Skype for Business Server.</p>
Undeprovision a deprovisioned master account	<p>Active Roles undeprovisions the master account and then re-enables the shadow account for Skype for Business Server.</p> <p>For undeprovisioning master accounts to have an effect on shadow accounts, the container that holds deprovisioned master accounts must be in the scope of the Built-in Policy - Skype for Business - Master Account Management Policy Object (or a copy of that Policy Object).</p>
Delete a master account	<p>Active Roles deletes the master account, and then removes the shadow account from Skype for Business Server.</p>

The Master Account Management policy requires that shadow accounts be in the scope of the [User Management policy](#) provided by Skype for Business Server User Management.

This enables Active Roles to perform the Skype for Business Server related actions on the shadow account.

Scheduled synchronization

Skype for Business Server User Management includes an Active Roles scheduled task that complements the Master Account Management policy to enforce synchronization of master and shadow account properties, and to capture existing Skype for Business Server users whose master account happens to fall under the control of that policy. The scheduled task object is in the **Configuration/Server Configuration/Scheduled Tasks/Built-in** container. The name of the object is **Skype for Business - Master Account Management**. The task is scheduled to run on a daily basis. Normally, you do not need to modify that scheduled task.

The operation of the task affects only the user accounts that are in the scope of the **Built-in Policy - Skype for Business - Master Account Management** Policy Object (or a copy of that Policy Object). When run, the task performs the following actions on each of those user accounts:

- If the user account does not have a shadow account that is enabled for Skype for Business Server, then skip over that user account.
- If the user account has a shadow account that is enabled for Skype for Business Server but does not store a reference to that shadow account, then create the reference to the shadow account on that user account.

This action enables Skype for Business Server User Management to administer exiting Skype for Business Server users, possibly enabled for Skype for Business Server by using an earlier version of Skype for Business Server User Management or without the use of Skype for Business Server User Management.

- If the user account has a shadow account that is enabled for Skype for Business Server and stores a reference to the shadow account, then copy the synchronized properties from the master account to the shadow account, and copy the back-synchronized properties from the shadow account to the master account.

This action ensures that the shadow account properties are updated with the latest changes to the master account properties and vice versa.

Access Templates for Skype for Business Server

Skype for Business Server User Management provides a number of Access Templates allowing you to delegate the tasks of managing Skype for Business Server users in Active Roles. You can find these Access Templates in the **Configuration/Access Templates/Skype for Business Server** container:

Table 21: Skype for Business Server User Management Access

Access Template	Description
Skype for Business Server - User Full Control	<p>Gives permission to perform the following tasks by using Active Roles:</p> <ul style="list-style-type: none">• Add and enable new Skype for Business Server users• View existing Skype for Business Server users• View or change the SIP address• View or change the telephony option and related settings• View or change the user policy assignments in Skype for Business Server• Temporarily disable or re-enable users for Skype for Business Server• Move users to another server or pool in Skype for Business Server• Remove users from Skype for Business Server
Skype for Business Server - User Telephony	<p>Gives permission to perform the following tasks by using Active Roles:</p> <ul style="list-style-type: none">• View existing Skype for Business Server users• View the SIP address• View or change the telephony option and related settings• View the user policy assignments in Skype for Business Server
Skype for Business Server - User Disable/Re-enable	<p>Gives permission to perform the following tasks by using Active Roles:</p> <ul style="list-style-type: none">• View existing Skype for Business Server users• View the SIP address• View the telephony option and related settings• View the user policy assignments in Skype for Business Server• Temporarily disable or re-enable users for Skype for Business Server
Skype for Business Server - User Policies	<p>Gives permission to perform the following tasks by using Active Roles:</p>

Access Template	Description
	<ul style="list-style-type: none"> • View existing Skype for Business Server users • View the SIP address • View the telephony option and related settings • View or change the user policy assignments in Skype for Business Server

When applying Access Templates for Skype for Business Server User Management, consider your Active Directory topology.

Table 22: Applying Access templates for Skype for Business Server User Management

Topology option	Where to apply Access Templates
Single forest	<p>Apply Access Templates to Active Directory domains and containers to which the Built-in Policy - Skype for Business - User Management Policy Object (or a copy of that Policy Object) is applied, to allow access to user accounts of Skype for Business Server users managed by Active Roles.</p>
Multiple forests - Resource forest	<p>Apply Access Templates to Active Directory domains and containers in external forests to which the Built-in Policy - Skype for Business - Master Account Management Policy Object (or a copy of that Policy Object) is applied, to allow access to master accounts of Skype for Business Server uses managed by Active Roles.</p> <p>You do not need to apply these Access Templates in the Skype for Business Server forest.</p>
Multiple forests - Central forest	<p>Apply Access Templates to Active Directory domains and containers in external forests to which the Built-in Policy - Skype for Business - Master Account Management Policy Object (or a copy of that Policy Object) is applied, to allow access to master accounts of Skype for Business Server uses managed by Active Roles.</p> <p>Apply Access Templates to Active Directory domains and containers in the Skype for Business Server forest to which the Built-in Policy - Skype for Business - User Management Policy Object (or a copy of that Policy Object) is applied, to allow access to logon-enabled user accounts of Skype for Business Server users managed by Active Roles in the Skype for Business Server forest.</p>

Deploying the Solution

- [Prerequisite conditions](#)
- [Deployment in a single-forest environment](#)
- [Deployment in a multi-forest environment](#)
- [Upgrade from an earlier version](#)

Prerequisite conditions

This section summarizes the prerequisite conditions that must be met before you deploy Exchange Resource Forest Management.

Skype for Business Server deployment

With Skype for Business Server User Management, you can perform user management on Microsoft Lync 2013 with limited support.

Single forest

In case of single forest, Skype for Business Server must be deployed in the forest that holds logon-enabled accounts for Skype for Business Server users. For further details, see [Single forest](#) earlier in this document.

Multiple forests

In case of multiple forests, Skype for Business Server must be deployed in the Skype for Business Server forest only. You don't need to deploy Skype for Business Server in external user forests or extend the Active Directory schema with Skype for Business Server attributes in those forests. For further details about multi-forest topology options, see [Multiple forests - Resource forest](#) and [Multiple forests - Central forest](#) earlier in this document.

Active Directory forest trust

The multi-forest topology option requires a one-way trust relationship between the Skype for Business Server forest and each user forest so that users can authenticate to the user forest but access services in the Skype for Business Server forest. Create a "forest" trust instead of an "external" trust because an external trust only supports NTLM, while a forest trust supports both NTLM and Kerberos, and therefore won't limit Skype for Business client authentication options.

Trusts are configured as one-way to prevent unauthorized access to the user forest from the Skype for Business Server forest. For details, see "How Domain and Forest Trusts Work" at <http://technet.microsoft.com/library/cc773178.aspx>.

Skype for Business Server contact management rights

In case of central forest deployment, you need to grant Skype for Business Server contact management rights on the container that is intended to hold shadow accounts (contacts enabled for Skype for Business Server in the Skype for Business Server forest). Otherwise, Skype for Business Server security groups do not have sufficient rights to manage contact objects, which causes an "access is denied" condition when Active Roles attempts to enable a shadow account for Skype for Business Server.

To grant Skype for Business Server contact management rights, use the following command in Skype for Business Server Management Shell:

```
Grant-CsOUPermission -OU "<DN of container>" -ObjectType "contact"
```

Replace <DN of container> with the Distinguished Name of the container that is intended to hold shadow accounts, for example: OU=Shadow Accounts,DC=Skype for BusinessServer,DC=lab. If the domain does not have permission inheritance disabled (which is the default case), then you can supply the Distinguished Name of the domain rather than container:

```
Grant-CsOUPermission -OU "DC=Skype for BusinessServer,DC=lab" -ObjectType "contact"
```

You must be a domain administrator in order to run the Grant-CsOUPermission cmdlet locally.

Active Roles deployment

The following Active Roles components must be installed in your Active Directory environment:

- Administration Service
- Web Interface
- Active Roles console

You can install these components on member servers in an accounts forest or in the Exchange forest. For installation instructions, see the Active Roles Quick Start Guide.

Log on as Active Roles Admin

To configure Skype for Business Server User Management, log on as Active Roles Admin. This ensures that you have sufficient rights to make the necessary configuration changes. Assuming the default configuration of the Active Roles Administration Service, you should log on with a domain user account that is a member of the Administrators group on the computer running the Administration Service.

Register domains with Active Roles

Skype for Business Server User Management requires the following domains to be registered with Active Roles:

- At least one domain that holds computers running the Front End Server or Standard Edition Server role in your Skype for Business Server deployment
- Domains that hold logon-enabled users you are going to administer with Skype for Business Server User Management
- In case of multi-forest topology, the domain in the Skype for Business Server forest that holds shadow accounts for Skype for Business Server users

When registering a domain, you are prompted to choose which account you want the Administration Service to use to access the domain. You can either specify a so-called *override account* or let the Administration Service use its service account. With either option, the account must have sufficient rights in the domain you are registering. At a minimum, the account must have the following rights:

- In the domain that holds Skype for Business Server computers, a member of the **RTCUniversalUserAdmins** group
- In the user domains, a member of the **Account Operators** group
- In the shadow accounts domain, a member of the **Account Operators** group

For a central forest deployment, the account must also have the rights to create, view, modify and delete contact objects in the shadow accounts domain. It will suffice to make the account a member of the **Domain Admins** group.

For instructions on how to register domains with Active Roles, see “Adding and removing managed domains” in the Active Roles Administrator Guide.

Deployment in a single-forest environment

In a single-forest environment, you only need to link the **Built-in Policy - Skype for Business - User Management** Policy Object to the Active Directory domains or containers that hold user accounts for which you want Active Roles to perform Skype for Business Server user management tasks.

To link the Policy Object to an organizational unit or domain

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.
2. In the details pane, right-click the **Built-in Policy - Skype for Business - User Management** Policy Object, and then click **Policy Scope**.
3. In the dialog box that appears, click **Add**, and then select the desired organizational unit or domain.

Out of the box, the Policy Object has all policy settings configured. You can use the Active Roles console to view or change policy settings as needed.

To view or change policy settings

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.
2. In the details pane, double-click the **Built-in Policy - Skype for Business - User Management** Policy Object.
3. In the **Properties** dialog box that appears, go to the **Policies** tab, and double-click the entry in the list of policies.
4. In the **Properties** dialog box that appears, do any of the following:
 - On the **Server** tab, specify how you want Active Roles to select a computer running Skype for Business Server.
 - On the **SIP User Name** tab, configure a rule for generating the SIP user name in the user SIP address.
 - On the **SIP Domain** tab, configure a rule to restrict selection of a SIP domain for the user SIP address.
 - On the **Pool** tab, configure a rule to restrict selection of an Enterprise Edition Front End pool or Standard Edition server to which Skype for Business Server users can be assigned.
 - On the **Telephony** tab, configure a rule to restrict selection of a Telephony option for Skype for Business Server users.

For detailed description of the policy settings, see [User Management policy settings](#) earlier in this document.

Deployment in a multi-forest environment

In a multi-forest environment, you need to perform the following deployment tasks:

- [Apply the Master Account Management policy](#) Adjust the **Forest Mode** policy setting in the **Built-in Policy - Skype for Business - Master Account Management** Policy Object and then link that Policy Object to Active Directory domains or containers that hold logon-enabled user accounts in user forests (master accounts) for which you want Active Roles to perform Skype for Business Server user management tasks.
- [Apply the User Management policy](#) Link the **Built-in Policy - Skype for Business - User Management** Policy Object to Active Directory domains or containers in the Skype for Business Server forest that hold shadow accounts.

In case of central forest, you also need to link the **Built-in Policy - Skype for Business - User Management** Policy Object to Active Directory domains or containers in the Skype for Business Server forest that hold logon-enabled user accounts for which you want Active Roles to perform Skype for Business Server user management tasks.

Apply the Master Account Management policy

The **Built-in Policy - Skype for Business - Master Account Management** Policy Object enables Active Roles to perform Skype for Business Server user management tasks on user accounts in Active Directory forests that are external to the Skype for Business Server forest. It needs to be configured as appropriate to your Skype for Business Server forest mode (resource forest or central forest) and then linked to domains or containers in external user forests.

To configure the Policy Object

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.
2. In the details pane, double-click the **Built-in Policy - Skype for Business - Master Account Management** Policy Object.
3. In the **Properties** dialog box that appears, go to the **Policies** tab, and double-click the entry in the list of policies.
4. In the **Properties** dialog box that appears, go to the **Forest Mode** tab and select the option that matches the Skype for Business Server forest mode in your Skype for Business Server deployment (see [Skype for Business Server forest mode](#)).
5. Review other policy settings:
 - On the **Shadow Account** tab, view or change the container and default description for new shadow accounts.
 - On the **Master Account** tab, view or change the attribute to store a reference to shadow account.
 - On the **Synced** tab, view or change the list of synchronized properties.
 - On the **Substituted** tab, configure your custom list of substituted properties in addition to the default list.
 - On the **Back-synced** tab, view or change the list of back-synchronized properties.

For detailed description of the policy settings, see [Master Account Management policy settings](#) earlier in this document.

To link the Policy Object to an organizational unit or domain

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.
2. In the details pane, right-click the **Built-in Policy - Skype for Business - Master Account Management** Policy Object, and then click **Policy Scope**.
3. In the dialog box that appears, click **Add**, and then select the desired organizational unit or domain.

Apply the User Management policy

The **Built-in Policy - Skype for Business - User Management** Policy Object enables Active Roles to perform Skype for Business Server user management tasks on user accounts in the Skype for Business Server forest. It needs to be linked to domains or containers in the Skype for Business Server forest that hold shadow accounts. In case of central forest, you also need to link that Policy Object to Active Directory domains or containers in the Skype for Business Server forest that hold logon-enabled user accounts for which you want Active Roles to perform Skype for Business Server user management tasks.

To link the Policy Object to an organizational unit or domain

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Built-in**.
2. In the details pane, right-click the **Built-in Policy - Skype for Business - User Management** Policy Object, and then click **Policy Scope**.
3. In the dialog box that appears, click **Add**, and then select the desired organizational unit or domain.

Out of the box, the Policy Object has all policy settings configured. You can use the Active Roles console to view or change policy settings as needed.

To view or change policy settings

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Built-in**.
2. In the details pane, double-click the **Built-in Policy - Skype for Business - User Management** Policy Object.
3. In the **Properties** dialog box that appears, go to the **Policies** tab, and double-click the entry in the list of policies.
4. In the **Properties** dialog box that appears, do any of the following:
 - On the **Server** tab, specify how you want Active Roles to select a computer running Skype for Business Server.
 - On the **SIP User Name** tab, configure a rule for generating the SIP user name in the user SIP address.
 - On the **SIP Domain** tab, configure a rule to restrict selection of a SIP domain for the user SIP address.
 - On the **Pool** tab, configure a rule to restrict selection of an Enterprise Edition Front End pool or Standard Edition server to which Skype for Business Server users can be assigned.
 - On the **Telephony** tab, configure a rule to restrict selection of a Telephony option for Skype for Business Server users.

For detailed description of the policy settings, see [User Management policy settings](#) earlier in this document.

Upgrade from an earlier version

You can use the following steps to upgrade from Active Roles Add-on for Skype for Business Server to Skype for Business Server User Management:

1. Identify the Active Directory topology option used by the add-on. The possible options are:

- [Single forest](#)
- [Multiple forests - Resource forest](#)
- [Multiple forests - Central forest](#)

In case of multiple forests, note down the Distinguished Name of the container in which the add-on creates shadow accounts.

2. Uninstall the earlier version of the add-on from Active Roles Add-on Manager, and then uninstall the add-on from the system
3. Upgrade to Active Roles version 8.0 LTS. For upgrade instructions, see the Active Roles 8.0 LTS Quick Start Guide.
4. Deploy Skype for Business Server User Management. Depending on the Active Directory topology option used by the add-on:
 - In case of single forest, follow the [Deployment in a single-forest environment](#) instructions.
 - In case of multiple forests, follow the [Deployment in a multi-forest environment](#) instructions. Configure the **Built-in Policy - Skype for Business - Master Account Management** Policy Object to match the topology option and container for shadow accounts you identified in Step 1.

The following instructions elaborate on these steps. The instructions apply to Active Roles Add-on for Skype for Business Server 2.1.

To identify the Active Directory topology option used by the add-on

1. In the Active Roles console tree, select **Applications | Active Roles Add-on for Skype for Business Server**.
2. Review the add-on settings in the **Configure Add-on** area in the details pane:
 - The Active Directory topology option is selected in the **Active Directory topology** box.
 - If a multi-forest option is selected, the Distinguished Name of the container in which the add-on creates shadow accounts is specified in the **Container for shadow accounts/contacts** box.

If the add-on was configured with the resource forest or central forest option, you need to configure and apply the **Built-in Policy - Skype for Business - Master Account Management** Policy Object as follows.

To configure and apply the Master Account Management policy

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.
2. In the details pane, double-click the **Built-in Policy - Skype for Business - Master Account Management** Policy Object.
3. In the **Properties** dialog box that appears, go to the **Policies** tab, and double-click the entry in the list of policies.
4. In the **Properties** dialog box that appears, go to the **Forest Mode** tab and select the option that matches the Active Directory topology option that was used by the add-on:
 - If the add-on was configured with the option **Multiple forests - Resource forest**, then select the **Resource forest** option on the **Forest Mode** tab.
 - If the add-on was configured with the option **Multiple forests - Central forest**, then select the **Central forest** option on the **Forest Mode** tab.
5. Go to the **Shadow Account** tab and configure the policy to use the container for shadow accounts that was used by the add-on: Click **This container**, click **Browse**, and select the container.
6. Click **OK** to close the **Properties** dialog for the policy entry.
7. In the **Properties** dialog box for the Policy Object, click **Apply**, go to the **Scope** tab, and then click the **Scope** button on that tab.
8. In the dialog box that appears, add the containers that hold the master accounts you managed using the add-on, and then click **OK**.
9. Click **OK** to close the **Properties** dialog box for the Policy Object.

Skype for Business Server User Management recognizes the existing master accounts, enabling Active Roles to manage their shadow accounts for Skype for Business Server in the same way as when using the add-on. To expedite the recognition of the existing master accounts, you might execute the Master Account Management task without waiting for its scheduled run: In the Active Roles console, navigate to the **Configuration/Server Configuration/Scheduled Tasks/Builtin** container, right-click the object **Skype for Business - Master Account Management** in that container, point to **All Tasks**, and then click **Execute**.

Managing Skype for Business Server Users

The Skype for Business Server User Management solution enables Active Roles to administer Skype for Business Server users. Once you have deployed Skype for Business Server User Management, the Active Roles Web Interface can be used to perform the following tasks:

- [Enabling or disabling users for Skype for Business Server](#)
- [Managing Skype for Business Server user properties](#)

Enabling or disabling users for Skype for Business Server

By using the Active Roles Web Interface, you can enable, temporarily disable, or remove Active Directory users from Skype for Business Server.

Add and enable a new Skype for Business Server user

For an existing Active Directory user account, you can use the Active Roles Web Interface to create and enable a new Skype for Business Server user account by adding the Active Directory user to Skype for Business Server.

To add and enable a new Skype for Business Server user

1. Select the user account in the Active Roles Web Interface for administrators.
2. Click the **Enable for Skype for Business Server** command.

The command is available if you have sufficient rights in Active Roles to enable users for Skype for Business Server, and the selected account is in the scope of the policy provided by Skype for Business Server User Management and is not enabled for Skype for Business Server; otherwise, the Web Interface does not display the **Enable for Skype for Business Server** command.

3. On the page that appears, assign the user to a Skype for Business Server pool, specify any additional details, assign Skype for Business Server policies to the user as needed, and then click **Finish**.

Disable or re-enable a user account for Skype for Business Server

You can use the Active Roles Web Interface to disable a user account for logon to Skype for Business Server. This allows you to disable a previously enabled user account in Skype for Business Server while retaining all the Skype for Business Server settings that were configured for the user account. Because you do not lose the Skype for Business Server user account settings, you can re-enable a disabled user account again without having to reconfigure the user account.

To disable or re-enable a previously enabled user account for Skype for Business Server

1. In the Active Roles Web Interface for administrators, select the user account that you want to disable or re-enable.
2. Do one of the following:
 - To disable the user account, click the **Temporarily Disable for Skype for Business Server** command.
 - To re-enable the user account, click the **Re-enable for Skype for Business Server** command.

The Web Interface displays the **Temporarily Disable for Skype for Business Server** command if you have sufficient rights in Active Roles to perform that command, and the user account you have selected is in the scope of the policy provided by Skype for Business Server User Management and is enabled for Skype for Business Server.

The Web Interface displays the **Re-enable for Skype for Business Server** command if you have sufficient rights in Active Roles to perform that command, and the user account you have selected is in the scope of the policy provided by Skype for Business Server User Management and was disabled by using the **Temporarily Disable for Skype for Business Server** command.

Remove a user account from Skype for Business Server

You can use the Active Roles Web Interface to remove a user account from Skype for Business Server. This removes all the Skype for Business Server related attributes from the user account, including the identities of any per-user policies that have been assigned to that user account. You can later re-add the account to Skype for Business Server by using the **Enable for Skype for Business Server** command (see [Add and enable a new Skype for Business Server user](#)). However, all the Skype for Business Server-related information (including policy assignments) previously associated with that account will have to be re-created. If you want to prevent a user from logging on to Skype for Business Server, but do not want to lose all of their account information, you can temporarily disable the user account for Skype for Business Server (see [Disable or re-enable a user account for Skype for Business Server](#)).

To remove a user account from Skype for Business Server

1. In the Active Roles Web Interface for administrators, select the user account that you want to remove from Skype for Business Server.
2. Click the **Remove from Skype for Business Server** command.

The Web Interface displays the **Remove from Skype for Business Server** command if you have sufficient rights in Active Roles to perform that command, and the user account you have selected is in the scope of the policy provided by Skype for Business Server User Management and is enabled or temporarily disabled for Skype for Business Server.

Managing Skype for Business Server user properties

By using the Active Roles Web Interface, you can:

- View or change Skype for Business Server user properties such as the user's SIP address, telephony options and Skype for Business Server policy assignments
- Move Skype for Business Server users to a different Enterprise Edition Front End pool or Standard Edition server

View or change Skype for Business Server user properties

For a user account that is enabled or temporarily disabled for Skype for Business Server, you can use the Active Roles Web Interface to view or change Skype for Business Server user properties such as the user's SIP address, telephony options and Skype for Business Server policy assignments.

To view or change Skype for Business Server user properties

1. In the Active Roles Web Interface for administrators, select the user account whose properties you want to view or change.
2. Click the **Skype for Business Server User Properties** command.

The Web Interface displays the **Skype for Business Server User Properties** command if you have sufficient rights in Active Roles to view Skype for Business Server user properties of the selected account, and the user account you have selected is in the scope of the policy provided by Skype for Business Server User Management and is enabled or temporarily disabled for Skype for Business Server.

3. On the page that appears, view or change the following settings:
 - **Enabled for Skype for Business Server** Indicates whether or not the user is enabled to log on to Skype for Business Server. If you clear this check box, the user will no longer be able to log on to Skype for Business Server. Selecting this check box re-enables the user to log on to Skype for Business Server. The function of this check box is equivalent to the **Temporarily Disable for Skype for Business Server** and **Re-enable for Skype for Business Server** commands (see [Disable or re-enable a user account for Skype for Business Server](#)).
 - **SIP address** Indicates the user's SIP address (SIP URI), a unique identifier that allows the user to communicate using SIP devices such as Microsoft Skype for Business. The SIP address consists of the SIP user name on the left side of the @ symbol, and the SIP domain name on the right side. It must be prefaced by "sip: "; for example, sip:John.Smith@company.com.

- **Registrar pool** Identifies the Enterprise Edition Front End pool or Standard Edition server where the Skype for Business Server user is homed. If you need to move the user to a different server or pool, see [Move a user to another server or pool in Skype for Business Server](#) later in this document.
- **Telephony** Specifies whether the Skype for Business Server user can make PC-to-PC calls with audio and video, route incoming and outgoing calls, and control the desktop phone. The possible telephony options are as follows:
 - **PC-to-PC only** The user can make only PC-to-PC audio or video calls.
 - **Audio/video disabled** The user cannot make calls with audio and video.
 - **Remote call control** The user can use Skype for Business Server to control the desktop phone, and can also make PC-to-PC calls.
 - **Enterprise Voice** The user can use Skype for Business Server to route all incoming and outgoing calls, and can also make PC-to-PC calls.
 - **Remote call control only** The user can use Skype for Business Server to control the desktop phone, but cannot make PC-to-PC audio calls.
- **Line URI** Applies to all telephony options but **Audio/video disabled**. Specifies the primary phone number assigned to the Skype for Business Server user.
 The line URI must use the E.164 format and have the "TEL:" prefix. For example: TEL:+12345678997. The extension number, if any, should be added at the end of the line URI, for example: TEL:+12345678997;ext=65431.
- **Line server URI** Applies to the **Remote call control** and **Remote call control only** options. Specifies the URI of the remote call control telephone gateway assigned to the Skype for Business Server user.
 The line server URI is the gateway URI, prefaced by "sip:"; for example, sip:rccgateway@company.com.
- **Dial plan policy** Applies to the **Enterprise Voice** option. Identifies the dial plan currently assigned to the Skype for Business Server user, and allows you to assign a different dial plan.
- **Voice policy** Applies to the **Enterprise Voice** option. Identifies the voice policy currently assigned to the Skype for Business Server user, and allows you to assign a different voice policy.
- **Conferencing policy** Identifies the conferencing policy currently assigned to the Skype for Business Server user, and allows you to assign a different conferencing policy to the user.
- **Conferencing policy** Identifies the conferencing policy currently assigned to the Skype for Business Server user, and allows you to assign a different conferencing policy to the user.
- **Client version policy** Identifies the client version policy currently assigned to the Skype for Business Server user, and allows you to assign a different client version policy.

- **PIN policy** Identifies the personal identification number (PIN) policy currently assigned to the Skype for Business Server user, and allows you to assign a different PIN policy.
- **External access policy** Identifies the external access policy currently assigned to the Skype for Business Server user, and allows you to assign a different external access policy.
- **Archiving policy** Identifies the archiving policy currently assigned to the Skype for Business Server user, and allows you to assign a different archiving policy.
- **Location policy** Identifies the location policy currently assigned to the Skype for Business Server user, and allows you to assign a different location policy.
- **Mobility policy** Identifies the mobility policy currently assigned to the Skype for Business Server user, and allows you to assign a different mobility policy.
- **Persistent Chat policy** Identifies the persistent chat policy currently assigned to the Skype for Business Server user, and allows you to assign a different persistent chat policy.
- **Client policy** Identifies the client policy currently assigned to the Skype for Business Server user, and allows you to assign a different client policy.

Skype for Business Server user account properties allow you to assign certain policies to a Skype for Business Server user in order to specify particular settings that differ from the settings defined in policies assigned to other users, such as global policies. These policies are referred to as user policies.

In Skype for Business Server, deploying and assigning user policies is optional. It is possible to deploy only global policies or site policies. If user policies are deployed, they must be assigned to users explicitly. When managing Skype for Business Server user settings, you can select the appropriate user policy from a list. The list also includes the **<Automatic>** entry. If **<Automatic>** is selected, the global policy (or, if defined, the site policy) is assigned to the user.

Move a user to another server or pool in Skype for Business Server

For a user account that is enabled or temporarily disabled for Skype for Business Server, you can use the Active Roles Web Interface to move the user account to a specific Enterprise Edition Front End pool or Standard Edition server.

To move a Skype for Business Server user account to a different server or pool

1. In the Active Roles Web Interface for administrators, select the user account you want to move.
2. Click the **Move to Skype for Business Server Pool** command.

The Web Interface displays the **Move to Skype for Business Server Pool** command if you have sufficient rights in Active Roles to perform that command, and the user account you have selected is in the scope of the policy provided by Skype for

Business Server User Management and is enabled or temporarily disabled for Skype for Business Server.

3. On the page that appears, select the server or pool to which you want to move the Skype for Business Server user.
4. Click **Finish**.

Management Pack for SCOM

The Active Roles Management Pack for Microsoft System Center Operations Manager (SCOM) provides a basic solution for monitoring availability and health of the Active Roles Administration Service and its information store, Active Roles replication status, and availability of the Active Roles Web Interface. By detecting, alerting on, and automatically responding to critical events, the Management Pack helps indicate, correct, and in many cases prevent outages of the Administration Service and Web Interface.

Features

The Management Pack provides the features that you need to monitor your Active Roles environment, such as automated discovery, availability and performance monitoring, and replication monitoring. The Management Pack alerts you to the following error conditions:

- Administration Service is not responding
- Active Roles replication failure has occurred
- Connection to the Active Roles database has been lost
- Administration Service failed to update a Dynamic Group
- Administration Service failed to update a Group Family
- Active Roles Web Interface is unavailable

Monitoring views

The monitoring views are used to centrally monitor availability and health of the Active Roles components in the Operations Manager console's Monitoring pane. The Management Pack provides the following views:

- **Alerts** Displays the alerts on the computers running the Active Roles Administration Service or Web Interface.

- **Computers** Shows information about the state of the computers running the Active Roles Administration Service or Web Interface.
- **Events** Displays the events on the computers running the Active Roles Administration Service or Web Interface.
- **Performance** Shows performance information collected from the computers running the Active Roles Administration Service or Web Interface.
- **Service Level Exceptions** Displays the unresolved alerts that have exceeded service levels on the computers running the Active Roles Administration Service or Web Interface.
- **Task Status** Shows information indicating task results on the computers running the Active Roles Administration Service or Web Interface.
- **Discovery** Contains separate views allowing you to examine the state of the computers running the Web Interface, computers running the Administration Service, and computers running the Web Interface or Administration Service.
- **Services Monitoring** Contains the views allowing you to monitor availability, health and performance of the Administration Service instances in your environment.
- **Web Interfaces Monitoring** Contains the views allowing you to monitor availability and health of the Web Interface instances in your environment.

Getting started

Install the Management Pack by importing the ActiveRoles.SCOM.MP.xml file into System Center Operations Manager (SCOM). You can install this Management Pack on the following SCOM versions:

- System Center Operations Manager 2007 R2
- System Center 2012 - Operations Manager
- System Center Operations Manager 2016
- System Center Operations Manager 2019

Monitoring Active Roles Administration Service

This section briefly discusses the processing rules that the Management Pack uses to monitor availability and health of the Active Roles Administration Service:

- General response
- Replication monitoring
- Monitoring of connection to configuration database

- Monitoring of Dynamic Group-related operations
- Monitoring of Group Family-related operations
- Internal error
- Critical error on startup
- License system failure

Monitoring of general response and replication is performed by using custom, script-based processing rules. Those rules run on a scheduled basis, analyzing information returned by the scripts and raising an appropriate event if an error situation is detected. The schedule is stored as part of rule configuration data, and can be adjusted by managing rule properties in the Operations Manager console.

General response - Script

This rule uses a script to check the responsiveness of the Administration Service by periodically issuing a simple request to the Service. By default, this rule is scheduled to run every 10 minutes. The schedule can be adjusted by managing rule properties in the Operations Manager console.

General response - Alert

This rule generates an alert when the **General response** script detects that the Administration Service is unavailable.

Possible causes of the alert include:

- Administration Service is not running
- Administration Service is not configured properly
- Administration Service has encountered a critical error
- Administration database is unavailable

Replication monitoring - Script

This rule uses a script to check the status of Active Roles replication. The script is intended to run on the Publisher Administration Service so as to verify the replication status of the Publisher and Subscribers. By default, this rule is scheduled to run every 30 minutes. The schedule can be adjusted by managing rule properties in the Operations Manager console.

Replication monitoring - Alert

This rule generates an alert when the **Replication monitoring** script detects that the Active Roles replication status indicates a replication failure.

Possible causes of the alert include:

- The SQL Server Agent service is not started on the computer running the Publisher SQL Server
- The Snapshot Agent or a Merge Agent is not started at the Publisher SQL Server
- The Merge Agent uses incorrect credentials when connecting to the Publisher or a Subscriber
- The Snapshot Agent uses incorrect credentials when connecting to the Publisher

For more information, and details on how resolve replication-related problems, refer to the “Troubleshooting” section in the *Replication: Best Practices and Troubleshooting* document, which is part of the Active Roles product documentation set.

Monitoring connection to configuration database

This category includes the event-based processing rules to monitor health of the connection to the configuration database:

- **Connection to database has been lost** Administration Service has lost connection to the configuration database, and is making attempts to re-establish the connection.
- **Connection to database has been restored** Administration Service has restored connection to the configuration database.

The following sub-sections elaborate on each of these processing rules.

Connection to database has been lost - Alert

This rule generates an alert indicating that the Administration Service has lost a connection to the configuration database, and is making attempts to restore the connection. For details, refer to the alert description generated by this rule. Losing the connection to the database does not affect the directory management functions of the Administration Service. All operations related to Active Directory management continue to work as expected.

Until after the connection has been restored, unavailable are the functions of the Administration Service that require access to the database. These include:

- Collecting data related to change history and user activity
- Retrieving and updating configuration data
- Retrieving changes to configuration data made by other Administration Services (both directly and via replication)
- Retrieving and updating virtual attributes stored in the configuration database

Connection to database has been restored - Alert

This rule generates an alert indicating that the Administration Service has restored the connection to the configuration database. For details, refer to the alert description generated by this rule. Once the connection has been restored, available are all the functions of the Administration Service that require access to the database.

Monitoring of Dynamic Group-related operations

This category includes the event-based processing rules to monitor the background activities of Active Roles related to Dynamic Groups:

- **Rebuilding has been started** Administration Service has been forced to recalculate (rebuild) the membership list of a Dynamic Group.
- **Failed to add object to Dynamic Group** Administration Service failed to add an object to a Dynamic Group.
- **Failed to remove object from Dynamic Group** Administration Service failed to remove an object from a Dynamic Group.
- **Failed to process membership rule** Administration Service failed to apply a query-based membership rule when updating the membership list of a Dynamic Group.
- **Failed to update membership list** Administration Service failed to update the membership list of a Dynamic Group in accordance with the membership rules.
- **Failed to update membership list of nested group** Administration Service failed to update the membership list of an additional (nested) group generated to accommodate extra members of a Dynamic Group.
- **Failed to update membership rule upon deletion of object** When updating a Dynamic Group, Administration Service failed to delete or update a membership rule of a Dynamic Group upon deletion of an object.
- **Failed to look up object when updating** When updating a Dynamic Group, Administration Service failed to locate an object that is referred to by a certain membership rule. The object may have been deleted.

- **Failed to retrieve information from domain** Administration Service failed to retrieve information about Dynamic Groups from a certain domain.
- **Membership rule domain unavailable** When updating a Dynamic Group, Administration Service failed to apply a membership rule because the rule applies to a domain unavailable on the network.
- **Membership rule failed** When updating a Dynamic Group, Administration Service failed to apply one of the membership rules, which prevented all rules from being applied and stopped changes to the members list of the Dynamic Group.

The following sub-sections elaborate on each of these processing rules.

Dynamic Group - Rebuilding has been started - Alert

This rule generates an alert indicating that an administrator has forced Active Roles to recalculate (rebuild) the membership list of a Dynamic Group. For details, refer to the alert description generated by this rule.

The administrator could start the rebuilding of a Dynamic Group from the **Members** tab in the **Properties** dialog box for that Dynamic Group, in the Active Roles console.

Failed to add object to Dynamic Group - Alert

This rule generates an alert indicating that the Administration Service failed to add an object to a Dynamic Group due to a certain problem. The object is missing from the Dynamic Group until after the problem has been resolved. For details, refer to the alert description generated by this rule.

Try to force rebuilding of the Dynamic Group from the **Members** tab in the **Properties** dialog box for that Dynamic Group, in the Active Roles console.

Failed to remove object from Dynamic Group - Alert

This rule generates an alert indicating that the Administration Service failed to remove an object from a Dynamic Group due to a certain problem. The object remains in the Dynamic Group until after the problem has been resolved. For details, refer to the alert description generated by this rule.

Try to force rebuilding of the Dynamic Group from the **Members** tab in the **Properties** dialog box for that Dynamic Group, in the Active Roles console.

Dynamic Group - Failed to process membership rule - Alert

This rule generates an alert indicating that the Administration Service failed to apply a query-based membership rule when updating the membership list of a Dynamic Group. The failed rule is not taken into account, so the membership list may be incompliant with the membership rules. For details, refer to the alert description generated by this rule.

Try to force rebuilding of the Dynamic Group from the **Members** tab in the **Properties** dialog box for that Dynamic Group, in the Active Roles console. Check membership rules by using the Membership Rules tab in that dialog box.

Dynamic Group - Failed to update membership list - Alert

This rule generates an alert indicating that the Administration Service failed to update the membership list of a Dynamic Group in accordance with the membership rules. The membership list may be incompliant with the membership rules. For details, refer to the alert description generated by this rule.

Try to force rebuilding of the Dynamic Group from the **Members** tab in the **Properties** dialog box for that Dynamic Group, in the Active Roles console.

Dynamic Group - Failed to update membership list of nested group - Alert

This rule generates an alert indicating that the Administration Service failed to update the membership list of an additional (nested) group generated to accommodate extra members of a Dynamic Group. The membership list of the nested group may be incompliant with the membership rules. For details, refer to the alert description generated by this rule.

Try to force rebuilding of the Dynamic Group from the **Members** tab in the **Properties** dialog box for that Dynamic Group, in the Active Roles console.

Dynamic Group - Failed to update membership rule upon deletion of object - Alert

This rule generates an alert indicating that the Administration Service failed to delete or update a membership rule of a Dynamic Group upon deletion of a certain object. The membership rule could be one of the following:

- Implicit inclusion or exclusion of that object from the Dynamic Group
- Query with a filter referring to that object
- Inclusion or exclusion of the members of the group represented by that object

For details, refer to the alert description generated by this rule.

To resolve these issues, delete or update membership rules by using the **Membership Rules** tab in the **Properties** dialog box for that Dynamic Group, in the Active Roles console. Then, force rebuilding of the Dynamic Group from the **Members** tab in that dialog box.

Dynamic Group - Failed to look up object when updating - Alert

This rule generates an alert indicating that the Administration Service failed to locate an object when updating the membership list of a Dynamic Group in accordance with the membership rules. The object may have been deleted. The object could be referred to by:

- A membership rule to explicitly include or exclude that object from the Dynamic Group
- A query-based membership rule (the object may represent the base of a search or be a member of the search result set)
- A membership rule to include or exclude the members of a certain group (the object may represent the domain of that group)
- A directory synchronization (DirSync) query (this may be one of the objects returned by that query)

For details, refer to the alert description generated by this rule.

The membership rules referring to that object are inoperative and are not taken into account when updating the Dynamic Group, so the membership list may be incompliant with the membership rules.

To prevent issues with the membership list of the Dynamic Group, check membership rules by using the **Membership Rules** tab in the **Properties** dialog box for that Dynamic Group, in the Active Roles console. Then, force rebuilding of the Dynamic Group from the **Members** tab in that dialog box.

Dynamic Group - Failed to retrieve information from domain - Alert

This rule generates an alert indicating that the Administration Service failed to retrieve information about Dynamic Groups from a certain domain. The Dynamic Groups contained in that domain are inoperative until after the problem has been resolved. For details, refer to the alert description generated by this rule.

Dynamic Group - Membership rule domain unavailable - Alert

This rule generates an alert indicating that Active Roles failed to update the members list of the Dynamic Group in accordance with one of the membership rules. The failed membership rule applies to a domain that is currently unavailable. The membership rule is disregarded, so the members list of the Dynamic Group may be incompliant with the membership rules. For details, refer to the alert description generated by this rule.

Ensure that the domain is available on the network, and then update the Dynamic Group by clicking **Rebuild** on the **Members** tab in the **Properties** dialog box for that group in the Active Roles console or wait for Active Roles to update the Dynamic Group on a schedule.

Dynamic Group - Membership rule failed - Alert

This rule generates an alert indicating that Active Roles failed to update the members list of the Dynamic Group in accordance with one of the membership rules. As one of the membership rules failed, no membership rules are applied until the issue is resolved, so the members list of this Dynamic Group remains unchanged. For details, refer to the alert description generated by this rule.

Try forcing update of the Dynamic Group by clicking **Rebuild** on the **Members** tab in the **Properties** dialog box for that group in the Active Roles console. Check the membership rules on the **Membership Rules** tab in that dialog box.

Monitoring of Group Family-related operations

This category includes the event-based processing rules to monitor the background activities of Active Roles related to Group Families:

- **Cannot find configuration storage group** Administration Service failed to run a Group Family due to the following problem: The Group Family configuration storage group cannot be found.
- **Failed to retrieve configuration data** Administration Service failed to run a Group Family due to the following problem: Group Family configuration data cannot be retrieved from the Group Family configuration storage group.
- **Incorrect configuration data** Administration Service failed to run a Group Family due to the following problem: Incorrect configuration data was encountered in the Group Family configuration storage group.
- **Failed to retrieve configuration data for controlled group** Administration Service encountered an error when running a Group Family, failed to retrieve

configuration data for a controlled group. Changes to the controlled group may not be applied until a subsequent run of the Group Family.

- **Failed to retrieve data from container** Administration Service encountered an error when running a Group Family, failed to search a certain container within the Group Family scope. Until a subsequent run, Group Family does not consider information about objects held in that container.
- **Failed to update configuration data** Administration Service encountered an error when running a Group Family, failed to update data in the Group Family configuration storage group. Information about controlled groups may be incorrect until a subsequent run of the Group Family.
- **Failed to update configuration data for controlled group** Administration Service encountered an error when running a Group Family, failed to update configuration data for a controlled group. The controlled group is not linked with the Group Family until a subsequent run of the Group Family.
- **Cannot find controlled group** Administration Service encountered an error when running a Group Family, failed to find a controlled group. Changes to the controlled group, if any, are not applied until a subsequent run of the Group Family.
- **Failed to create controlled group** Administration Service encountered an error when running a Group Family, failed to create a controlled group. Administration Service will attempt to create that controlled group during a subsequent run of the Group Family.
- **Failed to update membership list of controlled group** Administration Service encountered an error when running a Group Family, failed to update membership data for a controlled group. The membership list of the controlled group may be incorrect until a subsequent run of the Group Family.
- **Failed to create run task** Administration Service failed to create a task to run a Group Family. The Group Family is inoperative until the task is created.
- **Failed to modify run task** Administration Service failed to update a task to run a Group Family. The Group Family runs in accordance with the earlier schedule settings of that task.
- **Failed to delete run task** Administration Service failed to delete a task to run a Group Family. The Group Family continues to run in accordance with the schedule settings of that task.
- **Run task has been started manually** A task to run a Group Family was started manually.
- **Group Family run has been completed** Administration Service has completed a run of a Group Family.

Group Family - Cannot find configuration storage group - Alert

This rule generates an alert indicating that the Administration Service failed to run a Group Family due to the following problem: The Group Family configuration storage group cannot

be found. The Administration Service cannot run the Group Family until the problem is resolved.

The configuration storage group may have been either inaccessible or deleted. For details, refer to the alert description generated by this rule.

Group Family - Failed to retrieve configuration data - Alert

This rule generates an alert indicating that the Administration Service encountered the following problem when running a Group Family: Group Family configuration data cannot be retrieved from the configuration storage group. The Administration Service cannot run the Group Family until the problem is resolved. For details, refer to the alert description generated by this rule.

Group Family - Incorrect configuration data - Alert

This rule generates an alert indicating that the Administration Service failed to run a Group Family due to the following problem: Incorrect configuration data was encountered in the Group Family configuration storage group. The configuration storage group may have been corrupted. The run of the Group Family has been canceled. For details, refer to the alert description generated by this rule.

Group Family - Failed to retrieve configuration data for controlled group - Alert

This rule generates an alert indicating that the Administration Service encountered the following problem when running a Group Family: Failed to retrieve configuration data for a certain group that is under the control of the Group Family (controlled group). Changes to the controlled group may not be applied until a subsequent run of the Group Family. For details, refer to the alert description generated by this rule.

Group Family - Failed to retrieve data from container - Alert

This rule generates an alert indicating that the Administration Service encountered the following problem when running a Group Family: Failed to search a certain container within the Group Family scope. The groupings that were calculated during this run of the Group Family may not take into account information about some objects held in that container. For details, refer to the alert description generated by this rule.

During a subsequent run of the Group Family, the Administration Service will attempt to search the entire Group Family scope, including the failed container, in order to recalculate the Group Family groupings.

Group Family - Failed to update configuration data - Alert

This rule generates an alert indicating that the Administration Service encountered the following problem when running a Group Family: Failed to update configuration data in the Group Family configuration storage group. The Active Roles console may display incorrect information about results of the Group Family run and about groups that are under the control of the Group Family (controlled groups). For details, refer to the alert description generated by this rule.

During a subsequent run of the Group Family, the Administration Service will attempt to update configuration data in the configuration storage group.

Group Family - Failed to update configuration data for controlled group - Alert

This rule generates an alert indicating that the Administration Service encountered the following problem when running a Group Family: Failed to update configuration data for a certain group that is under the control of the Group Family (controlled group). The group is removed from the control of the Group Family. For details, refer to the alert description generated by this rule.

During a subsequent run of the Group Family, the Administration Service will attempt to locate the failed group and put it under the control of the Group Family.

Group Family - Cannot find controlled group - Alert

This rule generates an alert indicating that the Administration Service encountered the following problem when running a Group Family: Cannot find a certain group that is under the control of the Group Family (controlled group). Some changes to the controlled group may not be applied. For details, refer to the alert description generated by this rule.

During a subsequent run of the Group Family, the Administration Service will attempt to locate the controlled group and apply the changes, if any, to that group.

Group Family - Failed to create controlled group - Alert

This rule generates an alert indicating that the Administration Service encountered the following problem when running a Group Family: Failed to create a certain group to be put under the control of the Group Family (controlled group). For details, refer to the alert description generated by this rule.

During a subsequent run of the Group Family, the Administration Service will attempt to create the controlled group and apply the changes, if any, to that group.

Group Family - Failed to update membership list of controlled group - Alert

This rule generates an alert indicating that the Administration Service encountered the following problem when running a Group Family: Failed to update the membership list of a certain group that is under the control of the Group Family (controlled group). Some changes to the membership list of the controlled group may not be applied. For details, refer to the alert description generated by this rule.

During a subsequent run of the Group Family, the Administration Service will attempt to locate the controlled group and apply the changes, if any, to the membership list of that group.

Group Family - Failed to create run task - Alert

This rule generates an alert indicating that the Administration Service failed to create a task to run a Group Family. The Group Family is inoperative until the task is created. For details, refer to the alert description generated by this rule.

Group Family - Failed to modify run task - Alert

This rule generates an alert indicating that the Administration Service failed to update a task to run a Group Family. The Group Family continues to run in accordance with the earlier schedule settings of that task. For details, refer to the alert description generated by this rule.

Try to adjust the schedule settings by using the **Schedule** tab in the **Properties** dialog box for the Group Family configuration storage group, in the Active Roles console.

Group Family - Failed to delete run task - Alert

This rule generates an alert indicating that the Administration Service failed to delete a task to run a Group Family while the configuration storage group of that Group Family was successfully deleted. The Group Family continues to run in accordance with the schedule settings of that task, which may cause an error situation. For details, refer to the alert description generated by this rule.

Delete the run task manually. You can do this by switching the Active Roles console into Raw view mode, and then deleting the appropriate task from the **Configuration/Server Configuration/Scheduled Tasks/Group Family** container.

Group Family - Run task has been started manually - Alert

This rule generates an alert indicating that an administrator has forced Active Roles to run a Group Family. For details, refer to the alert description generated by this rule.

The administrator could start the run task for a Group Family by using the **Force Run** command on the configuration storage group of that Group Family, in the Active Roles console.

Group Family run has been completed - Alert

This rule generates an alert indicating that the Administration Service has completed the run task for a Group Family. For task results, refer to the alert description generated by this rule.

The alert description also includes the name of the Group Family configuration storage group, so you could use the **Properties** dialog box for that group in order to examine task results in more detail.

Internal error - Alert

This rule generates an alert when a fatal error occurs at Administration Service run time. Normally, the alert indicates that Administration Service execution stopped.

Critical error on startup - Alert

This rule generates an alert when a fatal error occurs at Administration Service startup time. The alert includes information detailing the error.

License system failure - Alert

This rule generates an alert when a failure occurs in the Administration Service licensing system. The alert includes information detailing the problem.

Monitoring Active Roles Web Interface

This section briefly discusses the processing rules that you can use to monitor availability of the Active Roles Web Interface.

Availability - Script

This rule uses a script to check the availability of the Web Interface. The script invokes a self-diagnostic script built into the Web Interface so as to verify the Web Interface configuration, including the customization settings, and to check whether the Administration Service is available.

The rule ensures that both the default and customized Web Interface sites are monitored properly if customization is performed by using the point-and-click tools included in the Web Interface.

The rule does not check the availability of the Web Interface functions that are based on custom ASP files integrated with the Web Interface, if any. An additional, custom rule needs to be implemented in Operations Manager to monitor such functions.

By default, this rule is scheduled to run every 30 minutes. The schedule can be adjusted by managing rule properties in the Operations Manager console.

Availability - Alert

This rule generates an alert when the **Availability** script detects that the Web Interface is unavailable.

- Possible causes of the alert include:
- Web Interface is not running
- Web Interface is not configured properly
- Administration Service is unavailable

Monitoring performance

This section provides information on the processing rules based on performance counters that allow you to evaluate performance of the Administration Service:

- [AD changes processed/sec](#)
- [Changes queue length \(AD + Database\)](#)
- [Connected clients](#)
- [Database changes processed/sec](#)
- [LDAP operations in progress](#)
- [LDAP operations/sec](#)
- [Private bytes](#)
- [Queued post-processing policies](#)
- [Requests in progress](#)
- [Requests/sec](#)
- [Script module average execution time](#)
- [Script modules executing](#)

AD changes processed/sec

This rule collects **AD changes processed/sec** counter samples for the **AR Server:External Changes** performance object. A sample of the counter is the number of changes received from Active Directory and processed by the Active Roles Administration Service per second.

Changes queue length (AD + Database)

This rule collects **Changes queue length (AD + Database)** counter samples for the **AR Server:External Changes** performance object. A sample of the counter is the number of unprocessed changes that the Active Roles Administration Service received from Active Directory and from the Active Roles database.

Connected clients

This rule collects **Connected clients** counter samples for the **AR Server:Miscellaneous** performance object. A sample of the counter is the current number of the clients connected to the Active Roles Administration Service.

Database changes processed/sec

This rule collects **Database changes processed/sec** counter samples for the **AR Server:External Changes** performance object. A sample of the counter is the number of changes received from the Active Roles database and processed by the Active Roles Administration Service per second.

LDAP operations in progress

This rule collects **LDAP operations in progress** counter samples for the **AR Server:LDAP Operations** performance object. A sample of the counter is the current number of the LDAP operation requests that are in progress on the Active Roles Administration Service.

LDAP operations/sec

This rule collects **LDAP operations/sec** counter samples for the **AR Server:LDAP Operations** performance object. A sample of the counter is the number of LDAP operations executed by the Active Roles Administration Service per second.

Private bytes

This rule collects **Private Bytes** counter samples for the **Process** performance object specific to the Active Roles Service (arssvc) process. A sample of the counter is the amount of virtual memory (in bytes) that the Active Roles Administration Service process allocates (process private bytes).

Queued post-processing policies

This rule collects **Queued post-processing policies** counter samples for the **AR Server:Miscellaneous** performance object. A sample of the counter is the number of the post-processing policy operations queued by the Active Roles Administration Service.

Requests in progress

This rule collects **Requests in progress** counter samples for the **AR Server:Requests** performance object. A sample of the counter is the current number of the client requests

being processed by the Active Roles Administration Service.

Requests/sec

This rule collects **Requests/sec** counter samples for the **AR Server:Requests** performance object. A sample of the counter is the number of requests received by the Active Roles Administration Service per second.

Script module average execution time

This rule collects **Script module average execution time** counter samples for the **AR Server:Script Modules** performance object. A sample of the counter is the average execution time of all script module instances run by the Active Roles Administration Service.

Script modules executing

This rule collects **Script modules executing** counter samples for the **AR Server:Script Modules** performance object. A sample of the counter is the current number of the script module instances being executed by the Active Roles Administration Service.

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product