One Identity Active Roles 7.2

Evaluator Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Active Roles Evaluator Guide
Updated - December 2017
Version - 7.2

Contents

1

Introduction

Active Roles is an administrative platform that facilitates user and group administration for Microsoft Active Directory and Exchange. Active Roles enables organizations to create flexible administration solutions that suit their needs, while ensuring secure delegation of tasks, reduced workloads, and lower costs. It also enables the integration of diverse corporate data sources and provisioning processes, which can expedite business workflow and eliminate data inconsistencies.

This document is for IT specialists who are evaluating Active Roles. The document provides evaluation scenarios to help better understand the Active Roles functionality. The document covers the following topics:

- Active Roles test lab setup
- Managing users and groups
- Delegating administration using Active Roles
- Using Managed Units to delegate administration
- Using Active Roles policies
- Managing Exchange recipients
- Managing native Active Directory security
- Using dynamic (rules-based) groups
- Delegating and managing computer resources
- Using Active Roles audit trail and reporting
- Using Active Roles replication
- Customizing the Web Interface

NOTE:

- Unless otherwise indicated, the instructions in this document assume that you are logged on as Active Roles Admin. The Active Roles Admin account is specified when installing the Administration Service, and defaults to the Administrators local group of the computer running the Administration Service.
- You should verify that the Active Roles console is in Advanced view mode: On the **View** menu, click **Mode**; then, click **Advanced Mode**.

2

Test lab setup

Successful deployment requires thorough testing in a lab environment. When planning your testing, we recommend:

- Designing your lab to reflect your production environment. For example, if your network has multiple sites, then your lab should have multiple sites.
- Having your lab's number of users and computers be at least two to five percent of the number of users and computers in your production environment.

This section describes how to initially set up your test lab for evaluation purposes: install Active Roles on your computer, connect to the Active Roles Administration Service and register domains with Active Roles.

Preparing a server for Active Roles installation

To perform evaluation, you need a test Active Directory domain with a member server set up and configured. Your server must meet the following hardware requirements:

- 64-bit (x64) processor, 2.0 GHz or faster
- At least 8 GB of RAM
- At least 100 GB of free hard disk space
- Network adapter
- Video adapter and monitor with screen resolution of 1280x800 or higher
- Mouse, or other pointing device

Ensure that you have the following software available:

- Microsoft Windows Server 2008 R2 SP1 or a later version of Windows Server
- Active Roles 7.2 distribution package

Install the Windows Server operating system on your server, and join the server to your test Active Directory domain.

Then, install the following software on your server:

- Microsoft .NET Framework 4.6.2 (see "Installing the .NET Framework 4.6.2" at http://go.microsoft.com/fwlink/p/?LinkId=257868)

  NOTE: You only need to install .NET Framework 4.6.2 on Windows Server 2008 R2. Later versions of Windows Server include this software as a part of the operating system.

- Windows Management Framework 3.0 (see "Windows Management Framework 3.0" at http://go.microsoft.com/fwlink/p/?LinkId=272757)

  NOTE: You only need to install Windows Management Framework 3.0 on Windows Server 2008 R2. Later versions of Windows Server include this software as a part of the operating system.

- Microsoft SQL Server 2012 Express (see "Microsoft SQL Server 2012 Service Pack 1 (SP1) Express" at http://go.microsoft.com/fwlink/?LinkID=267905)

Once you have prepared your server, you are ready to install and configure Active Roles.

Installing and configuring Active Roles

To install and configure Active Roles for evaluation purposes, you will follow these steps:

1. Run Setup, which installs binaries and configures registry settings for Active Roles.
2. Run Active Roles Configuration Center, which creates and configures the Active Roles database, Administration Service, and Web Interface.

Setup user account

Ensure that the account that you use to install and configure Active Roles meets the following requirements:

- Domain user account that is a member of the Domain Admins group in your test Active Directory domain
- Member of the Administrators group on your computer intended for installing Active Roles
- SQL login on the SQL Server Express instance that runs on your computer for installing Active Roles
- Member of the **sysadmin** fixed server role on that SQL Server Express instance

Run Setup

Setup installs binaries and configures registry settings for Active Roles.

To run Setup

1. Log on with a user account that meets the requirements listed in Setup user account.
2. Navigate to the location of the Active Roles distribution package, and start the Setup wizard by double-clicking `Setup.exe`.
3. In the Setup wizard, review the **Introduction** page, and click **Next**.
4. On the **License Terms** page, review the Active Roles license agreement, select the option indicating that you accept the terms in the license agreement, and then click **Next**.
5. On the **Component Selection** page, verify that the Administration Service, Web Interface, and Console components are selected, and click **Next**.
6. On the **Ready to Install** page, click **Install** to begin installation.
7. On the **Completion** page, verify that the **I want to perform configuration** check box is selected, and click **Finish**.

Setup will start Active Roles Configuration Center, allowing you to configure your Active Roles installation (see Run Active Roles Configuration Center).

Run Active Roles Configuration Center

After you complete Active Roles Setup, run Active Roles Configuration Center to create and configure the Active Roles database, Administration Service, and Web Interface.

To run Active Roles Configuration Center

1. In the Active Roles Setup wizard (see Run Setup), select the **I want to perform configuration** check box on the **Completion** page and click **Finish** to start Active Roles Configuration Center.

   You can also start Configuration Center by selecting **Active Roles 7.2 Configuration Center** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

2. In the Active Roles Configuration Center main window, under **Administration Service**, click **Configure**.

   This starts the wizard that will create and configure the Active Roles database and Administration Service.

3. On the **Service Account** page, verify that the **Logon name** field displays the name of your Setup user account, type the password of that user account in the **Password** field, and then click **Next**.
4. On the **Active Roles Admin** page, verify that the **Name** field reads `BUILTIN\Administrators` (which identifies the Administrators group of the computer on which you are configuring Active Roles), and then click **Next**.

5. On the **Database Options** page, verify that the **New Active Roles database** option is selected and the **Use a pre-created blank database** check box is cleared, and then click **Next**.
6. On the **Connection to Database** page:
    a. In the **SQL Server** field, specify the name of your SQL Server Express instance, such as `<computername>\SQLEXPRESS` where `<computername>` stands for the short name of the computer on which you are configuring Active Roles.
    b. Verify that the **Windows authentication** option is selected.
    c. Click **Next**.
7. On the **Ready to Configure** page, click **Configure**.
8. Wait for the wizard to complete the operation.
9. On the **Completion** page, click **Finish** to close the wizard.
10. In the Active Roles Configuration Center main window, under **Web Interface**, click **Configure**.

    This starts the wizard that will create and configure the default Web Interface sites.
11. On the **Administration Service** page, select the **Administration Service on the computer running the Web Interface** option, and then click **Configure**.
12. Wait for the wizard to complete the operation.
13. On the **Completion** page, click **Finish** to close the wizard.

Installing the reporting components

You can install reporting components from the Active Roles distribution package. For the purposes of this evaluation, install the Active Roles Collector on the computer where you have installed Active Roles and then use the Collector wizard to deploy the Report Pack.

To install the Collector

- In the Active Roles distribution package, navigate to the **Solutions/Collector and Report Pack** folder, double-click the .msi file held in that folder, and follow the instructions in the Setup wizard to install Collector.

Once you have installed the Collector, you can start the Collector wizard by selecting **Active Roles Active Roles Collector and Report Pack** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

Report Pack requires Microsoft SQL Server Reporting Services (SSRS). Make sure that you have SSRS deployed in your environment. When deploying Report Pack, the Collector wizard prompts you for the address (URL) of the Report Server Web service. You can find this address on the **Web Service URL** page in the Reporting Services Configuration Manager tool on the server where SSRS is installed.

To deploy the Report Pack

1. Start the Collector wizard by selecting **Active Roles Active Roles Collector and Report Pack** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.
2. On the **Select Task** page, click **Deploy reports to Report Server**, and then click **Next**.
3. On the **Report Server** page, type the URL of your SSRS Report Server in the **Report Server Web Service URL** box. Click **Next**.

   By default, the URL is http://<*ComputerName*>/reportserver where <*ComputerName*> stands for the name of the computer on which SSRS is installed.
4. On the **Data Source** page, click **Next**.
5. Wait while the wizard deploys the Report Pack.

Connecting to Administration Service

The next step is to start the Active Roles console (MMC Interface) and have the console connect to the Administration Service.

To start the Active Roles console

- Depending upon the version of your Windows operating system, click **Active Roles 7.2 Console** on the **Apps** page or select **All Programs | Active Roles Active Roles 7.2 | Active Roles 7.2 Console** from the **Start** menu.

Normally, the Active Roles console automatically connects to the appropriate Administration Service. Optionally, you can select a different Administration Service to connect to.

To select Administration Service

1. Right-click the console tree root, and then click **Connect**.
2. In the **Connect to Administration Service** dialog box, type or select the name of the computer running the Administration Service. Click **OK**.
3. Wait while the console establishes a connection to the Administration Service.

Once the connection is established, the name of the Administration Service computer is displayed in the brackets next to the console tree root.

Registering the domain

The next step is to register your test domain with Active Roles. This operation is also referred to as *adding a managed domain*.

A list of managed domains is part of Active Roles configuration. After you initially install the Administration Service, the list is empty. By registering a domain, you add a record to that list.

To register your test domain

1. Click the console tree root.
2. In the details pane, click the **Add Domain** button to start the Add Managed Domain wizard.
3. Click **Next**.
4. Type the name of your test domain, or click **Browse** to select the domain. Click **Next**.
5. Verify that the following option is selected: **The service account information the Administration Service uses to log on**.
6. Click **Next**.
7. Click **Finish** to close the wizard.
8. Wait while Active Roles completes the domain registration.

NOTE: You can un-register domains by deleting their registration objects from the **Managed Domains** container. To access that container, select the console tree root, and then, in the details pane, click **Go to Managed Domains** in the **Domains** area.

3

Managing users and groups

This section provides sample procedures that illustrate how to manage users and groups in Active Directory using the Active Roles console or Web Interface.

NOTE: To walk through the scenarios outlined in this chapter, you must be logged on as a user with sufficient permissions in Active Roles. For example, it would suffice if you are logged on as Active Roles Admin—a member of the Administrators group on the computer running the Administration Service. Alternatively, you might be granted full control of the organizational unit that holds your test users and groups. For information on how to specify user permissions in Active Roles, see Delegating administration later in this document.

Use the Active Roles console

Create a user

To create a user account

1. In the console tree, expand **Active Directory** and select the OU where you want to add the user.
2. In the console tree, right-click the OU, and select **New | User**.
3. Type in the **First name**, **Last name**, and **User logon name** boxes. Click **Next**.
4. Click the button next to the **Password** box to generate a password. Click **Next**.
5. If Microsoft Exchange Server is deployed in your test domain, you can make the user mailbox-enabled. To do this, select the **Create an Exchange mailbox** check box. Click **Next**.
6. If you need to specify additional properties of the new user, select the **Display the object properties when this wizard closes** check box. Click **Finish**.

Create a group

To create a group

1. In the console tree, expand **Active Directory** and select the OU where you want to add the group.
2. In the console tree, right-click the OU, and select **New | Group**.
3. Type a name for the new group, click the **Group scope** and **Group type** you want, and then click **Next**.
4. If Microsoft Exchange Server is deployed in your test domain, you can establish an e-mail address for the group. To do this, select the **Create an Exchange e-mail address** check box. Click **Next**.
5. Use the **Add** and **Remove** buttons to populate the group membership list. When finished, click **Next**.
6. If you need to specify additional properties of the new group, select the **Display the object properties when this wizard closes** check box. Click **Finish**.

Find and disable a user account

To find and then disable a user account

1. In the console tree, select **Active Directory**.
2. In the details pane, right-click your test domain and click **Find**.
3. In the **Find** window, do the following:
    a. From the **Find** list, select **Users**.
    b. In the **Name** box, type the name of the user you want to find, or part of the name.
    c. Click **Find Now**.
    d. In the list of search results, right-click the user and click **Disable Account**.

Use the Active Roles Web Interface

Create a user account and add it to groups

To create a user account and add it to groups

1. Connect to the Web Interface for Administrators: Open your Web browser and navigate to http://localhost/ARWebAdmin.
2. In the **Search** box on the header of the Web Interface page, type the name of the OU where you want to create the user, and then press **Enter**.
3. In the list of search results, click the name of the OU.
4. In the right pane of the Web Interface page, click **New User**.
5. Type in the **First Name**, **Last Name**, and **User logon name** boxes. Click **Next**.
6. Click the **Generate** button (beneath the **Confirm password** box) to generate a password. Click **Finish** (or **Next**, if Microsoft Exchange Server is deployed in your test domain).
7. If Microsoft Exchange Server is deployed in your test domain, you can create a mailbox for the new user. To do this, select the **Create an Exchange mailbox** check box. Click **Finish**.
8. Close the property page that appears.
9. In the **Search** box on the header of the Web Interface page, type the name of the user account you have created.
10. In the list of search results, select the check box next to the name of the user account.
11. In the right pane of the Web page, click **Member Of**.
12. On the **Member Of** page that appears, click the **Add** button.
13. On the **Select Object** page that appears, choose the groups to which you want to add the user account:
    a. Specify search criteria and press Enter to build a list of groups.
    b. Choose the desired groups by selecting the check box next to the name of the group in the list.
    c. When finished, click **OK**.

    For example, you can type group names separated by a semicolon in the Search box at the top of the **Select Object** page, and then press Enter.
14. To remove the user account from groups, on the **Member Of** page, select the check box next to the name the group and then click the **Remove** button.

Find a user and reset the user's password

To find a user account and then reset its password

1. Connect to the Web Interface for Help Desk: Open your Web browser and navigate to http://localhost/ARWebHelpDesk.
2. In the **Search** box on the header of the Web Interface page, type the name of the user you want to find, and then press **Enter**.
3. In the list of search results, select the check box next to the name of the user account.
4. In the right pane of the Web Interface page, click **Reset Password**.
5. On the **Reset Password** page that appears, click the **Generate** button.

   The new password is displayed in the **Password** box.
6. Click the **Finish** button to apply your changes.

Perform self-administration

Active Roles makes it possible to authorize users to administer their own accounts in Active Directory. Specifically, users may be permitted to modify personal information in their accounts. An administrator can use the Active Roles console to delegate this task.

To delegate self-administration

1. In the console tree, select the domain or OU where you want to delegate the self-administration task.
2. Right-click the selection and click **Delegate Control**.
3. In the **Active Roles Security** dialog box, click **Add**.
4. Follow the steps in the Delegation of Control Wizard.
5. On the **Users or Groups** page, click **Add**, use the **Select Objects** dialog box to select the **Self** object, and then click **Next**.
6. On the **Access Templates** page, expand **User Self-management**, and select the check box next to **Self - Account Management**. Click **Next**.
7. Click **Next** two times, and then click **Finish**.
8. In the **Active Roles Security** window, click **OK**.

Once you have delegated the self-administration task, you can check how users can perform self-administration in the Active Roles Web Interface.

To perform self-administration

1. Log on to your server as any user defined in your test domain.
2. Connect to the Web Interface for Self-Administration: Open your Web browser and navigate to http://localhost/ARWebSelfService.
3. On the Web Interface Home page, click **User Profile Editor**.
4. On the **User Profile Editor** page that appears, use the **General**, **Address**, **Telephones**, and **Picture** tabs to view or change your personal information.
5. When finished, click the **Save** button.

Delegating administration

The examples in this section demonstrate how to delegate administration using Active Roles.

Assign the Help Desk role for an OU

When you assign the Help Desk role to a group for a given OU, you authorize the members of that group to reset user passwords, unlock user accounts, and view all properties of user accounts in that OU and its child OUs. The members of the group to which you have assigned an administrative role are referred to as *delegated administrators*.

To assign the Help Desk role for an OU

1. In the Active Roles console, right-click the OU, and then click **Delegate Control**.
2. In the **Active Roles Security** window, click **Add**.
3. Follow the steps in the Delegation of Control wizard.
4. On the **Users or Groups** page, click **Add**.
5. Select the group to which you want to assign the Help Desk role and click **OK**.
6. Click **Next**.
7. On the **Access Templates** page, expand **Active Directory**, select the check box next to **Users – Help Desk**, and then click **Next**.
8. Click **Next**, click **Next**, and then click **Finish**.
9. In the **Active Roles Security** window, click **OK**.

To enable the delegated administrators to browse OUs in the domain, you must grant them the **Read All Properties** permission on the OU objects at the domain level.

To grant the Read All Properties permission

1. Select the domain and use the Delegation of Control wizard as described in the previous procedure.
2. On the **Access Templates** page, expand **Active Directory**, and select the check box next to **OUs – Read All Properties**.

Test the delegated administrator's rights

The delegated administrator can use the Active Roles console to perform administrative tasks. Use the following steps to verify the rights of a delegated administrator using the Active Roles console (MMC Interface).

To verify delegation using the Active Roles console

1. Open the Active Roles console and connect to the Administrative Service as the delegated administrator:
    a. Right-click the console tree root, and then click **Connect**.
    b. In the **Connect to Administration Service** dialog box, click **Options**.
    c. In the **Connect as** area, click **The following user** and specify the user logon name and password of the delegated administrator.
2. In the console tree, select the OU for which the delegated administrator is assigned the Help Desk role.
3. Verify that you can reset passwords and unlock accounts: Right-click a user account in the details pane, and click **Reset Password**.
4. Verify that you can view user properties: Right-click a user account in the details pane, and click **Properties**.

The delegated administrator can also use the Web Interface to perform administrative tasks. Take the following steps to verify the rights of a delegated administrator using the Active Roles Web Interface.

To verify delegation using the Web Interface

1. Log on to your computer with the delegated administrator's user name and password.
2. Connect to the Web Interface for Help Desk: Open your Web browser and navigate to http://localhost/ARWebHelpDesk.
3. In the Search box on the header of the Web Interface page, type the name of the OU for which the delegated administrator is assigned the Help Desk role, and then press Enter.
4. In the list of search results, click the name of the OU to display a list of objects held in that OU.
5. In the list of objects, select the check box next to the name of a user account.
6. Verify that you can reset the user's password and unlock the user account:
    a. In the right pane of the Web Interface page, click **Reset Password**.
    b. On the Reset Password page that appears, specify a new password, clear the **Account is locked out** check box if the check box is selected, and then click **Finish**.

If the user account is not locked out, the **Account is locked out** check box is unavailable.

5

Using Managed Units

The examples in this section demonstrate how to configure Managed Units, and allow you to see how Managed Units work.

Managed Unit (MU) is a collection of objects (administrative view), created for the purposes of distribution of administration, enforcement of business rules, and management of complex network environments. Managed Units provide the capability to separate the management framework from the Active Directory design. By using Managed Units, directory objects can be grouped into administrative views regardless of object location in Active Directory.

Create a Managed Unit

Consider an example in which the AD design is based on geographic locations, with domains named after cities or regions and OUs named for corporate departments or groups. Managed Units could be designed to manage specific departments or groups that are divided across multiple geographic locations.

In this example, each AD domain has a Human Resources (HR) OU and a Sales OU. The Active Roles design has an HR MU and a Sales MU. The HR MU enables administrators to configure the policies and security restrictions for all HR users in one place, while the Sales MU provides the same kind of capability for all Sales users.

MUs are defined by membership rules—criteria that Active Roles uses to evaluate which objects belong to specific MU.

In your test domain, create three OUs named PHX Sales, BST Sales, and SEA Sales. Then, perform the following steps to create the Sales MU.

To create Managed Unit

1. Start the Active Roles console and connect to the Administration Service.
2. Ensure that the console is in Advanced View mode: On the **View** menu, click **Mode**, and then select the **Advanced Mode** option.
3. In the console tree, expand **Configuration**, right-click **Managed Units**, and select

New | Managed Unit.

The New Object - Managed Unit wizard starts.

4. In the **Name** box, type the name of the Managed Unit - **Sales MU**. Click **Next**.
5. Click **Add**.
6. In the list of rule types, click **Include by Query**. Click **OK**.
7. From the **Find** list, select **Organizational Units**.
8. Click **Browse** next to the **In** box, and select your test domain.
9. In the **Name** box, type ***Sales***
10. Optionally, click **Preview Rule**.

    The window displays a list of all the Sales OUs found.
11. Click **Add Rule**.
12. In the wizard, click **Next**, click **Next**, and then click **Finish**.

This procedure ensures that all OUs with names containing 'Sales' are included in the Sales MU. If you only want the MU to include the OUs with specific names, such as 'PHX Sales OU', 'BST Sales OU' and 'SEA Sales OU', use explicit inclusion. To create the Sales MU using explicit inclusion, modify the above procedure as follows:

1. In Step 6, select **Include Explicitly** from the list of rule types.
2. In the **Select Objects** window, specify the OU names (separated by semicolons), and then click **OK**.
3. Follow the steps in the wizard to complete the creation of the MU.

Assign the Full Control role for an MU

Active Roles ensures that security restrictions specified on an MU are applied to all objects held in that MU. When an MU holds a container, all child objects in that container inherit the security restrictions defined at the MU level. This inheritance continues down the directory tree within all containers held in a given MU.

When you assign the Full Control role to a group for a given MU, you authorize the members of that group to perform all administrative tasks in that MU. The members of the group to which you have assigned an administrative role are referred to as *delegated administrators*.

To assign the Full Control role for an MU

1. In the Active Roles console, right-click the Sales MU, and then click **Delegate Control**.
2. In the **Active Roles Security** window, click **Add**.
3. Follow the steps in the Delegation of Control wizard.
4. On the **Users or Groups** page, click **Add**.

5. Select the group to which you want to assign the Full Control role and click **OK**.
6. Click **Next**.
7. On the **Access Templates** page, expand **Active Directory**, select the check box next to **All Objects – Full Control**, and then click **Next**.
8. Click **Next**, click **Next**, and then click **Finish**.
9. In the **Active Roles Security** window, click **OK**.

When assigned the Full Control role for an MU, the delegated administrator is authorized to view the MU and manage all objects in it. In the Active Roles console, the MU appears under **Managed Units** in the console tree.

Test the delegated administrator's rights

Delegated administrators can use the Active Roles console to perform administrative tasks within the MU. Take the following steps to verify the rights of the delegated administrator using the Active Roles console.

To verify delegation using the Active Roles console

1. Start the Active Roles console and connect to the Administrative Server as the delegated administrator:
    a. Right-click the console tree root, and then click **Connect**.
    b. In the **Connect to Administration Service** dialog box, click **Options**.
    c. In the **Connect as** area, click **The following user** and specify the user logon name and password of the delegated administrator.
2. In the console tree, expand **Managed Units | Sales MU**, and select an OU.
3. Verify that you can administer objects in the OU: Right-click an object in the details pane and use commands on the shortcut menu.
4. Verify that you can create new objects: In the console tree, under **Sales MU**, right-click an OU, point to **New**, and select the type of the object to create.

Delegated administrators can also use the Web Interface to perform administrative tasks. Take the following steps to verify the rights of the delegated administrator using the Active Roles Web Interface.

To verify delegation using the Web Interface

1. Log on to your computer with the user name and password of the delegated administrator.
2. Connect to the Web Interface for Administrators: Open your Web browser and navigate to http://localhost/ARWebAdmin.
3. On the Web Interface Home page, click **Directory Management**.

4. On the **Views** tab in the left pane of the Web Interface page, click **Managed Units**.
5. In the list of Managed Units, click **Sales** to display a list of OUs held in the Sales Managed Unit.
6. In the list of OUs, click the name of an OU to display a list of objects held in that OU.
7. Verify that you can create new objects in the OU and administer the OU using commands in the right pane of the Web Interface page.
8. Verify that you can administer objects held in the OU: Select the check box next to the name of an object in the list and then use commands in the upper part of the right pane.

Using Active Roles policies

The examples in this section demonstrate how to configure provisioning policies, and allow you to see how provisioning policy enforcement works in Active Roles.

NOTE: The instructions in this section assume that you are logged on as an Active Roles Admin. The Active Roles Admin account is specified when installing the Administration Service, and defaults to the Administrators local group of the computer running the Administration Service.

Enforce user naming conventions

This section describes how to enforce the following user naming conventions:

- **Full name** must be **ABC**, where

  A consists of max 5 first characters of **Last name**; in case of long **Last name**, **A** consists of only the first 5 characters

  B consists of min 2 characters: numbering beginning with 00; in case of short **Last name**, filling characters are added: 000, 0000, so that **AB** consists of exactly 7 characters

  C consists of one first character of **First name**

  Example: **ivano00a** (**ivano** = 5 characters of **Last name** Ivanov; **00** = numbering; **a** = the first character of **First name** Andre)

- **User logon name** must be the same as **Full name**
- **User logon name (pre-Windows 2000)** must be the same as **Full name**

To enforce these naming conventions, you need to create and apply an Active Roles Policy Object.

Create and apply the Policy Object

Perform the following steps to create and apply the Policy Object using the Active Roles console. First, you create the Policy Object, configure policy for the **Full name** property, and apply the Policy Object to your test domain. Next, you modify the Policy Object to add the policy for the **User logon name** and **User logon name (pre-Windows 2000)** properties.

To create and apply the Policy Object

1. In the console tree, expand **Configuration | Policies**, right-click **Administration**, and select **New | Provisioning Policy**.
2. On the **Welcome** page of the New Provisioning Policy Object wizard, click **Next**.
3. In the **Name** box, type the name for the Policy Object: **User Naming Conventions**. Click **Next**.
4. On the **Policy to Configure** page, select **Property Generation and Validation**. Click **Next**.
5. On the **Controlled Property** page, click **Select**.
6. In the **Select Object Type and Property** dialog box:
    a. From the **Object type** list, select **User**.
    b. From the **Object property** list, select **Name**.
    c. Click **OK**.
7. On the **Controlled Property** page, click **Next**.
8. On the **Configure Policy Rule** page, select the **'Name' must be <value>** check box, and then click the item **<click to add value>** in the **Edit policy rule** box.
9. In the **Add Value** dialog box, click **Configure**.
10. In the **Configure Value** dialog box, click **Add**.
11. In the **Add Entry** window:
    a. Under **Entry type**, click **User Property**.
    b. Under **Entry properties**, click **Select**, and then select **Last Name** from the **Object property** list. Click **OK**.
    c. Click **The first**, and then enter **5** in the box next to that option.
    d. Select the **If value is shorter, add filling characters at the end of value** check box, and then, in the **Filling character** box, enter **0**.
    e. Click **OK**.
12. In the **Configure Value** dialog box, click **Add**.
13. In the **Add Entry** window, click **Text**, type **00**, and click **OK**.
14. In the **Configure Value** dialog box, click **Add**.

15. In the **Add Entry** window:
    a. Under **Entry type**, click **User Property**.
    b. Under **Entry properties**, click **Select**, and then select **First Name** from the **Object property** list. Click **OK**.
    c. Click **The first**, and then enter **1** in the box next to that option.
    d. Click **OK**.
16. In the **Configure Value** dialog box, click **OK**.
17. In the **Add Value** dialog box, click **OK**.
18. On the **Configure Policy Rule** page, click **Next**.
19. On the **Policy Description** page, click **Next**.
20. On the **Enforce Policy** page, click **Add**.
21. In the **Select Objects** window, select your test domain, click **Add**, and then click **OK**.
22. Click **Next**, and then click **Finish**.

Next, perform the following steps to configure policy for the **User logon name** and **User logon name (pre-Windows 2000)** properties.

To add policies to the Policy Object

1. In the console tree, select **Configuration | Policies | Administration**.
2. In the details pane, right-click **User Naming Conventions** and click **Properties**.
3. On the **Policies** tab in the **User Naming Conventions Properties** dialog box, click **Add**.
4. On the **Welcome** page of the Add Provisioning Policy wizard, click **Next**.
5. On the **Policy to Configure** page, select **Property Generation and Validation**. Click **Next**.
6. On the **Controlled Property** page, click **Select**.
7. In the **Select Object Type and Property** dialog box:
    a. From the **Object type** list, select **User**.
    b. From the **Object property** list, select **Account Name (UPN Prefix)**.
    c. Click **OK**.
8. On the **Controlled Property** page, click **Next**.
9. On the **Configure Policy Rule** page, select the **'Account Name (UPN Prefix)' must be <value>** check box, and then click the item **<click to add value>** in the **Edit policy rule** box.
10. In the **Add Value** dialog box, click **Configure**.
11. In the **Configure Value** dialog box, click **Add**.

12. In the **Add Entry** dialog box window:
    a. Under **Entry type**, click **User Property**.
    b. Under **Entry properties**, click **Select**, and then select **Name** from the **Object property** list. Click **OK**.
    c. Click **OK**.
13. In the **Configure Value** dialog box, click **OK**.
14. In the **Add Value** dialog box, click **OK**.
15. On the **Configure Policy Rule** page, click **Next**.
16. Click **Next**, and then click **Finish**.
17. Repeat Steps 3-16 with the following modification to configure policy for User logon name (pre-Windows 2000):
    - In Step 7, from the **Object property** list, select **Logon Name (pre-Windows 2000)**.
18. In the **User Naming Conventions Properties** dialog box, click **OK**.

Verify the naming conventions

Use the following steps to see how the naming conventions are enforced when you create a user account using the Active Roles console (MMC Interface).

To verify naming conventions using the Active Roles console

1. In the console tree, right-click an OU in your test domain, and select **New | User**.
2. Fill in the **First name** and **Last name** boxes.
3. Verify that the console automatically fills in the **Full name**, **User logon name**, and **User logon name (pre-Windows 2000)** boxes in accordance with the user naming conventions.
4. Complete the New Object - User wizard.
5. Right-click the newly created user account, click **Properties**, and examine the **Properties** dialog box to verify that the user properties are in compliance with the naming conventions.

Use the following steps to see how the naming conventions are enforced when you create a user account using the Active Roles Web Interface.

To verify naming conventions using the Web Interface

1. In the Web Interface for Administrators, select an OU from your test domain.
2. In the right pane of the Web Interface page, click **New User**.
3. Fill in the **First Name** and **Last Name** fields.

4. Verify that the Web Interface automatically fills in the **Name**, **User logon name**, and **User logon name (pre-Windows 2000)** fields in accordance with the user naming conventions.
5. Follow the steps in the wizard to complete the creation of the user account.

Clean up your test environment

The policy you configured and used in this section may interfere with the policies discussed in the sections that follow. To prevent this issue, you should block the effect of the User Naming Convention policy on your test domain before you proceed to the next sections.

To block the effect of the User Naming Conventions policy

1. In the Active Roles console, right-click your test domain, and click **Enforce Policy**.
2. In the **Active Roles Policy** window, locate the list entry named **User Naming Conventions**, and select the **Blocked** check box in that entry.
3. Click **OK** to close the **Active Roles Policy** window.

Use a Logon Name Generation policy

You can use a policy of the Logon Name Generation category to automate the assignment of the pre-Windows 2000 user logon name upon creation or modification of a user account. When configuring a policy of this category, you can define multiple rules or apply an incremental numeric value to ensure uniqueness of the policy-generated name.

This section covers both the scenario that uses a uniqueness number and the scenario that involves multiple rules to generate logon names.

Scenario 1: Using uniqueness number

The policy described in this scenario generates the pre-Windows 2000 user logon name in accordance with this rule: the first character of the user first name, optionally followed by a uniqueness number, followed by the user last name. The length of the policy-generated name is not more than 8 characters. If the name is longer, trailing characters are truncated as needed. Examples of names generated by this policy are as follows:

- JSmitson
- J1Smitso
- J2Smitso

The policy generates the name J1Smitso for the user John Smitson if the name JSmitson is in use. If both JSmitson and J1Smitso are in use, the policy generates the name J2Smitso, and so on.

To implement this scenario, you need to create and apply an Active Roles Policy Object. The following two sub-sections elaborate on the steps to implement this scenario.

Create and apply the Policy Object

You can create and apply the Policy Object using the Active Roles console as follows.

To create and apply the Policy Object

1. In the console tree, expand **Configuration | Policies**, right-click **Administration**, and select **New | Provisioning Policy**.
2. On the **Welcome** page of the New Provisioning Policy Object wizard, click **Next**.
3. In the **Name** box, type the name of the Policy Object: **User Logon Name Generation**. Click **Next**.
4. On the **Policy to Configure** page, select **User Logon Name Generation**. Click **Next**.
5. On the **User Logon Name (pre-Windows 2000) Generation Rules** page, click **Add**.
6. In the **Configure Value** dialog box, click **Add**.
7. In the **Add Entry** window, configure the entry to include the first character of the user first name:
    a. Under **Entry type**, click **User Property**.
    b. Under **Entry properties**, click **Select**.
    c. In the **Select Object Property** window, click **First Name** in the **Object property** list, and then click **OK**.
    d. Under **Entry properties**, click **The first**, and verify that the box next to that option reads **1**.
    e. Click **OK**.
8. In the **Configure Value** dialog box, click **Add**.
9. In the **Add Entry** window, configure the entry to optionally include a uniqueness number:
    a. Under **Entry type**, click **Uniqueness Number**.
    b. Under **Entry properties**, click **Add if the property value is in use**.
    c. Click **OK**.
10. In the **Configure Value** dialog box, click **Add**.

11. In the **Add Entry** window, configure the entry to include the user last name:
    a. Under **Entry type**, click **User Property**.
    b. Under **Entry properties**, click **Select**.
    c. In the **Select Object Property** window, click **Last Name** in the **Object property** list, and then click **OK**.
    d. Click **OK**.

    At this point, the **Configured value** box should display the following syntax:

    ```
    %1<givenName>{@counter(optional)}%<sn>
    ```
12. Click **OK** to close the **Configure Value** dialog box.
13. On the **User Logon Name (pre-Windows 2000) Generation Rules** page, click the **Advanced** button.
14. In the **Advanced** dialog box, in the **Maximum length, in characters** box, type **8**, and then click **OK**.
15. On the **User Logon Name (pre-Windows 2000) Generation Rules** page, click **Next**.
16. On the **Enforce Policy** page, click **Add**.
17. In the **Select Objects** window, select your test domain, click **Add**, and then click **OK**.
18. Click **Next**, and then click **Finish**.

You must also take certain steps to override the effect of the default logon name generation policy. You may block the policy effect for the entire domain or for individual containers within the domain.

To block the effect of the default logon name generation policy

1. In the Active Roles console, right-click your test domain (or a certain container, such as OU), and click **Enforce Policy**.
2. In the **Active Roles Policy** window, locate the list entry named **Built-in Policy - Default Logon Name**, and select the **Blocked** check box in that entry.
3. Click **OK** to close the **Active Roles Policy** window.

Test the User Logon Name Generation policy

The policy effect on the user creation operation is as follows. On the user creation forms, the Active Roles user interfaces provide a **Generate** button to create a pre-Windows 2000 user logon name in accordance with the policy rule. In the event of a naming conflict, clicking the **Generate** button causes the policy to add a uniqueness number to the name.

You can use the following steps to verify the policy behavior in the Active Roles console.

To verify the policy behavior using the Active Roles console

1. Create the user account for the first user:
    a. In the console tree, right-click an OU, and select **New | User**.
    b. In **First name**, type **John**; in **Last name**, type **Smitson**.
    c. Click the button next to the **User logon name (pre-Windows 2000)** box.
    This will generate **JSmitson**.
    d. Complete the creation of the user account.
2. Create the user account for the second user:
    a. In the console tree, right-click an OU, and select **New | User**.
    b. In **First name**, type **Jane**; in **Last name**, type **Smitson**.
    c. Click the button next to the **User logon name (pre-Windows 2000)** box.
    This will generate **J1Smitso**, because the name **JSmitson** is in use.
    d. Complete the creation of the user account.
3. Create the user account for the third user:
    a. In the console tree, right-click an OU in your test domain, and select **New | User**.
    b. In **First name**, type **Joanne**; in **Last name**, type **Smitson**.
    c. Click the button next to the **User logon name (pre-Windows 2000)** box.
    This will generate **J2Smitso**, since both the **JSmitson** and **J1Smitso** names are in use.
    d. Complete the creation of the user account.

Scenario 2: Using multiple rules

The policy described in this scenario uses multiple rules to generate the pre-Windows 2000 user logon name based on the following rules:

1. The first character of the user first name, followed by the user last name
2. The first two characters of the user first name, followed by the user last name
3. The first three characters of the user first name, followed by the user last name

The length of the policy-generated name is at most 8 characters. If the name is longer, trailing characters are truncated as needed.

Examples of names generated by this policy are as follows:

- JSmitson
- JoSmitso
- JohSmits

The policy generates the name JoSmitso for the user John Smitson if the name JSmitson is in use. If both JSmitson and JoSmitso are in use, the policy generates the name JohSmits.

If the policy fails to generate a unique name, it allows a name to be specified manually.

To implement this scenario, you might re-configure the **User Logon Name Generation** Policy Object, used in the previous scenario.

Configure the Policy Object

Use the Active Roles console to make the appropriate changes to the **User Logon Name Generation** Policy Object.

To modify the Policy Object

1. In the Active Roles console, right-click the **User Logon Name Generation** Policy Object, and click **Properties**.
2. On the **Policies** tab, select the policy, and then click **View/Edit**.
3. Remove the uniqueness number entry from the first rule:
    a. On the **Generation Rules** tab, select the rule, and then click **View/Edit**.
    b. In the **Configure Value** dialog box, select the **Uniqueness number** entry, click **Remove**, and then click **OK**.
4. Add the second rule:
    a. On the **Generation Rules** tab, click **Add**.
    b. In the **Configure Value** dialog box, click **Add**.
    c. In the **Add Entry** window:
        a. Select the **User Property** entry type
        b. Select the **First name** property
        c. Click **The first** and then type **2**
        d. Click **OK**
    d. In the **Configure Value** dialog box, click **Add**.
    e. In the **Add Entry** window:
        a. Select the **User Property** entry type
        b. Select the **Last name** property
        c. Click **OK**
    f. In the **Configure Value** dialog box, click **OK**.
5. Repeat Step 4, modifying Sub-step c) as follows in order to add the third rule: Click **The first** and then type **3**.
6. On the **Generation Rules** tab, select the **Allow manual edits of pre-Windows 2000 logon name** check box, and then click **Only if a unique name cannot be generated by this policy**.

7. Click **OK** to close the **User Logon Name Generation Policy Properties** dialog box.
8. Click **OK** to close the **Properties** dialog box for the Policy Object.

Test the User Logon Name Generation policy

The policy effect on the user creation operation is as follows. On the user creation forms, the Active Roles user interfaces provide a **Generate** button to create a pre-Windows 2000 user logon name in accordance with the policy rules. In the event of a naming conflict, clicking the **Generate** button causes the policy to apply a subsequent rule.

You can use the following steps to verify the policy behavior in the Active Roles console.

To verify the policy behavior using the Active Roles console

1. Create the user account for the first user:
    a. In the console tree, right-click an OU, and select **New | User**.
    b. In **First name**, type **Jack**; in **Last name**, type **Smitson**.
    c. Click the button next to the **User logon name (pre-Windows 2000)** box.
    This will generate **JaSmitso**. The policy applies the second rule.
    d. Complete the creation of the user account.
2. Create the user account for the second user:
    a. In the console tree, right-click an OU, and select **New | User**.
    b. In **First name**, type **Jay**; in **Last name**, type **Smitson**.
    c. Click the button next to the **User logon name (pre-Windows 2000)** box.
    This will generate **JaySmits**. The policy applies the third rule.
    d. Complete the creation of the user account.
3. Create the user account for the third user:
    a. In the console tree, right-click an OU, and select **New | User**.
    b. In **First name**, type **Jaycob**; in **Last name**, type **Smitson**.
    c. Click the button next to the **User logon name (pre-Windows 2000)** box.

    In this case, the policy fails to generate a unique name since each of the three generation rules returns a name that is in use by an existing user account in your test domain. The console prompts you to specify a name because the policy is configured to allow this action in the situation where it cannot generate a unique name.

Clean up your test environment

The policy you configured and used in this section may interfere with the policies discussed in the sections that follow. To prevent this issue, you should block the effect of the E-mail

Alias Generation policy on your test domain before you proceed to the next sections.

To block the effect of the E-mail Alias Generation policy

1. In the Active Roles console, right-click your test domain, and click **Enforce Policy**.
2. In the **Active Roles Policy** window, locate the list entry named **E-mail Alias Generation**, and select the **Blocked** check box in that entry.
3. Click **OK** to close the **Active Roles Policy** window.

Use an E-mail Alias Generation policy

To implement the scenario described in this section, you must have Microsoft Exchange 2007 or later installed in your test Active Directory forest.

You can use a policy of the E-mail Alias Generation category to automate the assignment of the e-mail alias when designating a user as mailbox-enabled on Microsoft Exchange Server. By default, Microsoft Exchange Server provides for the following recipient e-mail address format: <*alias*>@<*domain*>. You can use pre-defined rules to generate e-mail aliases, or configure custom rules. Custom rules provide for addition of an incremental numeric value to ensure uniqueness of the alias.

The policy described in this scenario generates the e-mail alias in accordance with this rule: user first name, optionally followed by a three-digit uniqueness number, followed by a period, followed by the user last name. Examples of aliases generated by this rule are as follows:

- John.Smith
- John001.Smith
- John002.Smith

The policy generates the alias John001.Smith for the user John Smith if the alias John.Smith is in use. If both John.Smith and John001.Smith are in use, the policy generates the alias John002.Smith, and so on.

The following two sections elaborate on the steps to implement this scenario.

Create and apply the Policy Object

You can create and apply the Policy Object using the Active Roles console as follows.

To create and apply the Policy Object

1. In the console tree, expand **Configuration | Policies**, right-click **Administration**, and select **New | Provisioning Policy**.
2. On the **Welcome** page of the New Provisioning Policy Object wizard, click **Next**.

3. In the **Name** box, type the name of the Policy Object: **E-mail Alias Generation**. Click **Next**.
4. On the **Policy to Configure** page, click **E-mail Alias Generation**. Click **Next**.
5. On the **E-mail Alias Generation Rule** page, click **Other combination of user properties**, and then click **Configure**.
6. In the **Configure Value** dialog box, click **Add**.
7. In the **Add Entry** window, configure the entry to include the user first name:
    a. Under **Entry Type**, click **User Property**.
    b. Under **Entry Properties**, click **Select**.
    c. In the **Select Object Property** window, click **First Name** in the **Object property** list, and then click **OK**.
    d. Click **OK**.
8. In the **Configure Value** dialog box, click **Add**.
9. In the **Add Entry** window, configure the entry to optionally include a uniqueness number:
    a. Under **Entry type**, click **Uniqueness Number**.
    b. Under **Entry properties**, set the entry options:
        a. Click **Add if the property value is in use**
        b. Select the **Fixed-length number, with leading zeros** check box
        c. In the box next to **Length of the number, in digits**, type **3**
    c. Click **OK**.
10. In the **Configure Value** dialog box, click **Add**.
11. In the **Add Entry** window, configure the entry to include the period character:
    a. Under **Entry properties**, type the period character.
    b. Click **OK**.
12. In the **Configure Value** dialog box, click **Add**.
13. In the **Add Entry** window, configure the entry to include the user first name:
    a. Under **Entry type**, click **User Property**.
    b. Under **Entry properties**, click **Select**.
    c. In the **Select Object Property** window, click **Last Name** in the **Object property** list, and then click **OK**.
    d. Click **OK**.

    At this point, the **Configured value** box should display the following syntax:

    ```
    %<givenName>{@counter(optional,3)}.%<sn>
    ```
14. Click **OK** to close the **Configure Value** dialog box.
15. On the **E-mail Alias Generation Rule** page, click **Next**.
16. On the **Enforce Policy** page, click **Add**.

17. In the **Select Objects** window, select your test domain, click **Add**, and then click **OK**.
18. Click **Next**, and then click **Finish**.

You must also take certain steps to override the effect of the default e-mail alias generation policy. You may block the policy effect for the entire domain or for individual containers within the domain.

To override the default e-mail alias generation policy

1. In the Active Roles console, right-click your test domain (or a certain container, such as OU), and click **Enforce Policy**.
2. In the **Active Roles Policy** window, locate the list entry named **Built-in Policy - Default E-mail Alias**, and select the **Blocked** check box in that entry.
3. Click **OK** to close the **Active Roles Policy** window.

Test the E-mail Alias Generation policy

The policy effect on the user creation operation is as follows. On the user creation forms, the Active Roles user interfaces provide a **Generate** button to create an e-mail alias in accordance with the policy rule. In the event of an alias naming conflict, clicking the **Generate** button causes the policy to add a uniqueness number to the alias.

You can use the following steps to verify the policy behavior in the Active Roles console.

To verify the policy behavior using the Active Roles console

1. Create the user account for the first user:
    a. In the console tree, right-click an OU in your test domain, and select **New | User**.
    b. In **First name**, type **John**; in **Last name**, type **Smith**.
    c. Fill in **User logon name** and **User logon name (pre-Windows 2000)**.
    d. Click **Next**.
    e. Fill in **Password** and **Confirm password**, and click **Next**.
    f. Click the button located next to the **Alias** box.

    This will generate **John.Smith** as the e-mail alias.
    g. Complete the creation of the user account.
2. Create the user account for the second user:
    a. In the console tree, right-click an OU in your test domain, and select **New | User**.
    b. In **First name**, type **John**; in **Initials**, type **A**, in **Last name**, type **Smith**.
    c. Fill in **User logon name** and **User logon name (pre-Windows 2000)**.
    d. Click **Next**.

e. Fill in **Password** and **Confirm password**, and click **Next**.

f. Click the button located next to the **Alias** box.

This will generate **John001.Smith** as the e-mail alias, since the alias **John.Smith** is in use.

g. Complete the creation of the user account.

3. Create the user account for the third user:

a. In the console tree, right-click an OU in your test domain, and select **New | User**.

b. In **First name**, type **John**; in **Initials**, type **B**, in **Last name**, type **Smith**.

c. Fill in **User logon name** and **User logon name (pre-Windows 2000)**.

d. Click **Next**.

e. Fill in **Password** and **Confirm password**, and click **Next**.

f. Click the button located next to the **Alias** box.

This will generate **John002.Smith** as the e-mail alias, since both the **John.Smith** and **John001.Smith** aliases are in use.

Clean up your test environment

The policy you configured and used in this section may interfere with the policies discussed in the sections that follow. To prevent this issue, you should block the effect of the E-mail Alias Generation policy on your test domain before you proceed to the next sections.

To block the effect of the E-mail Alias Generation policy

1. In the Active Roles console, right-click your test domain, and click **Enforce Policy**.
2. In the **Active Roles Policy** window, locate the list entry named **E-mail Alias Generation**, and select the **Blocked** check box in that entry.
3. Click **OK** to close the **Active Roles Policy** window.

Enforce group scope restrictions

This scenario describes how to configure a policy to ensure that only non-universal groups are permitted to be created. The script prevents Active Roles from creating universal groups.

The policy is based on a script that detects the group scope setting and disallows the creation of groups with universal scope. The script comes with Active Roles SDK. You can access the Active Roles SDK documentation by selecting **Active Roles 7.2 SDK** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

Prepare the script module

To implement this policy, you first need to prepare a script module using the Active Roles console.

To prepare the script module

1. In the console tree, expand **Configuration**, right-click **Script Modules**, and then click **Import**.
2. Use the **Import Script** window to open the file **RestrictGroupScope.ps1**, located in the folder **%ProgramFiles%\One Identity\Active Roles\7.2\SDK\Samples\RestrictGroupScope**
3. In the **Script** dialog box, click **OK**.

The module **RestrictGroupScope** is created in the **Script Modules** container. You can view the script code in the details pane by selecting the module in the console tree.

Create and apply the Policy Object

Once you have prepared the script module, you can create, configure, and apply the Policy Object using the Active Roles console.

To create and apply the Policy Object

1. In the console tree, expand **Configuration | Policies**, right-click **Administration**, and select **New | Provisioning Policy**.
2. On the **Welcome** page of the New Provisioning Policy Object wizard, click **Next**.
3. In the **Name** box, type the name of the Policy Object: **Group Scope Restrictions**. Click **Next**.
4. On the **Policy to Configure** page, select **Script Execution**. Click **Next**.
5. On the **Script Module** page, select **RestrictGroupScope**. Click **Next**.
6. On the **Policy Parameters** page, click **Next**.
7. On the **Enforce Policy** page, click **Add**.
8. In the **Select Objects** window, select your test domain, click **Add**, and then click **OK**.
9. Click **Next**, and then click **Finish**.

Test the group scope restrictions

Perform the following steps to see how group type restrictions are enforced when you create a mail-enabled group using the Active Roles console.

To verify the group type restrictions

1. In the console tree, right-click an OU in your test domain, and select **New | Group**.
2. Type a name for the group.
3. Under **Group scope**, click **Universal**.
4. Click **Next**.

   This will cause an error message to appear stating that you cannot create universal groups.
5. Close the error message box.
6. Under **Group scope**, click **Global**.
7. Click **Next** and notice that no error message appears this time.

As you can see, the policy allows you to created a group with any scope except for universal.

Use a Home Folder Provisioning policy

This section describes how to configure Active Roles to automatically create or rename the user's home folder on a certain file server when a user is created or renamed with Active Roles. In this scenario, renaming a user means modifying the User logon name (pre-Windows 2000) property of the user account.

NOTE: This scenario requires that the service account of the Administration Service be a member of the Administrators group of the file server on which you want Active Roles to manage home folders. You specify the service account in Active Roles Configuration Center when configuring the Administration Service (see Run Active Roles Configuration Center earlier in this document).

To implement this policy, you need to create and apply an Active Roles Policy Object.

Create and apply the Policy Object

Perform the following steps to create and apply the Policy Object using the Active Roles console.

To create and apply the Policy Object

1. In the console tree, expand **Configuration | Policies**, right-click **Administration**, and select **New | Provisioning Policy**.
2. On the Welcome page of the New Provisioning Policy Object wizard, click **Next**.
3. In the **Name** box, type the name of the Policy Object: **Handling Home Folders**. Click **Next**.

4. On the **Policy to Configure** page, select **Home Folder AutoProvisioning**. Click **Next**.
5. On the **Home Folder Management** page:
    a. In the **To** box, type \\<*Server*>\<*Home*>\%USERNAME%, where <*Server*> is the name of your file server, <*Home*> is the name of a network share on your file server. The policy will create home folders in the network share you have specified.
    b. Select both the **Apply this home folder setting when user account is created** and **Apply this home folder setting when user account is renamed** check boxes.
    c. Ensure that the **Create or rename home folder on file server as needed** check box is selected.
    d. Click **Next**.
6. On the **Home Share Management** page, click **Next**.
7. On the **Enforce Policy** page, click **Add**.
8. In the **Select Objects** window, select your test domain, click **Add**, and then click **OK**.
9. Click **Next**, and then click **Finish**.

Test the Home Folder policy

Perform the following steps to see how Active Roles manages the user's home folder when you create or rename a user account by using the Active Roles console.

To verify the home folder policy

1. Using the Active Roles console, create a user account in any OU in your test domain.
2. Right-click the user account created in Step 1 and click **Properties**.
3. In the **Properties** dialog box, click the **Profile** tab.
4. On the **Profile** tab, in the **Home folder** area, examine the home folder path: The path is identical to the network path you specified when creating the Policy Object, with the user logon name (pre-Windows 2000) substituted for %USERNAME%.
5. On your file server, verify that the home folder is created.
6. In the **Properties** dialog box for the user account, click the **Account** tab.
7. Modify the value in the **User logon name (pre-Windows 2000)** box, and click **Apply**.
8. On the **Profile** tab, in the **Home folder** area, examine the home folder path: The home folder name is identical to the new value of User logon name (pre-Windows 2000).
9. On your file server, verify that the home folder is renamed.

Managing Exchange recipients

This section provides sample procedures that illustrate how you can use the Active Roles console or Web Interface to perform Exchange tasks, and manage Exchange-related properties of users and groups. To follow these procedures, you must have Microsoft Exchange 2007 or later installed in your test domain.

Create a mailbox for an existing user

Using the Active Roles console or Web Interface, you can create an Exchange mailbox for an existing user account. To perform this task, follow the steps below.

To create a mailbox for an existing user by using the Active Roles console

1. Right-click the user account and click **Exchange Tasks**.
2. In the Exchange Task Wizard, click **Next**, click **Create User Mailbox**, and then click **Next**.
3. Verify that the information in the **Alias** and **Mailbox database** boxes is correct, and then click **Next**.
4. Click **Finish**.

To create a mailbox for an existing user by using the Web Interface

1. Connect to the Web Interface for Administrators: Open your Web browser and navigate to http://localhost/ARWebAdmin.
2. In the **Search box** on the header of the Web Interface page, type the name of the user account, and then press **Enter**.
3. In the list of search results, select the check box next to the name of the user account.
4. In the right pane of the Web Interface page, click **Create User Mailbox**.

   If the **Create User Mailbox** command is unavailable, the selected user already has a mailbox.

5. Verify that the information in the **Alias** and **Mailbox database** boxes is correct, and then click the **Finish** button.

Modify a user's e-mail address

You can use the Active Roles console or the Web Interface to modify the e-mail address of a mailbox-enabled user. To perform this task, follow the steps below.

To modify e-mail address using the Active Roles console

1. Right-click the mailbox-enabled user account you want to modify, and then click **Properties**.
2. On the **E-mail Addresses** tab, double-click the address you want to modify.
3. Modify the e-mail address information that appears for the address you have selected, and click **OK**.
4. Click **OK** to close the **Properties** dialog box.

To modify e-mail address using the Web Interface

1. Connect to the Web Interface for Administrators: Open your Web browser and navigate to http://localhost/ARWebAdmin.
2. In the **Search** box on the header of the Web Interface page, type the name of the mailbox-enabled user account, and then press **Enter**.
3. In the list of search results, select the check box next to the name of the user account.
4. In the right pane of the Web Interface, click **Exchange Properties**.
5. Click the **E-mail Addresses** tab on the **Exchange Properties** page that appears.
6. In the **E-mail addresses** list, click the address you want to modify, and then click the **Edit** button.
7. In the **E-mail Address** dialog box that appears, modify the e-mail address information as needed, and then click **OK**.
8. Click the **Save** button to commit your changes.

8

Managing permissions in Active Directory

The Active Roles console provides a centralized view of all permission entries for any object in Active Directory. For each permission entry, the view displays a number of properties, including the permission description, origin, and security principal. Additional properties of permission entries can be displayed and the native security editor can be accessed.

To further simplify and enhance the management of permission entries, Active Rolessions in Active Directory by using of Access Templates. Active Roles provides the option to keep Active Directory native security updated with selected permissions specified using Access Templates.

This section outlines the procedures to follow in order to see how Active Roles assists in managing Active Directory permission entries.

View or modify permission entries

Perform the following steps to manage Active Directory permission entries using the Active Roles console.

To view or modify permission entries

1. On the **View** menu, check **Advanced Details Pane**.
2. In the console tree, expand **Active Directory** and browse the domain to locate and select a directory object or container.
3. In the lower sub-pane of the details pane, click the **Native Security** tab.

   This tab displays a list of all permission entries for the selected object or container.
4. On the **Native Security** tab, right-click an entry in the list, and then click **Properties** to examine the selected permission entry.

   The **ACE Properties** window displays the following properties of the permission entry you have selected:

a. **Type** Permission type (Allow or Deny).

b. **Status** For an entry specified by using an Access Template, view whether the entry is in sync with Active Roles (**OK** if in sync or, otherwise, an indication of a problem). Disregard if the entry is specified in a different way.

c. **Trustee** Security principal to which the permission entry is assigned.

d. **Source** For an entry specified by using an Access Template, identifies the name of the Access Template. <None> or Default AD Security if the entry is specified in a different way.

e. **Inherited from** Container from which the permission entry is inherited (if any).

f. **Applies to** Where the permission entry is applied (this object only, this object and all child objects, etc.).

g. **Permissions** A list of permissions specified by the permission entry.

5. To delete a permission entry, right-click the entry, and then click **Delete**.
6. To start the native Active Directory ACL editor, right-click a permission entry, and then click **Edit Native Security**.

   You can use the ACL editor to add new permission entries and view or modify existing permission entries.

Manage native security with Access Templates

To add permission entries to Active Directory using an Access Template, perform the following steps in the Active Roles console.

To apply Access Template to Active Directory

1. Select an Active Directory container to which you want to add permission entries.
2. Right-click the selection and click **Delegate Control**.
3. In the **Active Roles Security** window, click **Add**.
4. Follow the steps in the Delegation of Control wizard.
5. On the **Permissions Propagation** page, select the **Propagate permissions to Active Directory** check box.
6. Complete the Delegation of Control wizard.
7. In the **Active Roles Security** window, click **OK**.

Once you have completed these steps, new permission entries are created in Active Directory. You can examine them using the Active Roles console.

To examine permission entries

- Select the container you selected in Step 1 of the previous procedure, and examine the list of permission entries on the **Native Security** tab in the lower sub-pane of the details pane.

  The new entries are added to the list. The name of an Access Template in the **Source** column indicates the entries specified through the use of that Access Template.

Active Roles maintains one-way synchronization from Active Roles security to each permission entry defined with the Permissions Propagation option.

To manage synchronization of permissions

1. Go to the **Active Roles Security** tab in the advanced details pane.

   The **Sync to Native Security** column indicates whether permissions are synchronized to Active Directory.

2. On the **Active Roles Security** tab, right-click an entry with the **Yes** label in the **Sync to Native Security** column, click **Desync to AD**, and then click **Yes**.

   The label in the **Sync to Native Security** column changes to **No**.

3. Go to the **Native Security** tab and refresh the view (press F5).

   Active Roles removes the permission entries corresponding to the entry you selected on the **Active Roles Security** tab in Step 2.

4. Go to the **Active Roles Security** tab, right-click the entry you selected in Step 2, and then click **Sync to AD**.

   The label in the **Sync to Native Security** column changes to **Yes**.

5. Go to the **Native Security** tab and refresh the view (press F5).

   Active Roles adds the permission entries corresponding to the entry you selected on the **Active Roles Security** tab in Step 4.

6. Go to the **Active Roles Security** tab, right-click a blank area of the tab, and then click **Add**.
7. Follow the steps in the Delegation of Control Wizard to apply an Access Template.
8. On the **Permissions Propagation** page of the wizard, select the **Propagate permissions to Active Directory** check box.
9. Go to the **Native Security** tab and refresh the view (press F5).

   Active Roles adds the permission entries corresponding to the Access Template you have applied by using the Delegation of Control Wizard.

9

Using dynamic groups

The groups whose membership lists are automatically maintained by Active Roles are referred to as *dynamic groups*. For dynamic groups, Active Roles ensures that their membership lists include only those objects that match membership rules, even if administrative tools other than Active Roles are used to manage groups.

To automate the maintenance of group membership lists, Active Roles provides:

- Rules-based mechanism that automatically adds and removes objects from groups whenever object attributes change in Active Directory
- Flexible membership criteria that enable both query-based and static population of groups

The membership criteria fall into these categories:

- **Include Explicitly** Ensures that specified objects are included in the membership list regardless of any changes made to the objects.
- **Include by Query** Populates the membership list with objects that have certain properties. When an object is created, or when its properties are changed, Active Roles adds or removes it from the membership list depending on whether the object's properties match the search criteria specified.
- **Include Group Members** Populates the membership list with members of specified groups. When an object is added or removed from those groups, Active Roles adds or removes that object from the membership list.
- **Exclude Explicitly** Ensures that specified objects are not in the membership list regardless of any changes made to those objects.
- **Exclude by Query** Ensures that objects with certain properties are not in the membership list. Active Roles automatically removes objects from the membership list depending on whether the objects' properties match the search criteria specified.
- **Exclude Group Members** Ensures that members of specified groups are not in the membership list. When an object is added to any one of those groups, Active Roles automatically removes that object from the membership list.

Active Roles processes membership rules in the following order by rule category:

- Include by Query
- Include Group Members

- Exclude by Query
- Exclude Group Members
- Include Explicitly
- Exclude Explicitly

This section outlines the procedures to follow in order to configure dynamic groups and to examine the behavior of dynamic groups.

Configure a dynamic group

To configure a dynamic group, perform the following steps using the Active Roles console.

To create a dynamic group

1. Right-click a group, and then click **Convert to Dynamic Group**.
2. In the confirmation message box, click **Yes**.

   The New Membership Rule wizard starts.
3. Select a rule type, such as **Include Explicitly**.
4. Click **Next**.
5. Click **Add** and select any objects to include in the group.
6. Click **Finish**.

NOTE: Once you have added a membership rule to a regular group, the group becomes a dynamic group. This behavior does not depend on the type of the rule. When a group is converted, all of its previous members are removed. Therefore, after you complete these steps, the group only includes the objects you selected.

Next, add membership rules to further configure the dynamic group. To accomplish this task, perform the following steps.

To set up membership rules

1. Right-click the dynamic group and click **Properties**.
2. In the **Properties** dialog box, click the **Membership Rules** tab.
3. On the **Membership Rules** tab, click **Add**.

   This displays the **Membership Rule Type** dialog box.
4. In the list of rule types, click **Include by Query**. Click **OK**.

   This displays the **Create Membership Rule** dialog box.
5. From the **Find** list, select **Users**.
6. From the **In** list, select your test domain.
7. In the **Name** box, type **a**.

8. Click **Add Rule**.

   As a result, the group will include all users whose names begin with the letter **a**. (You might specify a different query-based rule.)

9. On the **Membership Rules** tab, click **Add**.
10. In the list of rule types, click **Include Group Members** and click **OK**.
11. In the **Select Objects** window, select the Domain Admins group, click **Add**, and then click **OK**.

    As a result, the group will include all members of the Domain Admins group. (You might choose a different group.)

12. On the **Membership Rules** tab, click **Add**.
13. In the list of rule types, click **Exclude Explicitly**. Click **OK**.
14. In the **Select Objects** window, select the Administrator account, click **Add**, and then click **OK**.

    As a result, Administrator will be excluded from the group. (You might choose a different user account to exclude.)

15. In the **Properties** dialog box, click **OK**.

If you no longer want the group to be dynamic, right-click the group and then click **Convert to Basic Group**. This operation only removes all membership rules from the group, whereas the group membership list remains intact.

Test the dynamic group

Use the following tests to examine the behavior of the dynamic group you have configured. In the Active Roles console, right-click your dynamic group and click **Properties**. Examine the **Properties** dialog box:

- On the **General** tab, the **Notes** box contains a text indicating that this group is a dynamic group.
- On the **Members** tab, you cannot modify the membership list.
- The **Membership Rules** tab displays a list of membership rules. You can add, modify, and remove rules.

Explicit inclusion

To examine the behavior of membership rules based on explicit inclusion, perform the following steps with the Active Roles console.

To examine explicit inclusion

1. Open the **Properties** dialog box for your dynamic group, and go to the **Members** tab: the objects you explicitly included in the group are in the membership list.
2. Close the **Properties** dialog box.
3. Rename, modify, or move objects you selected for the explicit inclusion.
4. Open the **Properties** dialog box for your dynamic group, and go to the **Members** tab: the objects remain in the group membership list; for the objects you renamed, the list displays new names.

Explicit inclusion adds objects by object ID that remains unchanged during the entire object lifecycle. Once added through explicit inclusion, an object can only be removed from a dynamic group in one of these ways:

- Delete the membership rule for explicit inclusion of that object.
- Add the membership rule for explicit exclusion of that object.

To add or remove membership rules, you can use the **Membership Rules** tab in the **Properties** dialog box for the dynamic group.

Explicit exclusion

To examine the behavior of membership rules based on explicit exclusion, perform the following steps using the Active Roles console. These instructions assume that you have chosen the Administrator account for explicit exclusion from your dynamic group.

To examine explicit exclusion

1. Open the **Properties** dialog box for **Domain Admins** group and go to the **Members** tab to check that Administrator is a member of the Domain Admins group. Close the **Properties** dialog box.
2. Open the **Properties** dialog box for your dynamic group, go to the **Membership Rules** tab, and add the explicit inclusion rule that makes Administrator a member of your dynamic group.
3. Apply your changes by clicking **Apply** in the **Properties** dialog box for your dynamic group.
4. Go to the **Members** tab, click the **Rebuild** button and note that Administrator is not a member of your dynamic group although each of the following rules adds Administrator to the group:
    - Explicit inclusion rule (you configured it in Step 2).
    - Query-based inclusion rule (Administrator's name begins with the letter **a**).
    - Group membership inclusion rule (Administrator is a member of the group Domain Admins).

Explicit exclusion removes objects by object ID that remains unchanged during the entire object lifecycle. Once removed through explicit exclusion, an object can only be added to the dynamic group after deleting the Exclude Explicitly membership rule for that object.

Inclusion by query

To examine the behavior of query-based inclusion rules, perform the following steps using the Active Roles console. These instructions assume that your query-based rule is configured so that the group includes all users whose names begin with the letter **a**.

To examine inclusion by query

1. In any OU in your test domain, create a new user account with a full name that begins with the letter **a**.
2. Open the **Properties** dialog box for your dynamic group, and go to the **Members** tab: the new user account is in the membership list (unless it is removed from the dynamic group by exclusion rules).
3. Rename an existing user account so that its new full name begins with the letter **a**.
4. Go to the **Members** tab in the **Properties** dialog box for your dynamic group, and click the **Rebuild** button: the user account is added to the membership list (unless it is removed from the dynamic group by exclusion rules).
5. Rename the user account you managed in Step 4 so that its new full name begins with the letter **b**.
6. Go to the **Members** tab in the **Properties** dialog box for your dynamic group, and click the **Rebuild** button: the user account is removed from the membership list (unless it is added to the dynamic group by explicit inclusion rules).

Inclusion of group members

To examine the behavior of membership rules based on group membership, perform the following steps using the Active Roles console. These instructions assume that you have configured your dynamic group to include the members of the group Domain Admins.

To examine inclusion of group members

1. Open the **Properties** dialog box for your dynamic group, and go to the **Members** tab: the members of the Domain Admins group are in the membership list (except those removed from the dynamic group by exclusion rules).
2. Add a member to the Domain Admins group.
3. Go to the **Members** tab in the **Properties** dialog box for your dynamic group, and click the **Rebuild** button: the new member of the Domain Admins group is added to your dynamic group (unless that member is removed from the dynamic group by exclusion rules).

4. Remove a member from the Domain Admins group.
5. Go to the **Members** tab in the **Properties** dialog box for your dynamic group, and click the **Rebuild** button: the object you removed from the Domain Admins group is also removed from your dynamic group (unless that object is added to the dynamic group by explicit inclusion rules).

Enforcement of membership rules

When changes are made to the membership list of a dynamic group, Active Roles detects the changes regardless of their origin, and reapplies membership rules. This ensures that the group membership list is in compliance with the rules even if it was modified by using an administrative tool other than Active Roles. For example, you can use the Active Directory Users and Computers tool to make changes to the membership list of a dynamic group, and see how Active Roles reapplies membership rules.

Perform the following steps in the Active Directory Users and Computers.

To examine enforcement of membership rules

1. Open the Active Directory Users and Computers tool (run **dsa.msc** from a command prompt).
2. In any OU in your test domain, create a user account with a full name that begins with the letter **a**.
3. Open the **Properties** dialog box for your dynamic group, and go to the **Members** tab: the new user is in the group membership list.
4. On the **Members** tab, select that user, and click **Remove**. Click **Yes**. Click **OK**.
5. Open the **Properties** dialog box for your dynamic group, and go to the **Members** tab: the user is still in the group membership list.

   Active Roles has detected the removal, and added the user to the group in accordance with the membership rules.

10

Delegating computer resource management

Active Roles provides the capability to delegate administration of computer resources, such as network shares, services, and logical printers. It is also possible to delegate administration of local users and groups on member servers and workstations. Delegated administrators can use the Active Roles Web Interface to manage computer resource.

Active Roles comes with a suite of Access Templates that facilitate the delegation of computer management tasks. When applied to an OU, Access Templates from that suite provide for the following levels of access to the computers placed in that OU:

- **Full Control** Perform all management tasks on computer resources.
- **Local Account Operator** Create, modify, and delete local user accounts and groups.
- **Network Share Operator** Create, modify, and delete network shares.
- **Print Operator** View and modify properties of logical printers; manage print jobs.
- **Service Operator** Start/stop services; view/modify service properties.
- **Server Operator** Start/stop services; create, modify, and delete network shares; pause/resume/cancel printing; view properties of all computer resources.

This section outlines the procedure you can use to assign the **Server Operator** role to a delegated administrator for an OU, and briefly describes how to perform computer management tasks using the Active Roles Web Interface for Administrators.

Assign the Server Operator role for an OU

When you assign the Server Operator role to a group for a given OU, you authorize the members of that group to perform all management tasks on the services, network shares, and logical printers on any computer in that OU and its child OUs.

You can assign the Server Operator role using the Active Roles console as follows.

To assign the Server Operator role for OU

1. In the Active Roles console, right-click the OU and then click **Delegate Control**.
2. In the **Active Roles Security** window, click **Add**.
3. Follow the steps in the Delegation of Control wizard.
4. On the **Users or Groups** page, click **Add**.
5. Select the group you want to designate as the delegated administrator and click **OK**.
6. Click **Next**.
7. On the **Access Templates** page, expand **Computer Resources**, select the check box next to **Computer Management - Server Operator**, and then click **Next**.
8. Click **Next** two times, and then click **Finish**.

To enable the delegated administrators to browse OUs in the domain, you must grant them the **Read All Properties** permission on the OU objects at the domain level.

To grant the Read All Properties permission

1. Select the domain and use the Delegation of Control wizard as described in the previous procedure.
2. On the **Access Templates** page, expand **Active Directory**, and select the check box next to **OUs – Read All Properties**.

Test the delegated administrator's rights

The delegated administrator can use the Active Roles Web Interface for Administrators to perform management tasks on computer resources. Take the following steps to verify the administrator's rights.

To verify the delegated administrator's rights

1. Log on to your computer with the delegated administrator's user name and password.
2. Connect to the Web Interface for Administrators: Open your Web browser and navigate to http://localhost/ARWebAdmin.
3. In the Search box on the header of the Web Interface page, type the name of the OU for which the delegated administrator is assigned the Server Operator role, and then press Enter.
4. In the list of search results, click the name of the OU to displays a list of computers held in that OU.
5. In the list of computers, click select the check box next to the name of a computer.

6. In the right pane of the Web Interface page, click **Manage** to view a list of resource categories.
7. Verify that you can start and stop services on the selected computer:
    a. In the list of resource categories, click **Services** to view a list of services installed on the selected computer.
    b. To start a stopped service, select the check box next to the name of that service, and then click **Start** in the right pane.
    c. To stop a started service, select the check box next to the name of that service, and then click **Start** in the right pane.
8. Return to the list of resource categories: In the breadcrumb navigation control above the list of services, click the name of the computer, and then, in the right pane of the Web Interface page, click **Manage**.
9. Verify that you have full control of network shares on the selected computer:
    a. In the list of resource categories, click **Shares** to view a list of network file shares defined on the selected computer.
    b. To create a new share, click **New Share** in the right pane of the Web Interface page.
    c. To manage an existing share, select the check box next to the name of that share and use commands in the upper area of the right pane:
        - Click **Properties** to view or change the properties and security settings of the selected share.
        - Click the **Stop Sharing** command to remove the selected share.
10. Return to the list of resource categories: In the breadcrumb navigation control above the list of services, click the name of the computer, and then, in the right pane of the Web Interface page, click **Manage**.
11. Verify that you can view or change printer properties as well as pause, resume, and cancel printing of documents on a given printer:
    a. In the list of resource categories, click **Printers** to view a list of printers installed on the selected computer.
    b. In the list of printers, select the check box next to the name of a printer and then click commands in the right pane of the Web Interface page to perform the following tasks:
        - Click **Properties** to view or change the properties of the selected printer.
        - Click **Pause** to suspend printing of all documents on the printer. This will replace **Pause** with **Resume**.
        - To continue printing, click **Resume**.
        - Click **Cancel All Documents** to cancel printing of all documents on the printer.

- Click **Print Jobs** to view a list of documents being printed. You can select a document from the list, and then use command in the right pane to pause, resume, restart, or cancel printing of that document.

Using audit trail and reporting

This section describes how to view the Active Roles audit trail and how to work with Active Roles reports.

Analyze the Audit Trail

Active Roles provides a complete audit trail, showing who performed what actions and who tried to perform actions that were not permitted, and offers a rich suite of reports based on the audit trail.

Active Roles creates the audit trail by generating events and recording them into the **Active Roles Admin Service** event log. You can use Event Viewer to examine events in that log, or you can use Active Roles reports to perform an in-depth analysis of the audit trail.

Examine the audit trail using event viewer

To view details about an Active Roles event

1. On the computer running the Active Roles Administration Service, open Event Viewer.
2. In the console tree, under **Application and Services Logs**, select the **Active Roles Admin Service** log.
3. In the details pane, right-click an event, and then click **Event Properties**.

Use reports to analyze the audit trail

The Work with Active Roles reports section later in this document provides information on how to use reporting in Active Roles. The many reports you can prepare include special reports that are based on the Active Roles audit trail. Some examples are as follows.

Work with Active Roles reports

Active Roles comes with a rich suite of reports—Active Roles Report Pack. Active Roles reports cover all administrative actions that can be taken with this product. To create and view reports, you must install Active Roles Collector and Active Roles Report Pack. If you install Active Roles as described in the section Installing the reporting components earlier in this document, you have installed all components required to work with Active Roles reports.

Collect data for reporting

To prepare reports, you first need to collect data for reporting.

To collect data for reporting

1. Open the Active Roles Collector wizard by selecting **Active Roles Active Roles Collector** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.
2. On the **Welcome** page, click **Next**.
3. On the **Select Task** page, select the option **Collect data from the network**. Click **Next**.
4. Click **Browse** and complete the SQL Server Connection wizard as follows.

   You only need to complete the SQL Server Connection wizard once, when using the Collector wizard for the first time.
5. On the **SQL Server** page, click **Use SQL Server authentication**, and set the other options as follows:
   a. In the **Server** box, enter <*ServerName*>\sqlexpress, replacing <*ServerName*> with the name of the computer on which you installed SQL Server Express.
   b. In the **Logon Name** box, type **sa.**
   c. In the **Password** box, type the password for the **sa** login.
6. Click **Next**.
7. On the **Select database** page, in the **Database** box, type **ARServerReporting**.

   The wizard will create a database with the name you specify. It is advisable to create a new database rather than select an existing database. If you select an existing database, the data in that database may be corrupted during the data collection process.
8. In the **Configure Data Source** dialog box, review the settings you have specified, and then click **OK**.

9. In the **Active Roles Service** box, type the name of the computer running the Administration Service.
10. Select the **Current User** option (assuming that you are logged on as an administrator of that computer).
11. Click **Next**.
12. On the **Data Collection Tasks** page, in the **Collect** box, select all check boxes. Click **Next**.
13. On the **Data to Collect** page, in the **Collect** box, select all check boxes. Click **Next**.
14. On the **Select Domains or OUs** page, click **Add** and select your test domain. Click **Next**.
15. On the **Select Operation Mode** page, select the **Now** option. Click **Next**.
16. Wait while the wizard collects data for reporting.
17. Click **Finish** to close the wizard.

Generate and view reports

After the data for reporting is collected, you need to configure the data source for the Active Roles Report Pack to connect to the database where you have collected data for reporting.

To configure the data source

1. Start SSRS Report Manager from your Web browser.

   Report Manager is installed during setup of SQL Server Reporting Services (SSRS) on the same computer as the report server. To start Report Manager, open Internet Explorer, and then, in the address bar of the Web browser, type the Report Manager URL. By default, the URL is http://<*ComputerName*>/reports.

2. Perform the following steps on the Contents page that appears:
   a. Click **Details View**.
   b. Click **Active Roles**.
   c. Click **SharedDataSources**.
   d. Click the data source named **Active Roles 7.2 Report Data**.
3. In the **Connection string** box on the **Properties** page that appears, specify the SQL Server instance and the name of the database that holds the report data prepared by the Active Roles Collector.

   For example, if the name of the database is ARServerReporting and the database is on the SQL Server instance named MyServer\sqlexpress, then the connection string is as follows:

   ```
   data source = MyServer\sqlexpress initial catalog = ARServerReporting
   ```

4. Click **Apply**.

Once you have configured the data source, you can use Report Manager to generate and view reports.

To generate and view reports

1. In Report Manager, at the top of the window, click **Active Roles**.
2. Perform the following steps on the Contents page that appears:
    a. Click **7.2**.
    b. Click the folder containing a report you want to prepare.
    c. Click the name of the report.
3. Wait while the Report Manager generates the report.

Using Active Roles replication

Active Roles uses the replication functionality of Microsoft SQL Server to copy and distribute configuration data from one Administration Service database to another, and to synchronize between configuration databases for consistency.

Administration Service database servers synchronized by using the SQL Server replication function are referred to as *replication partners*. Each replication partner hosts a writable copy of the Active Roles configuration data. Whenever changes are made on one replication partner, the changes are propagated to the other replication partners.

This section outlines the procedures to follow in order for you to configure replication and see how replication works in Active Roles. To use these procedures, you must install Active Roles on two network computers, as described in the Test lab setup section earlier in this document. Two Active Roles instances will be configured to replicate configuration data with each other.

NOTE:

- Due to limited replication-related capabilities of SQL Server Express (may hold only the Subscriber role), the scenario discussed in this section requires a different edition of SQL Server (such as Enterprise, Standard, or Workgroup) to be used as the Publisher role holder.
- For the purposes of this evaluation scenario, you may use the same SQL Server to host the databases for both the Administration Services participating in the scenario.
- When installing the second Administration Service, specify a database name that is different from the name of the database used by the first Administration Service. This ensures that each Administration Service uses a separate database, so two databases could be synchronized with each other via replication of data.

Configure replication

When configuring Active Roles replication, you first create a replication group by designating the database server of a particular Administration Service as the Publisher.

When planning to assign the Publisher role to the database server of a certain Administration Service, ensure that the following requirements are met:

- The SQL Server Agent service is started on SQL Server that hosts the database of that Administration Service, and configured to log on as a domain user account with administrator rights on SQL Server.
- The Administration Service is configured to log on as a domain user account with administrator rights on SQL Server.

For evaluation purposes, you may configure both the SQL Server Agent service and the Administration Service to log on as a user account that belongs to the Domain Admins group of your test domain.

To assign the Publisher role to the database server of a certain Administration Service, perform the following steps using the Active Roles console.

To create the Publisher

1. Open the Active Roles console and connect to the Administration Service whose database server you want to designate as the Publisher.
2. In the console tree, expand **Configuration**, expand **Server Configuration**, and then select **Configuration Databases**.
3. In the details pane, right-click the database server and click **Promote**.
4. In the confirmation message box, click **Yes**.
5. Wait while Active Roles completes the operation.

The new replication group now has a single member—the Publisher. You can add replication partners—Subscribers. To add a Subscriber, perform the following steps using the Active Roles console.

To add a Subscriber

1. Open the Active Roles console and connect to the Administration Server whose database server you have designated as the Publisher.
2. In the console tree, expand **Configuration**, expand **Server Configuration**, and then select **Configuration Databases**.
3. In the details pane, right-click the Publisher, and then click **Add Replication Partner**.
4. Follow the instructions in the New Replication Partner wizard.
5. On the **Database Selection** page, click **Browse**.
6. Use the **Connect to Administration Service** dialog box to specify the Administration Service whose database server you want to add to the replication group. Click **OK**.
7. Click **Next** two times, and then click **Finish**.

Test replication

To see how replication works, create a Managed Unit on one of the Administration Services you have configured to be replication partners. Then, connect to the other Administration Service and verify that the new Managed Unit has been replicated to that Service.

To create a Managed Unit

1. Open the Active Roles console and connect to one of the Administration Services.
2. In the console tree, expand **Configuration**, right-click **Managed Units**, and select **New | Managed Unit**.
3. Complete the New Object - Managed Unit wizard.

Wait a few minutes and then use the Active Roles console to verify that the new Managed Unit is also created on the other Administration Service.

To verify replication of the Managed Unit

1. Open the Active Roles console and connect to the other Administration Service.
2. In the console tree, expand **Configuration**, and click **Managed Units**: the newly created Managed Unit appears in the details pane.

You can create, modify, or delete Active Roles configuration objects, such as Managed Units, Access Templates or Policy Objects, on one of the replication partners, regardless of whether it is the Publisher or a Subscriber, and then connect to other replication partners and see that your changes are propagated to all replication partners.

NOTE: Although Active Roles replication is configured to initiate the propagation of changes immediately after the changes are made, it may take a few minutes for SQL Server to propagate the changes between the Publisher and Subscribers.

Customizing the Web Interface

The Active Roles Web Interface allows you to customize menus, commands, and forms used to administer directory objects. You can add and remove commands or entire menus, assign tasks and forms to commands, modify existing forms, and create new commands, tasks, and forms.

To use the customization capabilities of the Web Interface, you must be logged on as Active Roles Admin. If you have used the default settings when installing the Administration Service, the Active Roles Admin account is set to the Administrators local group on the computer running the Administration Service. So, to customize the Web Interface in your test environment, log on with any user account that is a member of that group.

This section provides an example of how to customize the Site for Administrators. By default, the Web Interface pages for user account creation do not include the box where you could specify the user's telephone number. After you complete the following steps, a new field—**Telephone Number**—is added on the Web page for user account creation. When you fill in that field, the number is saved in the **telephoneNumber** property of the user account.

Add a text box to the user creation page

Perform the following steps to add the **Telephone number** field on the Web page for user creation.

To add the field to the form for user account creation

1. Connect to the Web Interface for Administrators: Open your Web browser and navigate to http://localhost/ARWebAdmin.
2. On the Web Interface Home page, click **Customization**.
3. On the Customization page that appears, click **Customization Tasks**.

   This displays a list of object types. Each object type is linked with a list of commands, referred to as a menu. When you manage an object in the Web Interface, the menu linked with the type of that object provides the commands to perform

management tasks. Since you want to customize the behavior of the user creation command, you should access the menu containing that command—the menu linked with the Container object type.

> NOTE: The **Customization** option is unavailable unless you are logged on as Active Roles Admin.

4. In the list of object types, click **Container**.
5. In the list of commands, click **New User**.
6. In the right pane of the Web Interface page, click **Edit Form**.

   This opens the form in the Form Editor. The Form Editor provides you with a central place to add, remove, or modify tabs and entries, as well as to change the order of tabs and entries on the form.

   In the Web Interface, the user creation task is divided into a series of steps. Therefore the form includes several tabs, with each tab being used to perform a particular step. You are going to add a field to the **General** tab.
7. On the toolbar in the Form Editor, point to **Add Entry** and click **Create**.

   This displays a list of properties. You can select the property you want to manage by using the new entry.
8. In the list of properties, click **Telephone Number**. Click **Next**.

   This displays the page where you can set the name of the entry. The entry name is used to label the field on the form.
9. Specify **Telephone number** as the entry name, and click **Finish**.

   This displays the entries disposed on the **General** tab. The tab now includes the **Telephone number** entry. For these changes to take effect, they must be saved, and then the Web Interface configuration data must be reloaded.
10. Click **Save**, and then click **Reload** on the message bar that appears at the top of the Form Editor page.

> NOTE: You can undo the changes you have made: In the leftmost pane of the Web Interface page, click to expand the **Customization** item, and then click **Restore Default**.

Test the user creation page

After you complete the steps in the previous section, you can use the Web Interface for Administrators to verify that the new field is added to the user creation page.

To verify the configuration of the user creation page

1. Go to the Web Interface Home page.
2. In the **Search** box on the header of the Web Interface page, type the name of the OU where you want to create the user, and then press **Enter**.
3. In the list of search results, click the name of the OU.
4. In the right pane of the Web Interface page, click **New User**.
5. Review the New User wizard: The **General** page now includes the **Telephone Number** field.

NOTE: You can also use the Customize link to add and remove user interface elements from the form. This link is equivalent to the command **Edit Form**.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product