Active Roles 8.2.1

Console User Guide

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

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

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

Refer to our website (http://www.OneIdentity.com) for regional and international office information.

Patents

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

Trademarks

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

Legend

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

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

Active Roles Console User Guide
Updated - 28 November 2024, 10:28

For the most recent documents and product information, see Online product documentation.

Contents

1

Introduction

Active Roles is an administrative platform that facilitates administration and provisioning for Active Directory and Microsoft Exchange. Active Roles enables the organization to develop a flexible administrative structure that suits their needs, while ensuring secure delegation of tasks, reduced workloads, and lower costs.

Active Roles increases the productivity of system administrators and helpdesk operators by automating provisioning tasks on directory objects in compliance with corporate administrative policies in corporate Active Directory and Exchange environments. The policy enforcement featured in the product guarantees that every administrative action taken is consistent with corporate security standards, which is a top priority for most organizations.

The Active Roles Console User Guide is designed for individuals responsible for performing administrative tasks using the Active Roles Console (MMC Interface). This document provides information about the Active Roles Console user interface, and includes instructions to help delegated administrators and helpdesk operators perform day-to-day administrative activities.

The Active Roles Console User Guide is supplemented with the Active Roles Administration Guide that provides conceptual information about the product, and includes systematic instructions on how to deploy the Active Roles administrative structure.

2

Getting started

This section provides an overview on how to start using the Active Roles Console for day-to-day administration operations by describing:

- How to start the Active Roles Console.
- The main use cases of administering resources in Active Roles, such as using Managed Units, configuring filters, finding objects, and looking for policy-related information.

> NOTE: For a description of the Active Roles Console user interface, see *Active Roles Console* in the *Active Roles Feature Guide*.

Starting the Active Roles Console

The Active Roles Console, also referred to as MMC Interface, is a comprehensive administrative tool that you can use to:

- Manage Active Directory and Microsoft Exchange resources.
- Work with approval workflows in effect in your organization.

With the Active Roles Console, you can easily find directory objects and perform administrative tasks.

To start the Active Roles Console

1. Log in to the system where Active RolesConsole is installed.
2. Depending on the version of your operating system:
    - In the **Apps** page, click **Active Roles 8.2.1 Console**.
    - From the **Start** menu, select **All Programs** > **One Identity Active Roles 8.2.1** > **Active Roles 8.2.1 Console**.

> NOTE: By default, the Active Roles Console automatically chooses an Administration Service instance and establishes a connection. If the Console cannot connect to the Administration Service or you want to manually select the Administration Service, see *Connecting to the Administration Service* in the *Active Roles Administration Guide*.

Sorting and filtering lists

To help you find directory objects quicker and easier, Active Roles Console supports filtering directory objects.

If you set up a filter, the filtering criteria immediately take effect on all directory object lists.

To sort objects in the details pane

1. Click a column heading to sort by the contents of that column.
2. Click the column heading again to switch between ascending and descending sort order.

To add or remove columns in the details pane

1. On the **View** menu, click **Choose Columns** or **Add/Remove Columns**.
2. Do the following, then click **OK**:
   - To add a column, in **Available columns**, click the column you want to display, then click **Add**.
   - To remove a column, in **Displayed columns**, click the column you want to hide, then click **Remove**.
   - To re-order columns, click a column name in **Displayed columns**, then click **Move Up** or **Move Down** to change the position of the column.

> NOTE: In the **Advanced Details Pane**, you can add or remove columns from a list in the upper sub-pane or in the lower sub-pane. To do so, click the list in the sub-pane you want to modify, then follow the steps above.

Filter options help you search for particular objects in the details pane. You can view all objects or only objects of selected type, configure the number of items that can be displayed for each folder, or create custom filters using object attributes and LDAP queries.

To select view filter options

1. On the **View** menu, click **Filter Options**.
2. Do one of the following, then click **OK**:
   - To view all objects, click **Show all types of objects**. With this option, the filter is turned off.
   - To view objects of certain types, click **Show only the following types of objects**, and select check boxes next to the types of objects you want to view.
   - To view objects that match custom filtering criteria, click **Create custom filter**. Then click **Customize**, and configure your filtering criteria by using the instructions outlined in Building a custom search.
3. (Optional) In **Maximum number of items displayed per folder**, modify the

maximum number of objects that can be displayed in the Console. The default maximum number of objects displayed in the Console is 2,000.

Finding directory objects

In the Active Roles Console you can search for objects of different types using the **Find** window. To access the **Find** window, right-click a container and click **Find**.

Searching for a user, contact, or group

You can search for Active Directory user accounts, contacts or groups with the Active Roles Console.

To search for a user, contact, or group

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click one of the following:
    - **Users, Contacts, and Groups**: Use this option to find users, groups, and contacts that match your search criteria.
    - **Users**: Use this option to find only users that match your search criteria.
    - **Groups**: Use this option to find only groups that match your search criteria.
    - **Contacts**: Use this option to find only contacts that match your search criteria.
3. In the **In** box, select the domain, container or Managed Unit you want to search, or click **Browse** to locate a domain, container or Managed Unit.
4. Type in a name, a description, or both:
    - In the **Name** box, type the name of the object you want to find.
    - In the **Description** box, type the description of the object you want to find.

    > TIP: You can search using partial search criteria. For example, **B** in the **Name** box will return all objects whose name begins with the letter **B**, such as **Backup Operators**.
5. To start your search, click **Find Now**.

> NOTE: Consider the following when searching for a user, contact, or group:
>
> - You can use the **Advanced** tab for more powerful search options. For details, see Using advanced search options.
> - The found objects are displayed at the bottom of the **Find** window.
> - You can manage the found objects directly from the list in the **Find** window by right-clicking a list item, then using commands on the shortcut menu to perform management tasks.

Searching for a computer

To search for a computer

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click **Computers**.
3. In the **In** box, select the domain, container or Managed Unit you want to search, or click **Browse** to locate a domain, container or Managed Unit.
4. In the **Name** box, type the name of the computer you want to find.

   > TIP: You can search using partial search criteria. For example, **B** in the **Name** box will return all computers whose name begins with the letter B.

5. (Optional) In the **Role** box, click one of the following:
   - **Domain Controller**: Use this option to find only domain controllers.
   - **Workstations and Servers**: Use this option to find only workstations and servers (not domain controllers).
6. To start your search, click **Find Now**.

> NOTE: Consider the following when searching for a computer:
>
> - You can use the **Advanced** tab for more powerful search options. For details, see Using advanced search options.
> - The found objects are displayed at the bottom of the **Find** window.
> - You can manage the found objects directly from the list in the **Find** window by right-clicking a list item, then using commands on the shortcut menu to perform management tasks.

Searching for an Organizational Unit

You can search for Organizational Units (OUs) with the Active Roles Console.

To search for an Organizational Unit

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click **Organizational Units**.
3. In the **In** box, select the domain, container or Managed Unit you want to search, or click **Browse** to locate a domain, container or Managed Unit.
4. In the **Name** box, type the name (or a part of the name) of the OU you want to find.
5. To start your search, click **Find Now**.

> NOTE: Consider the following when searching for an OU:

- You can use the **Advanced** tab for more powerful search options. For details, see Using advanced search options.
- The found objects are displayed at the bottom of the **Find** window.
- You can manage the found objects directly from the list in the **Find** window by right-clicking a list item, then using commands on the shortcut menu to perform management tasks.

Displaying members of a Managed Unit

Members of a Managed Unit are objects that match the criteria specified in the membership rules for the Managed Unit. You can display and customize the list of members in the Active Roles Console.

To display the members of a Managed Unit

1. In the Active Roles Console, on the **Console tree**, navigate to **Configuration** > **Managed Units**.
2. Under **Managed Units**, locate and select the Managed Unit.

   The members of the Managed Unit are listed in the details pane.

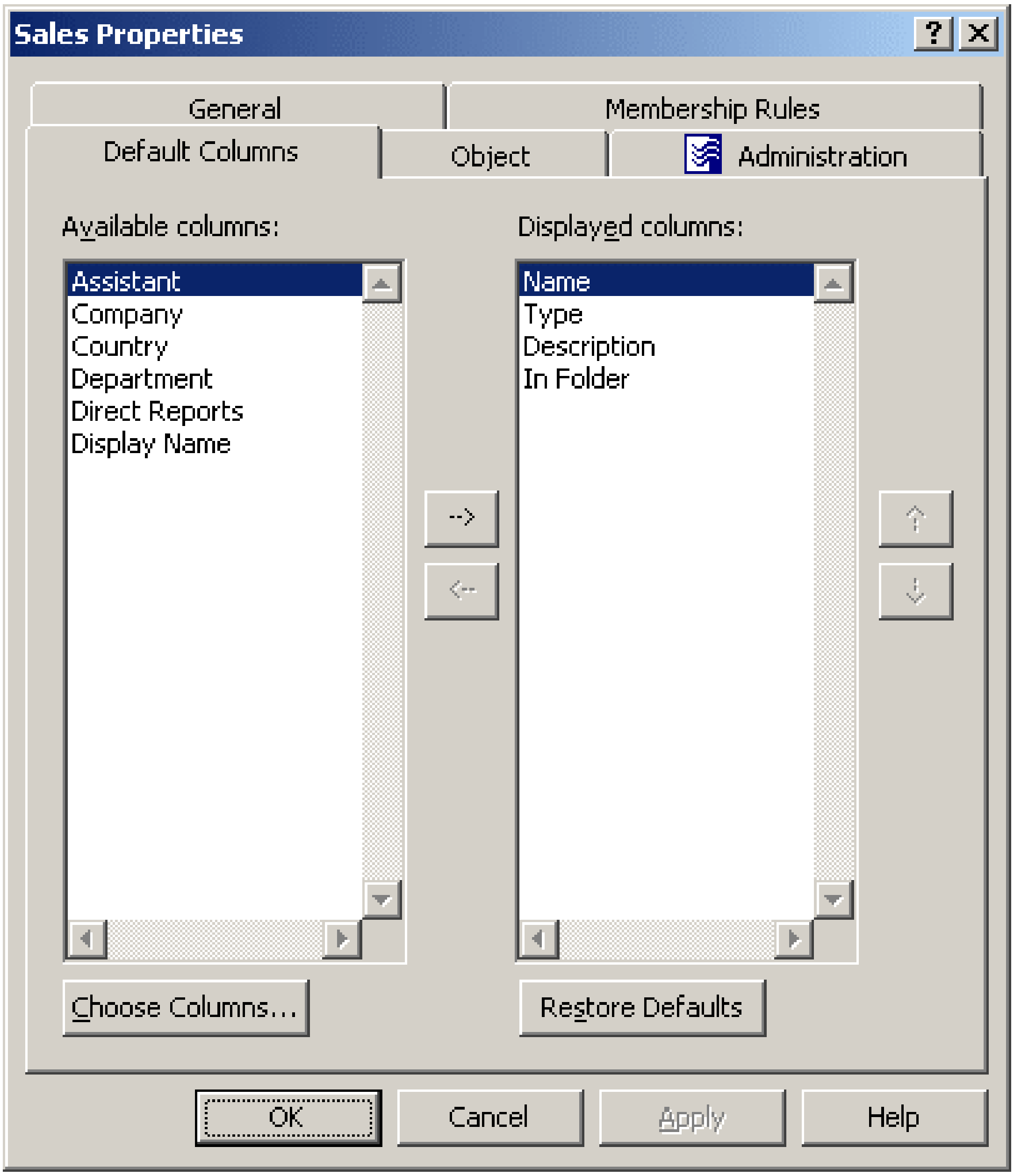
To customize the list of Managed Unit members in the details pane

1. Right-click the Managed Unit, and click **Properties**.
2. In the **Properties** dialog, click the **Default Columns** tab.
3. On the **Default Columns** tab, add or remove column names from the **Displayed Columns** list.
4. Click **OK**.

NOTE: Consider the following when displaying members of a Managed Unit:

- For each Managed Unit, you can configure an individual list of the default columns to display in the details pane, so you can perform the customization on a per-Managed Unit basis.
- You can populate the **Displayed columns** list by double-clicking column names in the **Available columns** list on the **Default Columns** tab. You can remove columns by double-clicking column names in the **Displayed columns** list.
- To add column items to the **Available Columns** list, click **Choose Columns**. In the **Choose Columns** dialog, you can select columns and, if necessary, modify column names.
- For your changes to the **Displayed columns** list to take effect, the details pane must be refreshed. To do so, right-click **Managed Units** in the **Console tree** and click **Refresh**.

Figure 1: Managed Unit - Preset columns



Available columns:

- Assistant
- Company
- Country
- Department
- Direct Reports
- Display Name

Displayed columns:

- Name
- Type
- Description
- In Folder

Using advanced search options

To fine-tune search results, the Active Roles Console allows you to perform advanced search on the Active Directory resources available in your organization.

To use advanced search options

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click the kind of object for which you want to search.
3. Click the **Advanced** tab.
4. Click **Field**, and select the object property you want to query.
5. In **Condition**, to find the objects that have the object property matching the condition-value pair you have specified, click the condition for your search, then, in **Value**, type a property value.
6. To add this search condition to your search, click **Add**.
7. Repeat the steps from selecting the object property you want to query until you have added all of the desired search conditions.
8. Click one of the following:
   - If you want to find the objects that meet all of the conditions specified, click **AND**.
   - If you want to find the objects that meet any of the conditions specified, click **OR**.
9. To start your search, click **Find Now**. The found objects are displayed at the bottom of the window.

Building a custom search

You can configure custom search queries in the Active Roles Console.

To build a custom search

1. On the **Action** menu, click **Find** to display the **Find** window.
2. In the **Find** box, click **Custom Search**.
3. In the **In** box, select the domain, container or Managed Unit you want to search, or click **Browse** to locate a domain, container or Managed Unit.
4. Do one of the following:
   - On the **Custom Search** tab, follow the steps from selecting the object property you want to query of the procedure outlined in Using advanced search options.
   - On the **Advanced** tab, specify a search filter using LDAP syntax, as described in LDAP Syntax.
5. To start your search, click **Find Now**.

LDAP Syntax

Search filters enable you to define search criteria and provide more efficient and effective searches. The search filters are represented by Unicode strings.

The Active Roles Console supports the standard LDAP search filters as defined in RFC 2254.

The following table lists some examples of standard LDAP search filters.

Table 1: LDAP search filters

Search filter	Description
`(objectClass=*)`	All objects
`(&(objectCategory=person)(objectClass=user)(!cn=andy))`	All user objects but `andy`
`(sn=sm*)`	All objects with a surname that starts with `sm`
`(&(objectCategory=person)(objectClass=contact)(|(sn=Smith)(sn=Johnson)))`	All contacts with a surname equal to `Smith` or `Johnson`

Search filter format

Search filters use one of the following formats:

- `<filter>=(<attribute><operator><value>)`
- `(<operator><filter1><filter2>)`

In this example, `<attribute>` stands for the LDAP display name of the attribute by which you want to search.

Operators

The following table lists some frequently used search filter operators.

Table 2: Operators

Logical Operator	Description
=	Equal to
~=	Approximately equal to
<=	Lexicographically less than or equal to

Logical Operator	Description
>=	Lexicographically greater than or equal to
&	AND
|	OR
!	NOT

Wildcards

You can add wildcards and conditions to a search filter. The following examples show substrings that can be used to search the directory.

Substring	Description
`(objectClass=*)`	Get all entries
`(cn=*bob*)`	Get entries containing `bob` somewhere in the common name
`(cn>='bob')`	Get entries with a common name greater than or equal to `bob`
`(&(objectClass=user)(mail=*))`	Get all users with an email attribute
`(&(sn=smith)(objectClass=user)(mail=*))`	Get all user entries with an email attribute and a surname equal to `smith`
`(&(objectClass=user) | (cn=andy*)(cn=steve)(cn=margaret))`	Get all user entries with a common name that starts with `andy`, `steve`, or `margaret`
`(!(mail=*))`	Get all entries without an email attribute

Special characters

If any of the following special characters must appear in the search filter as literals, they must be replaced with the listed escape sequence.

Table 3: Special characters

ASCII Character	Escape Sequence Substitute
*	\2a
(	\28
)	\29

ASCII Character	Escape Sequence Substitute
`\`	`\5c`
NUL	`\00`

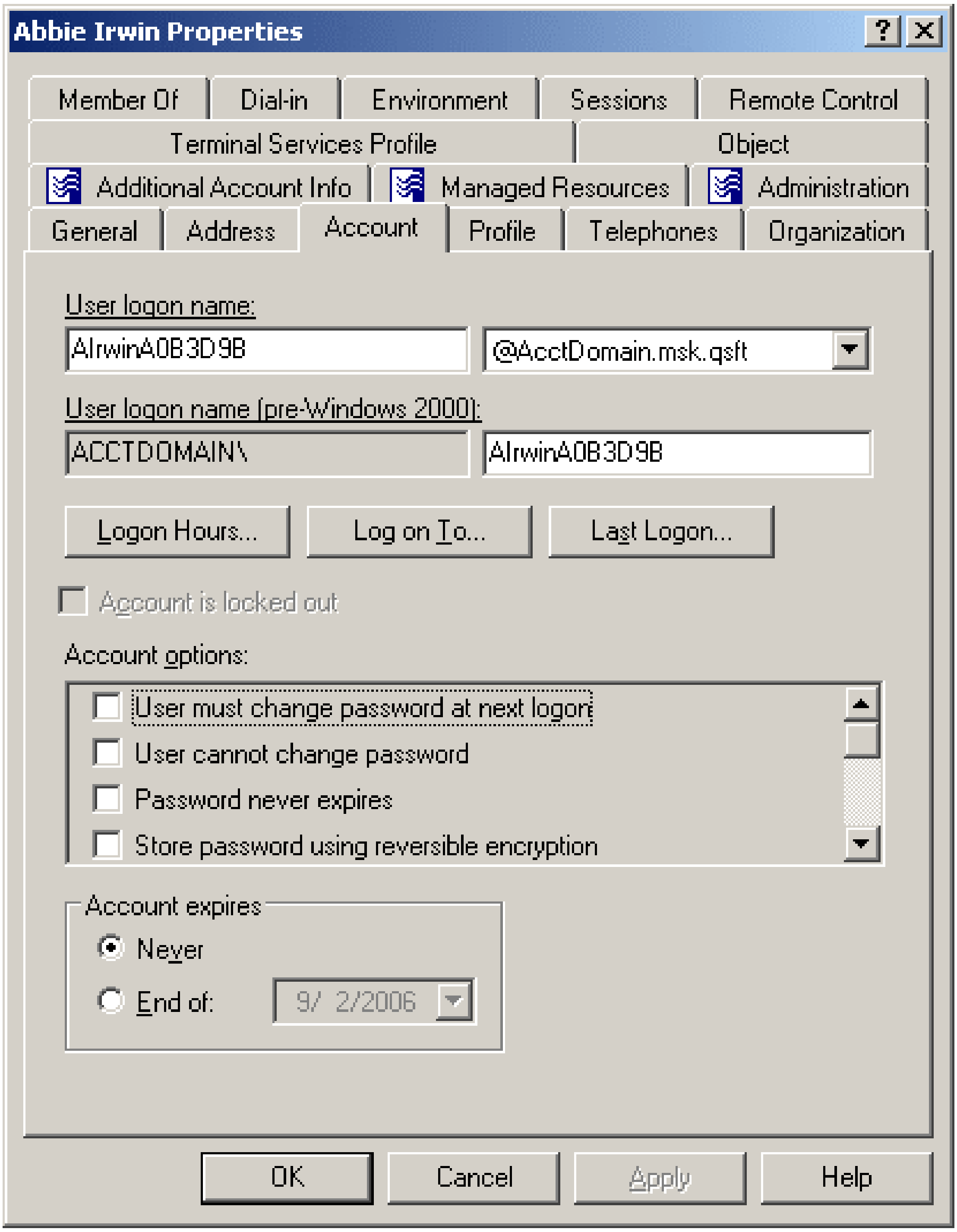
In addition, arbitrary binary data may be represented using the escape sequence syntax by encoding each byte of binary data with the backslash (\) followed by two hexadecimal digits. For example, the four-byte value `0x00000004` is encoded as `\00\00\00\04` in a filter string.

Getting policy-related information

In object creation wizards and properties dialogs, some property labels may be displayed as hyperlinks. This indicates that Active Roles enforces policy restrictions on the property.

In the following figure, the **User logon name** and **User logon name (pre-Windows 2000)** labels are underlined, which means that these properties are under the control of a certain policy defined with Active Roles.

Figure 2: Getting policy-related information



User logon name:
AIrwinA0B3D9B | @AcctDomain.msk.qsft

User logon name (pre-Windows 2000):
ACCTDOMAIN\ | AIrwinA0B3D9B

□ Account is locked out

Account options:

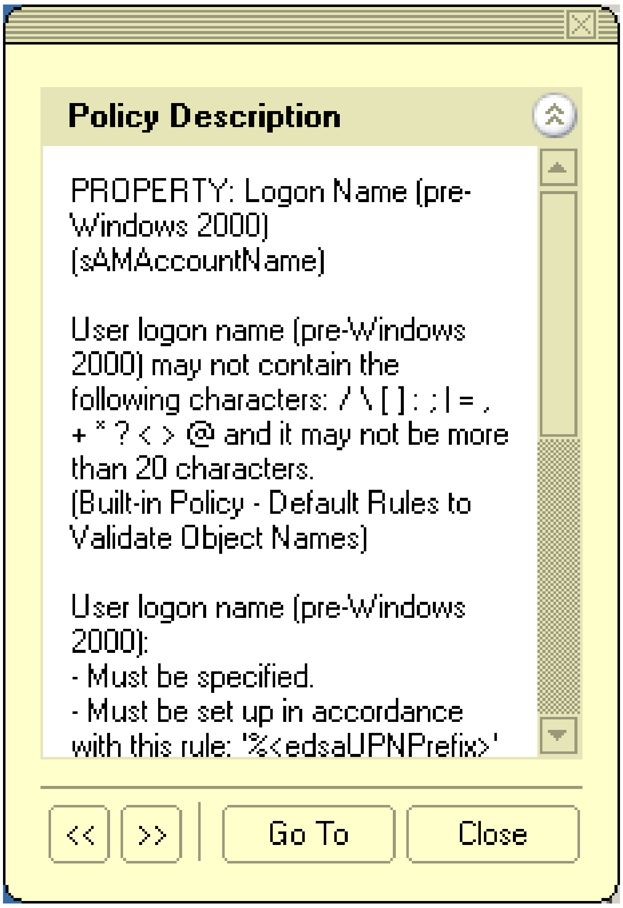
□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: 9/ 2/2006

To examine the policy in detail, click the label. For example, if you click **User logon name (pre-Windows 2000)**, the Active Roles Console presents you with a window similar to the following figure.

Figure 3: Policy description



Policy Description

PROPERTY: Logon Name (pre-Windows 2000) (sAMAccountName)

User logon name (pre-Windows 2000) may not contain the following characters: / \ [ ] : ; | = , + * ? < > @ and it may not be more than 20 characters.
(Built-in Policy - Default Rules to Validate Object Names)

User logon name (pre-Windows 2000):
- Must be specified.
- Must be set up in accordance with this rule: '%<edsaUPNPrefix>'

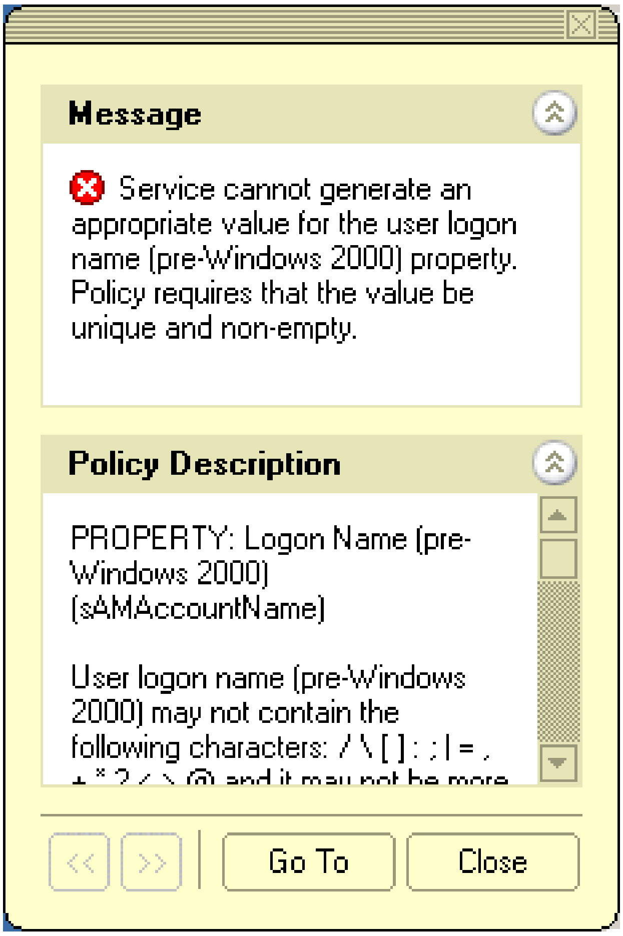
The window may display the following information:

- **Policy Description**: Provides a brief description of the policy.
- **Message**: Details the problem if the supplied property value violates the policy.

You can click arrows in the lower-left corner to display description of other policies enforced on the given property.

The **Message** section is displayed whenever the specified property value violates the policy. The following figure illustrates the situation where a value has not been supplied for a mandatory property.

Figure 4: Policy violation message



Message

Service cannot generate an appropriate value for the user logon name (pre-Windows 2000) property. Policy requires that the value be unique and non-empty.

Policy Description

PROPERTY: Logon Name (pre-Windows 2000) (sAMAccountName)

User logon name (pre-Windows 2000) may not contain the following characters: / \ [ ] : ; | = , + * ? < > @ and it may not be more

When you click **Go To** in this window, the Console moves the pointer to the field that needs to be corrected. You can type or select an appropriate value to correct your input.

3

User or service account management

Active Roles allows you to perform administrative tasks such as create, copy, rename, modify, and delete user accounts in Active Directory. You can also use this tool to unlock accounts, add and remove accounts from groups, and reset user passwords. Active Roles also supports Exchange tasks, such as create, delete, and move user mailboxes.

The following section guides you through the Active Roles Console to manage user accounts. You can also perform these tasks using the Active Roles Web Interface.

> NOTE: If your environment has a large number of Microsoft Exchange mailboxes (or a complex Microsoft Exchange deployment), Active Roles may retrieve the properties of users with Exchange mailboxes slower than for users without Exchange mailboxes.
>
> To solve this problem, enable a performance fix by creating a new registry key as described in Knowledge Base Article 4336544:
>
> 1. On the machine(s) running the Administration Service and the Web Interface, launch the Windows Registry Editor.
> 2. In the Registry Editor, navigate to the following registry path:
>
>   `HKEY_LOCAL_ MACHINE\SOFTWARE\One Identity\Active Roles\Configuration`
>
> 3. Create a new **DWORD (32-bit) Value** named `PerformanceFlag`.
> 4. Double-click the new **PerformanceFlag** DWORD, and set its **Value data** to `1`.
> 5. To apply the fix, restart the Active Roles Administration Service and IIS. If the fix is enabled successfully, the following Active Roles event log with Event ID 2508 will appear in the Event Viewer:
>
>    ```
>    Performance flag value set to 1.
>    ```
>
> 6. (Optional) To deactivate the fix later, set the **Value data** of the **PerformanceFlag** DWORD to 0.
>
> The **PerformanceFlag** registry key accepts only a value of `1` (to activate the fix) or `0` (to deactivate it).

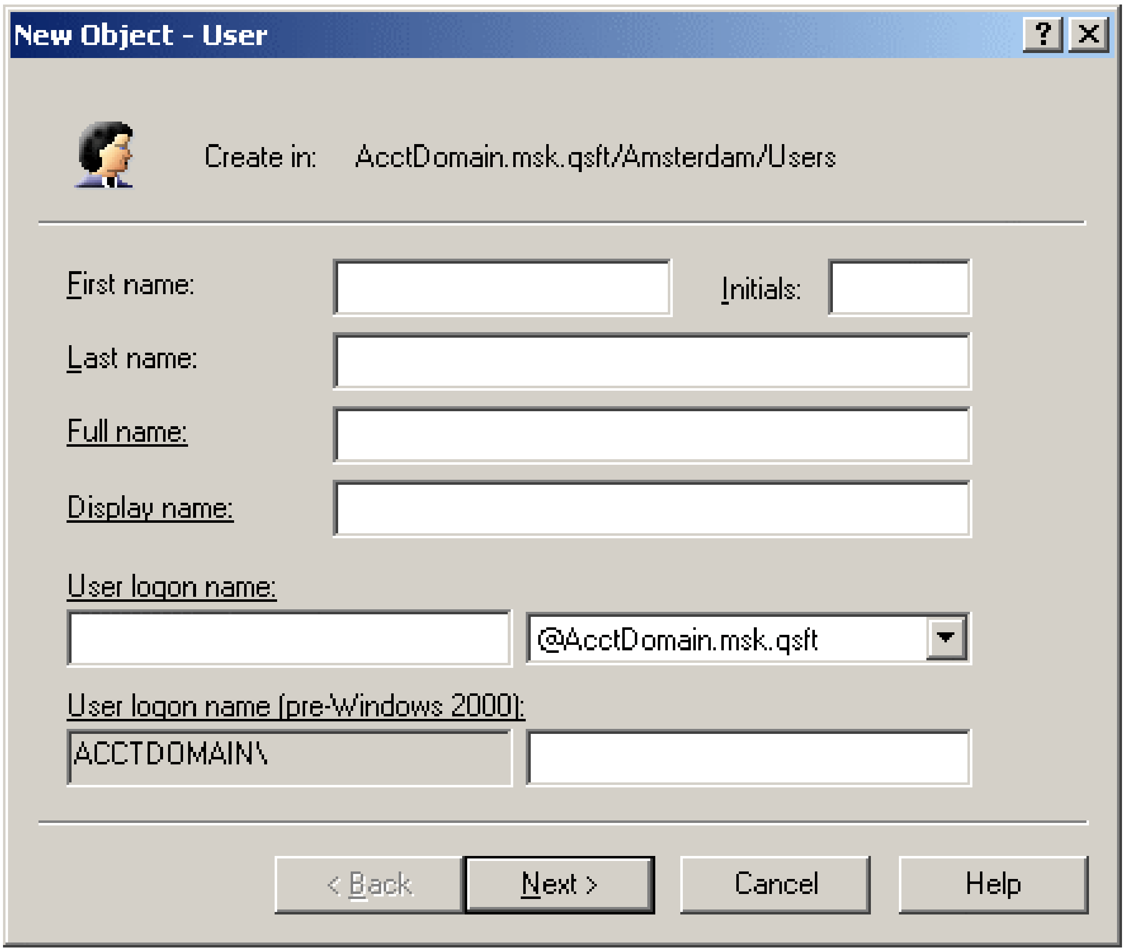
Creating a user account

You can create new Active Directory user accounts with the Active Roles Console.

To create a user account

1. In the **Console tree**, locate and select the folder in which you want to add the user account.
2. Right-click the folder, point to **New** and click **User** to start the **New Object - User** wizard.
3. Follow the wizard pages to specify properties of the new user account, such as the user first name, last name, full name, display name, logon name, pre-Windows 2000 logon name, password, and Exchange mailbox settings.

Figure 5: Creating a user account



New Object - User

Create in: AcctDomain.msk.qsft/Amsterdam/Users

First name:

Initials:

Last name:

Full name:

Display name:

User logon name:

@AcctDomain.msk.qsft

User logon name (pre-Windows 2000):

ACCTDOMAIN\

4. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the

wizard.

5. After setting any additional properties, click **Finish** on the completion page of the wizard.

> NOTE: Consider the following when creating a user account:
>
> - The behavior of the wizard pages may vary depending on the configuration of Active Roles policies. To determine whether a given item on a page is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the wizard pages. For more information, see Getting policy-related information.
>
>   The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.
> - You can start the **New Object - User** wizard by clicking on the toolbar.
> - To create a user account, you can also copy a previously created user account. For more information, see Copying a user account .
> - A new user account with the same name as a previously deleted user account does not automatically assume the permissions and group memberships of the previously deleted account because the security ID (SID) for each account is unique. To duplicate a deleted user account, you must manually reconfigure all of its permissions and memberships.

Finding a user account

To find a user account, right-click the container you want to search and click **Find**. In the **Find** window, select **Users** from the **Find** list, specify your search criteria, and start the search. In the search results list, you can right-click user accounts and use commands on the shortcut menu to perform management tasks.

For step-by-step instructions on how to search for user accounts, see Searching for a user, contact, or group.

Copying a user account

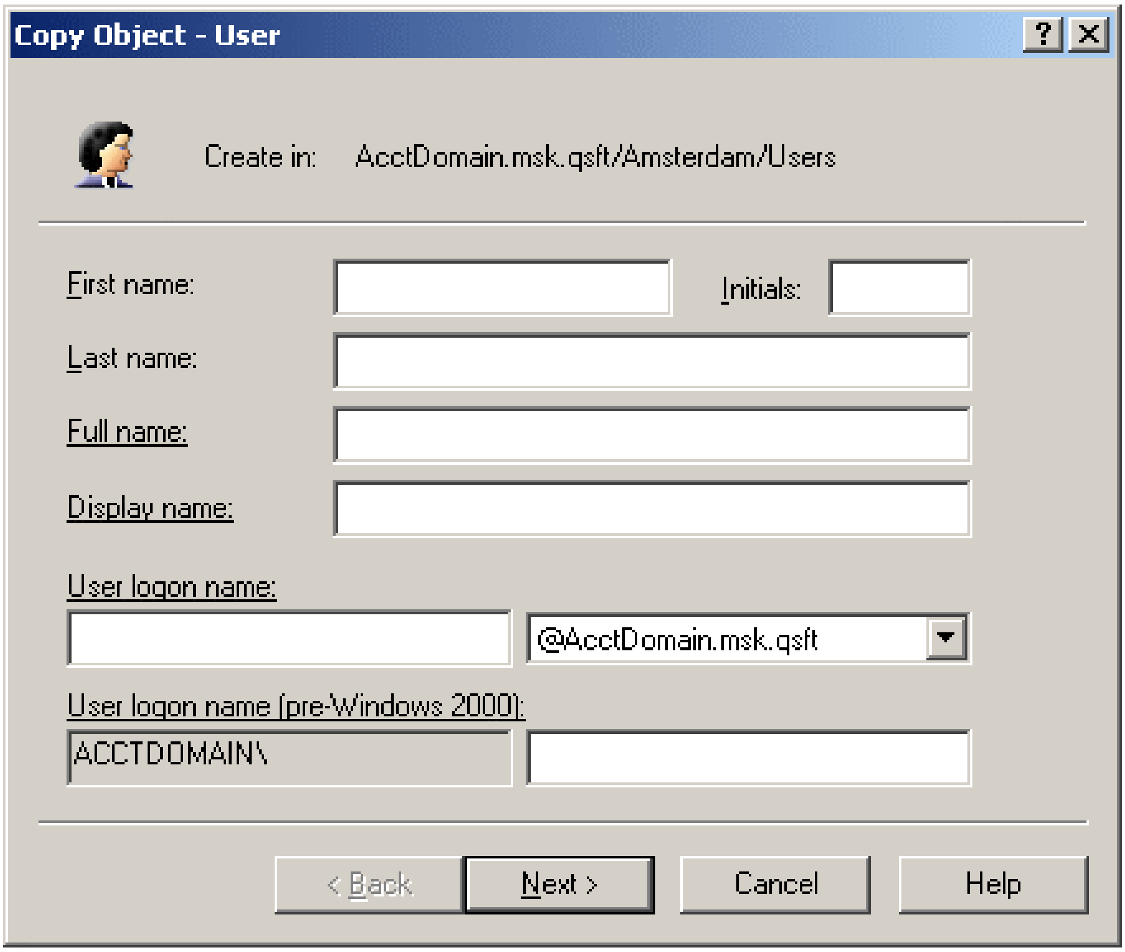
You can copy Active Directory user accounts with the Active Roles Console.

To copy a user account

1. In the **Console tree**, locate and select the folder that contains the user account you want to copy.

2. In the details pane, right-click the user account you want to copy, then click **Copy** to start the **Copy Object - User** wizard.
3. Follow the wizard pages to specify properties for the copy of the user account, such as the user first name, last name, full name, display name, login name, pre-Windows 2000 login name, password, and Exchange mailbox settings.

Figure 6: Copying a user account



Copy Object - User

Create in: AcctDomain.msk.qsft/Amsterdam/Users

User logon name: @AcctDomain.msk.qsft

User logon name (pre-Windows 2000): ACCTDOMAIN\

4. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the wizard.
5. After setting any additional properties, click **Finish** on the completion page of the wizard.

NOTE: Consider the following when copying a user account:

- The behavior of the wizard pages may vary depending on the configuration of Active Roles policies. To determine whether a given item on a page is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the wizard pages. For more information, see Getting policy-related information.

The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.

- By default, some common properties are carried over to the copied user account from the original user account. This includes the group membership settings as well, so if the original user account is a member of a specific group (or groups), the **Copy Object - User** wizard will automatically add the copied user account to the same group(s).

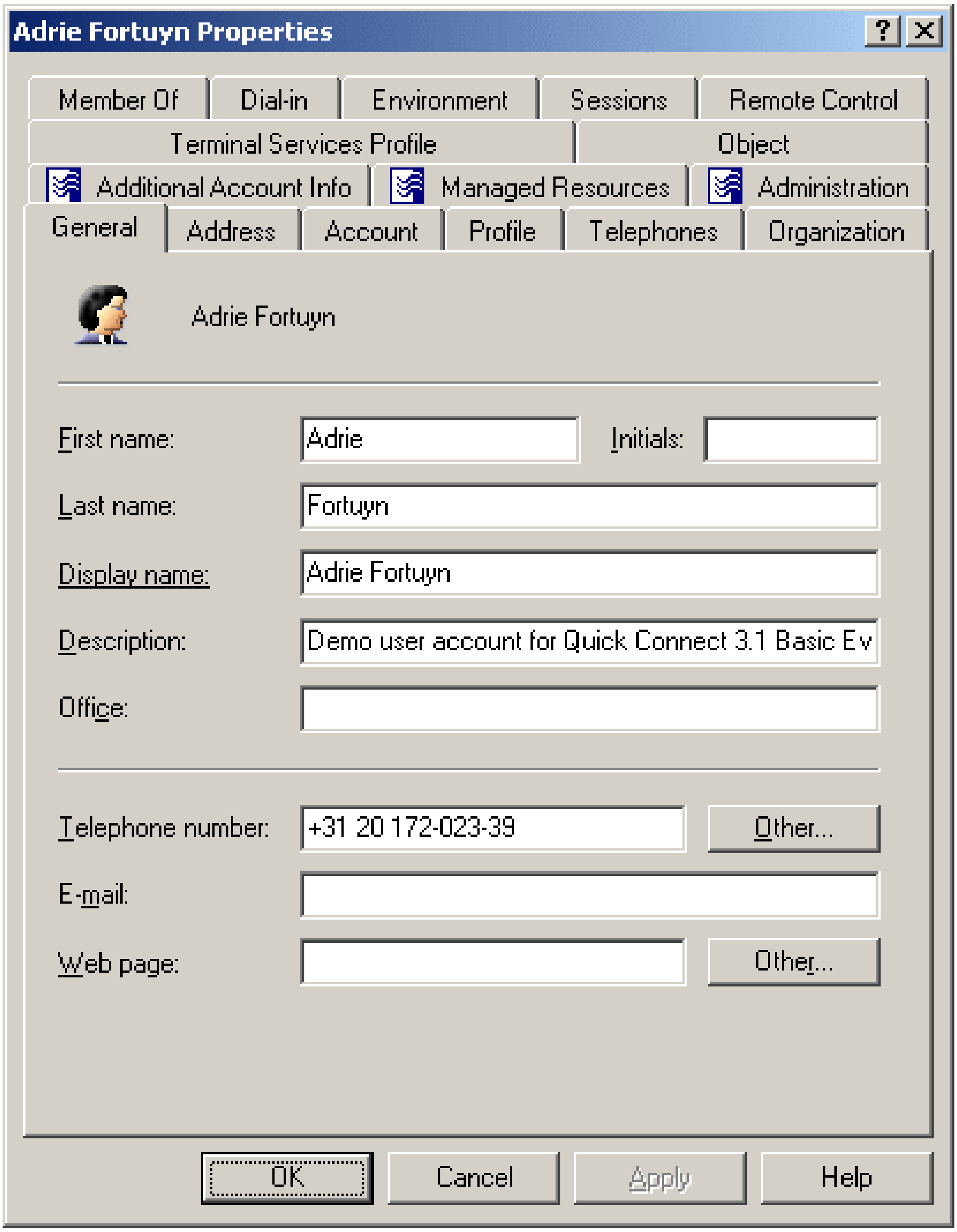
Modifying user account properties

You can modify the properties of Active Directory user accounts with the Active Roles Console.

To modify user account properties

1. In the **Console tree**, locate and select the folder that contains the user account you want to modify.
2. In the details pane, right-click the user account you want to modify, then click **Properties**.

Figure 7: User account properties



Adrie Fortuyn Properties

Adrie Fortuyn

First name: Adrie

Initials:

Last name: Fortuyn

Display name: Adrie Fortuyn

Description: Demo user account for Quick Connect 3.1 Basic Ev

Office:

Telephone number: +31 20 172-023-39

E-mail:

Web page:

3. Use the tabs in the **Properties** dialog to view or modify properties of the user account.

4. If you want to view or modify additional properties (those for which the tabs in the **Properties** dialog do not provide data entries), navigate to the **Object** tab and click **Advanced Properties**.
5. After setting all the properties you want, click **OK**.

> NOTE: Consider the following when modifying object properties:
>
> - In the wizard, some property labels may be displayed as hyperlinks. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed. For more information, see Getting policy-related information.
>
>   The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.
> - To modify properties for multiple objects, press and hold **Ctrl**, then click each object. Right-click the selection, then click **Properties**.
> - You can use the **Properties** dialog to view or modify any property of the object by navigating to the **Object** tab and clicking **Advanced Properties**. In the **Advanced Properties** window you can manage all properties, including those that cannot be accessed via the **Properties** dialog itself.
>
>   You can also display the **Advanced Properties** window by right-clicking the object and selecting **All Tasks** > **Advanced Properties**.
> - To locate the object that you want to modify, use the **Find** function of Active Roles. Once you found the object, open the **Properties** page by right-clicking the object, and clicking **Properties**.

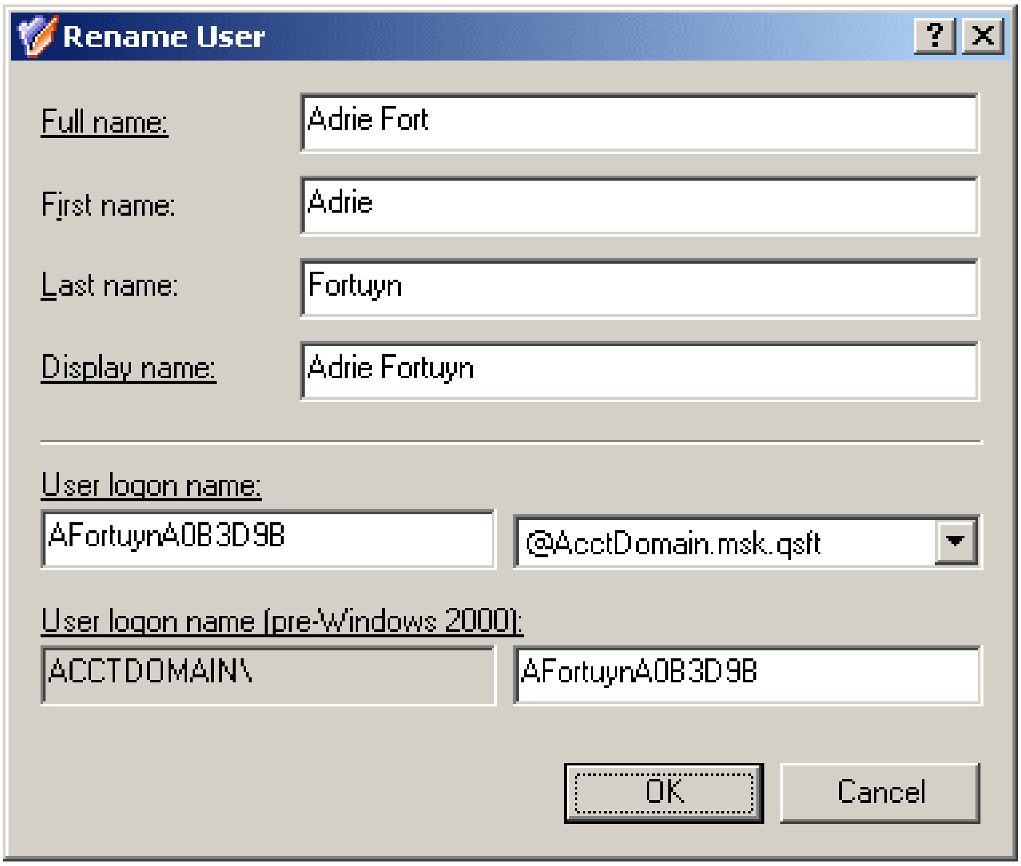
Renaming a user account

You can rename Active Directory user accounts with the Active Roles Console.

To rename a user account

1. In the **Console tree**, locate and select the folder that contains the user account you want to rename.
2. In the details pane, right-click the user account and click **Rename**.
3. Type a new name (or clear the existing name), then press **Enter** to display the **Rename User** dialog.

Figure 8: Rename User



Full name: Adrie Fort

First name: Adrie

Last name: Fortuyn

Display name: Adrie Fortuyn

User logon name:

AFortuynA0B3D9B @AcctDomain.msk.qsft

User logon name (pre-Windows 2000):

ACCTDOMAIN\ AFortuynA0B3D9B

4. Use the **Rename User** dialog to modify (if needed) the naming properties of the user account such as the user full name, first name, last name, display name, and login name.
5. When finished, click **OK**.

NOTE: Consider the following when renaming an object:

- The behavior of the dialog may vary depending on the configuration of Active Roles policies. To determine whether a given item in the dialog is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the dialog. For more information, see Getting policy-related information.
- To locate the object you want to rename, use the **Find** function of Active Roles. Once you found the object, rename it by selecting it in the list of search results, right-clicking it, clicking **Rename**, then specifying the new name. To apply the new name, press **Enter**.

Blocking and unblocking a user account

To prevent a particular user from logging on, you can block the user account as a security measure instead of deleting it. You can block and unblock Active Directory user accounts with the Active Roles Console.

To block a user account

1. In the **Console tree**, locate and select the folder that contains the user account you want to block.
2. In the details pane, right-click the user account and click **Disable Account**.

> NOTE: Consider the following when blocking a user account:
>
> - To prevent particular users from logging on for security reasons, the administrator can block user accounts instead of deleting user accounts.
> - The **Disable Account** command appears if the account is enabled and thus can be used for login; otherwise, the **Enable Account** command appears on the menu. By using the **Enable Account** command the administrator can change the status of the blocked account to allow the user to log in with that account.
> - To locate user accounts for blocking, use the **Find** function of Active Roles. Once you found the users, block them by selecting the accounts in the list of search results, right-clicking the selection, and clicking **Disable**.
> - Since the **Copy** function ensures that the copy of a user account belongs to the same groups as the original user account, you can create a blocked user account that belongs to certain groups, then make copies of that account to simplify the creation of user accounts with common group memberships.

You can unblock a blocked user account with the Active Roles Console. The **Enable Account** command only appears for deactivated accounts, marked with the icon.

To unblock a blocked user account

1. In the **Console tree**, locate and select the folder that contains the user account you want to unblock.
2. In the details pane, right-click the user account and click **Enable Account**.

> NOTE: Consider the following when unblocking a user account:
>
> - The **Enable Account** command appears if the account is blocked and cannot be used for login; otherwise, the **Disable Account** command appears in the menu. To prevent particular users from logging in for security reasons, block user accounts with the **Disable Account** command.
> - To locate user accounts for unblocking, use the **Find** function of Active Roles. Once you found the users, unblock them by selecting the accounts in the list of search results, right-clicking the selection, and clicking **Enable Account**.

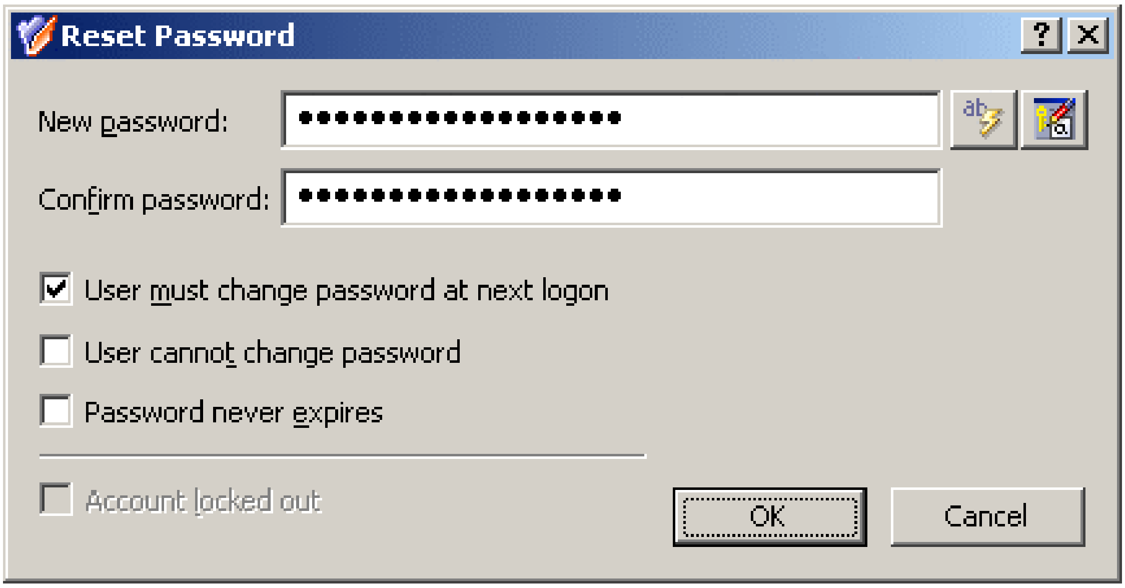
Resetting a user password

You can reset the password of a Active Directory user account with the Active Roles Console.

To reset a user password

1. In the **Console tree**, locate and select the folder that contains the user account whose password you want to reset.
2. In the details pane, right-click the user account whose password you want to reset, then click **Reset Password** to display the **Reset Password** dialog.
3. Type and confirm the password, or click the button next to the **New password** box to have Active Roles generate a password.

Figure 9: Reset Password



Reset Password

New password: •••••••••••••••••••

Confirm password: •••••••••••••••••••

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account locked out

4. Configure the available password options with the appropriate check boxes. For example, if your organization requires users to change the reset password during their next login, select **User must change password at next logon**.
5. When finished, click **OK**.

NOTE: Consider the following when resetting a user password:

- To spell out the specified or auto-generated password, click the **Spell out password** button.
- Services that are authenticated with a user account must be reset if the password for the service's user account is changed.
- To locate the user account whose password you want to reset, use the **Find** function of Active Roles. Once you found the user account, reset its password by

selecting it in the list of search results, right-clicking it, and clicking **Reset Password**.

Adding a user account to a group

You can add Active Directory user accounts to a group with the Active Roles Console.

To add a user account to a group

1. In the **Console tree**, locate and select the folder that contains the user account you want to add to a group.
2. In the details pane, right-click the user account, then click **Add to a Group**.
3. Use the **Select Objects** dialog to locate and select the group to which you want to add the user account (you can select more than one group).

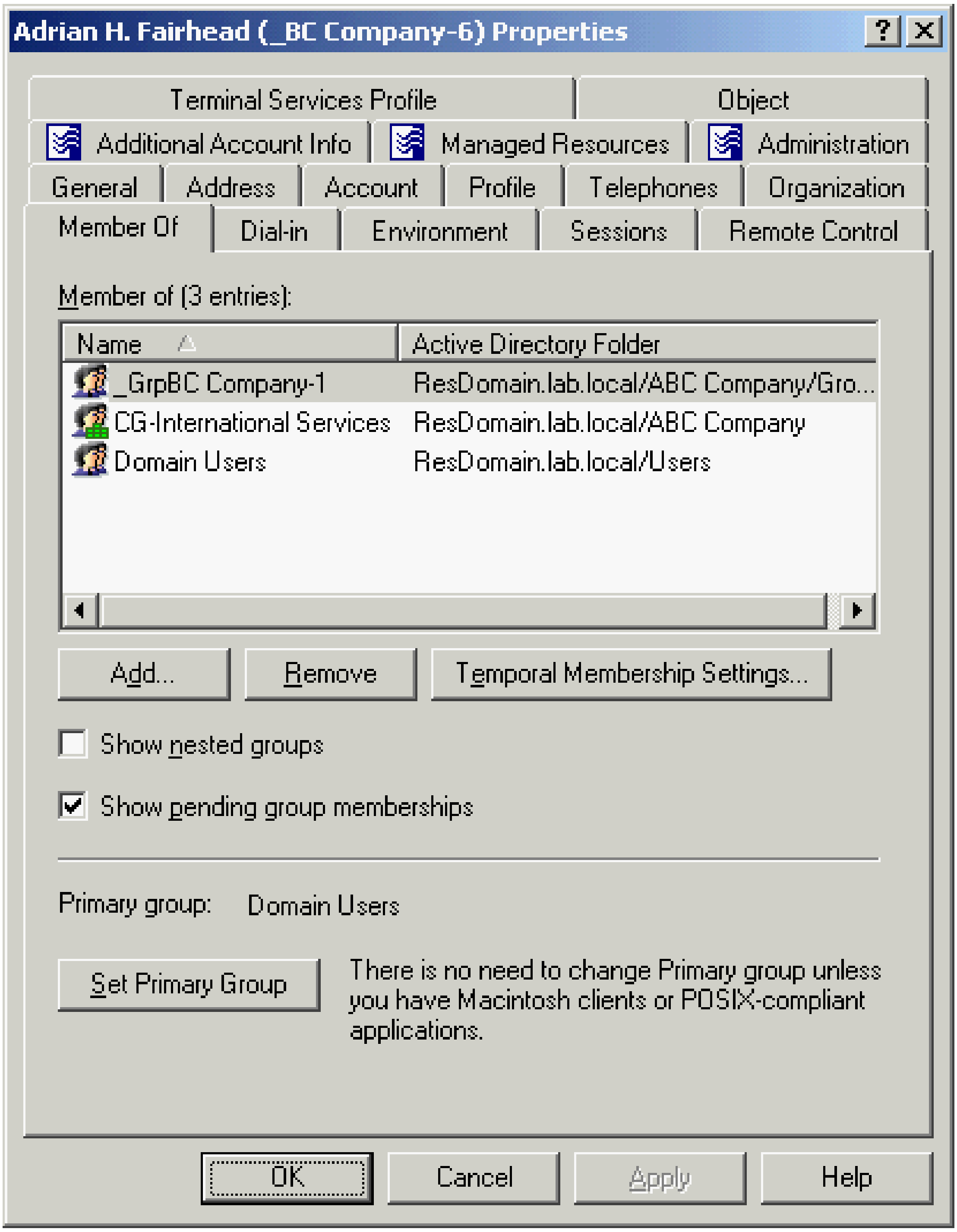
NOTE: Consider the following when adding an object to a group:

- In the **Select Objects** dialog, you can select groups from the list or type group names, separating them with semicolons. Click **Check Names** to verify the names you type. If Active Roles cannot find a group, it prompts you to correct the name.
- You can add multiple objects to a group at a time: Select the objects, right-click the selection, and click **Add to a Group**. To select multiple objects, press and hold down **Ctrl**, then click each object.

  When you select multiple objects, the **Member Of** tab lists the groups to which all the selected objects belong. If one of the objects does not belong to a given group, that group does not appear in the list.
- You can also add or remove objects from groups by using the **Properties** dialog: Select one or more objects, right-click the selection, click **Properties**, and go to the **Member Of** tab in the **Properties** dialog.
- On the **Member Of** tab, you can manage groups directly from the list of groups. To manage a group, right-click it, and use commands on the shortcut menu.
- The **Member Of** tab lists the groups to which the object belongs. If the **Show nested groups** check box is selected, the list also includes the groups to which the object belongs owing to group nesting.
- You can also add the object to groups by clicking **Add** on the **Member Of** tab. This displays the **Select Objects** dialog, allowing you to select the groups to which you want to add the object.
- The **Temporal Membership Settings** button can be used to specify the date and time when the object should be added or removed from the selected groups. For more information about this feature, see Using temporal group memberships.
- By adding an object to a group, you can assign permissions to all of the objects in that group and filter Group Policy settings on all objects in that group.

- To locate objects you want to add to a certain group, use the **Find** function of Active Roles. Once you found the objects, select the accounts in the list of search results, right-click the selection, and click **Add to a Group**.

Figure 10: Adding user accounts to groups



Member of (3 entries):

Name	Active Directory Folder
_GrpBC Company-1	ResDomain.lab.local/ABC Company/Gro...
CG-International Services	ResDomain.lab.local/ABC Company
Domain Users	ResDomain.lab.local/Users

□ Show nested groups

☑ Show pending group memberships

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Removing a user account from a group

You can remove user accounts from Active Directory groups with the Active Roles Console.

To remove a user account from a group

1. In the **Console tree**, locate and select the folder that contains the user account you want to remove from a group.
2. In the details pane, right-click the user account, then click **Properties**.
3. On the **Member Of** tab in the **Properties** dialog, clear the **Show nested groups** check box, select the group from which you want to remove the user account, and click **Remove**.

> NOTE: Consider the following when removing an object from a group:
>
> - If you have not cleared the **Show nested groups** check box, the list on the **Member Of** tab also includes the groups to which the object belongs indirectly, that is, because of group nesting. If you select such a group from the list, the **Remove** button is unavailable. An object can be removed only from those groups of which the object is a direct member.
> - You cannot remove objects from their primary groups. Instead, you can change the primary group of an object. To do so, on the **Member Of** tab, select a different group from the list, then click **Set Primary Group**.

Changing the primary group of a user

You can change the primary group of a user with the Active Roles Console.

To change the primary group of a user

1. In the **Console tree**, locate and select the folder that contains the user account whose primary group you want to change.
2. In the details pane, right-click the user account, then click **Properties**.
3. On the **Member Of** tab in the **Properties** dialog, click the group that you want to set as the primary group of the user, then click **Set Primary Group**.

> NOTE: Consider the following when changing a user's primary group:
>
> - Primary groups are used exclusively by Macintosh clients and POSIX-compliant applications. Unless you are using these services, there is no need to change the primary group from Domain Users, which is the default value.
> - The primary group of the user must be in the same domain as the user account. Also, the primary group must be either a global or universal security group. If you select a group with the group scope set to `Domain local`, or you select a distribution

> group, then the **Set Primary Group** button will not be available.
>
> - Setting the primary group of the user to a value other than Domain Users may negatively affect performance, as all users in the domain are members of Domain Users. If the primary group of the user is set to another group, it may cause the group membership to exceed the supported maximum number of members.

Performing Exchange tasks on a user account

You can perform Exchange-related tasks (for example, creating or deleting email addresses) on Active Directory (AD) user accounts with the Active Roles Console.

To perform Exchange tasks on a user account

1. In the **Console tree**, locate and select the folder that contains the user account you want to perform Exchange tasks on.
2. In the details pane, right-click the user account and click **Exchange Tasks** to start the Exchange Task Wizard.
3. On the **Available Tasks** page of the wizard, select the task you want to perform.

   The following tasks are available, depending on the selected group:

   - **Create User Mailbox**, **Establish E-mail Addresses**: The account is enabled, and does not have a mailbox or external email address.
   - **Create User Mailbox**, **Create Room Mailbox**, **Create Equipment Mailbox**, **Create Linked Mailbox**, **Create Shared Mailbox**, **Establish E-mail Addresses**: The account is disabled, and does not have a mailbox or external email address.
   - **Move Mailbox**, **Disable Mailbox**: The account has a mailbox.
   - **Delete E-mail Addresses**: The account has an external email address.
   - **Enable Archive**: The account has a user mailbox without an archive.
   - **Disable Archive**: The account has a user mailbox with an archive.
4. On the next page of the wizard, do one of the following, depending on the selected task:
   - **Mailbox Settings**: Specify the alias and mailbox database. You can select a retention policy, Exchange ActiveSync mailbox policy, or address book policy for the mailbox.
   - **Enable Archive**: (Optional) Specify the mailbox database for the archive.
   - **Resource Information**: Configure the resource capacity and custom properties for the room or equipment mailbox.
   - **Master Account**: Select the master account for the linked mailbox.

- **Mailbox Sharing**: Specify the users who you want to have access to the mailbox.
- **Establish E-mail Addresses**: Specify the user alias and external email address.
- **Move Mailbox**: Select the database to which you want to move the mailbox. If the mailbox has an archive enabled, specify whether to move only the mailbox, only the archive, or both the mailbox and the archive.
- **Disable Mailbox**, **Disable Archive**, **Delete E-mail Addresses**: Confirm the operation.

5. On the completion page of the wizard, review the results of the task. To view the progress report, click **Back**. To close the wizard, click **Finish**.

> NOTE: Consider the following when performing Exchange tasks:
>
> - You can perform Exchange tasks on multiple objects at a time. To do so, start the Exchange Task Wizard by selecting the objects, right-clicking the selection, and clicking **Exchange Tasks**.
> - To locate the objects on which you want to perform Exchange tasks, use the **Find** function of Active Roles. Once you found the objects, start the Exchange Task Wizard by selecting the objects in the list of search results, right-clicking the selection, and clicking **Exchange Tasks**.

Moving a user account

You can move user accounts from one Active Directory container to another with the Active Roles Console.

To move a user account

1. In the **Console tree**, locate and select the folder that contains the user account you want to move.
2. In the details pane, right-click the user account and click **Move** to display the **Move** dialog.
3. In the **Move** dialog, select the folder to which you want to move the user account, then click **OK**.

> NOTE: Consider the following when moving an object:
>
> - With Active Roles, directory objects can only be moved within the same domain. This means that the folder to which you want to move the object must belong to the same domain as the object.
> - You can move multiple objects at a time with the **Move** dialog. To open the dialog, select the objects, right-click the selection, and click **Move**. To select multiple objects, press and hold **Ctrl**, then click each object.

- To locate the object that you want to move, use the **Find** function of Active Roles. Once you found the accounts, open the **Move** dialog by right-clicking the object, and clicking **Move**.
- The Console provides the drag-and-drop function for moving objects. To move objects, you can drag the selection from the details pane to a destination container in the **Console tree**.

Exporting and importing user accounts

With the Active Roles Console, you can export user accounts to an XML file and then import them from that file to populate a container in a different domain. The export and import operations provide a way to relocate user accounts between domains.

To export user accounts, select them, right-click the selection, and select **All Tasks** > **Export**. In the **Export Objects** dialog, specify the file where you want to save the data, and click **Save**.

To import user accounts, right-click the container where you want to place the accounts, and then click **Import**. In the **Import Directory Objects** dialog, select the file to which the user accounts were exported, and click **Open**.

Deleting a user account

You can delete Active Directory user accounts with the Active Roles Console.

To delete a user account

1. In the **Console tree**, locate and select the folder that contains the user account you want to delete.
2. In the details pane, right-click the user account, then click **Delete**.

NOTE: Consider the following when deleting a user account:

- Deleting an account is a destructive operation that cannot be undone. Once an account is deleted, the permissions and memberships associated with that account are also permanently deleted. Because the security ID (SID) for each account is unique, a new account with the same name as the previously deleted account does not automatically receive the permissions and memberships that the previously deleted account had. To duplicate a deleted account, you must recreate all permissions and memberships manually.
- You can delete multiple objects at the same time by selecting the objects, right-clicking the selection, and clicking **Delete**. To select multiple objects, press and hold **Ctrl**, then click each object. If you select multiple objects, clicking **Delete** displays a dialog. To delete all the selected objects, select the **Apply to all items**

check box, then click **Yes**.

- Instead of deleting user accounts, you can also deprovision them by selecting the accounts, right-clicking the selection, then clicking **Deprovision**.
- To locate user accounts for deletion or deprovisioning, use the **Find** function of Active Roles. Once you found the users, delete or deprovision them by selecting the accounts in the list of search results, right-clicking the selection, and clicking **Delete** or **Deprovision**.
- When attempting to delete an object, you may receive an error message that access is denied to the object. This can typically occur if the object is protected from deletion. To remove this protection, navigate to the **Properties** > **Object** tab of the object you want to delete, then clear the **Protect object from accidental deletion** check box. After that, try deleting the object again.

Deprovisioning a user account

Active Roles provides the ability to deprovision rather than delete or only deactivate user accounts. Deprovisioning a user refers to a set of actions that are performed by Active Roles in order to prevent the user from logging in to the network and accessing network resources such as the user mailbox or home folder.

The **Deprovision** command on a user account updates the account according to the deprovisioning policies. Active Roles comes with a default policy to automate some commonly-used deprovisioning tasks, and allows administrators to configure and apply additional policies.

You can deprovision Active Directory user accounts with the Active Roles Console.

To deprovision a user account

1. In the **Console tree**, locate and select the folder that contains the user account you want to deprovision.
2. In the details pane, right-click the user account, then click **Deprovision**.
3. Wait while Active Roles updates the user account.

NOTE: Consider the following when deprovisioning a user account:

- You can deprovision multiple accounts at a time. Select two or more user accounts, right-click the selection, then click **Deprovision**.
- The **Deprovision** command is also available in the Active Roles Web Interface. When you click the **Deprovision** command, the operation progress and results are displayed. When the operation is completed, Active Roles displays the operation summary, and allows you to examine operation results in detail.
- On a deprovisioned user account, you can use the **Deprovisioning Results** command to view a report that lists the actions taken during the deprovisioning of the account. For each action, the report informs about success or failure of the

action. In the event of a failure, the report provides a description of the error situation.

- If a deprovisioned user account needs to be restored (for example, if a user account has been deprovisioned by mistake), the account can be reset to the state it was in before the deprovisioning occurred. This can be accomplished by using the **Undo Deprovisioning** command on the deprovisioned account.

Restoring a deprovisioned user account

Active Roles provides the ability to restore deprovisioned user accounts. The purpose of this operation, referred to as the Undo Deprovisioning operation, is to roll back the changes that were made to a user account by the Deprovision operation. When a deprovisioned user account needs to be restored (for example, if a user account has been deprovisioned by mistake), the Undo Deprovisioning operation allows the account to be restored to the state it was in before the changes were made.

You can restore previously deprovisioned Active Directory user accounts with the Active Roles Console.

To restore a deprovisioned user account

1. In the **Console tree**, locate and select the folder that contains the user account you want to restore.
2. In the details pane, right-click the user account, then click **Undo Deprovisioning**.
3. In the **Password Options** dialog, choose the options to apply to the password of the restored account, then click **OK**.

   For information about each option, open the **Password Options** dialog, then press **F1**.
4. Wait while Active Roles restores the user account.

   When you click the **Undo Deprovisioning** command, the operation progress and results are displayed. When the operation is completed, Active Roles displays the operation summary, and allows you to examine the operation results in detail. You can view a report that lists the actions taken during the restore operation. For each action, the report informs about success or failure of the action. In the event of a failure, the report provides a description of the error situation.

Managing user certificates

You can use Active Roles to add or remove digital (X.509) certificates from user accounts in Active Directory. By adding a certificate to a user account you make the certificate (including the public key associated with the certificate) available to other Active Directory users and to Active Directory-aware applications and services.

The certificates added to Active Directory user accounts are referred to as published certificates. Published authentication certificates are used by Active Directory domain controllers during certificate-based authentication. Published encryption certificates can be used to enable access to encrypted contents. For instance, in the case of e-mail encryption, the sender retrieves the recipient's certificate from the Active Directory user account and uses that certificate to encrypt the email message so that the recipient could decrypt the message by using the private key associated with the certificate. A similar process occurs when you want to allow a given user to read an encrypted file. The certificate retrieved from the user account is used to encrypt the file encryption key so that the file encryption key could be obtained by using the private portion of the user's certificate to decrypt the encrypted key material.

To view or change the list of digital certificates for a particular user account, open the **Properties** page for that user account in the Active Roles Console or Web Interfaceand go to the **Published Certificates** tab. From the **Published Certificates** tab, you can perform the following tasks:

- View the list of the certificates published for the user account in Active Directory.
- Examine each of the published certificates in detail.
- Add a certificate from the local certificate store (available in the Console only).
- Add a certificate that is saved in a certificate file.
- Remove a certificate from the user account.
- Copy a published certificate to a certificate file.

For each of the certificates that are listed on the **Published Certificates** tab, you can view the following information:

- The purposes that the certificate is intended for (available in the Console only).
- The name of the person or company to which the certificate was issued.
- The name of the certification authority that issued the certificate.
- The time period for which the certificate is valid.
- Additional information about the certification authority that issued the certificate, if available.
- The list of all X.509 fields, extensions, and associated properties found in the certificate.
- The hierarchy of certification authorities for the certificate (available in the Console only).

To add or remove a certificate for a user account using the Active Roles Console

1. Open the **Properties** dialog for the user account and click the **Published Certificates** tab.
2. Do the following:
    - Click **Add from Store** to add a certificate from the local certificate store.
    - Click **Add from File** to add a certificate that is saved in a certificate file.

- Select a certificate from the list on the tab and click **Remove** to remove the certificate.

From the **Published Certificates** page in the Active Roles Console, you can also view or export any of the certificates listed on that page. Select a certificate from the list, then click **View Certificate** to examine the certificate in detail or click **Copy to File** to save a copy of the certificate to a file.

Management of group Management Service Accounts

You can administer group Managed Service Accounts (gMSAs) with Active Roles. gMSA is a domain security principal whose password is managed by Domain Controllers (DCs) and can be retrieved by multiple systems running supported Windows Server operating systems. Having Windows services use gMSA as their login account minimizes the administrative overhead by enabling Windows to handle password management for service accounts. gMSAs provide the same functionality as Managed Service Accounts (MSAs), but extend that functionality over multiple servers.

As you can use a single gMSA on multiple servers, gMSA provides a single identity solution for services running on a server farm. With a service hosted on a server farm, gMSA enables all service instances to use the same logon account (which is a requirement for mutual authentication between the service and the client), while letting Windows change the account password periodically instead of relying on the administrator to perform that task.

For more information about group Managed Service Accounts, see Group Managed Service Accounts Overview.

gMSA management tasks

The Active Directory domain in which you are going to create and administer group Managed Service Accounts must meet the following requirements:

- The domain has an least one Domain Controller (DC) that runs Windows Server 2016 or newer.
- The domain has the KDS Root Key created.

  You can create a KDS Root Key by running the `Add-KDSRootKey` PowerShell command on the DC. For more information, see at Create the Key Distribution Services KDS Root Key for further details.

NOTE: You cannot perform Exchange-related operations on the on-premises Exchange Server environment with the gMSA account. For example, you cannot manage remote mailboxes, user mailboxes, or contacts.

Creating a gMSA

Perform the following steps in the Active Roles Console to create a group Service Managed Account (gMSA).

To create a gMSA

1. Right-click the OU or container in which you want to create a gMSA and select **New** > **Group Managed Service Account**.
2. In the wizard that opens, complete following fields:
   - **Name**: Specifies the name of the gMSA in Active Directory.
   - **Description**: Specifies a description of the gMSA.
   - **DNS host name**: Specifies the DNS hostname. Typically, this is the fully qualified domain name of the server on which you will use the gMSA, for example `your-organization.domain.com`.
   - **Account name (pre-Windows 2000)**: Specifies the legacy login name of the gMSA (`sAMAccountName`). Typically, the value of this setting is the same as the name of the gMSA.
   - **Password change interval (days)**: Specifies the number of days before the managed password is automatically changed for the gMSA.

     > NOTE: You can configure this setting only when creating the gMSA. After creating the gMSA, this setting will be read-only.

   - **Computers or groups**: Specifies the computers on which the gMSA can be used to run services. You can add individual computers to this field, or you can add computers to a security group, then add the group to this field.

Managing the properties of a gMSA

For an existing group Managed Service Account (gMSA), perform the following steps in the Active Roles Console to view or change the properties of the gMSA.

To view or change the properties of the gMSA, right-click the gMSA you want to administer and click **Properties**.

This opens the **Properties** dialog containing the same fields as the gMSA creation wizard (see Creating a gMSA) with the only difference that the **Password change interval** field is read-only. In addition, the **Account is disabled** check box on the **Account** page shows whether the gMSA is disabled for login, and allows you to disable and re-enable the gMSA.

Searching for gMSA in the directory

The Active Roles Console allows you to find group Managed Service Accounts that meet your search conditions.

To search for gMSA in the directory

1. Right-click the OU, domain or container in which you want to search for gMSA and click **Find**.
2. In the **Find** window that opens, configure and start your search:
   a. In the **Find** list, click **Custom Search**.
   b. Click **Field**, and select the **msDS-GroupManagedServiceAccount** object type and the object property to search for.
   c. Configure and add the desired search condition for the object property you have selected.
   d. If needed, add more search conditions by repeating Steps b and c.
   e. Click **Find Now**.

In the list of search results, right-click a gMSA and use the shortcut menu to perform management tasks. For example, you can right-click a gMSA and then click **Properties** to view or change the properties of the gMSA.

Disabling and enabling a gMSA

The Active Roles Console allows you to disable a gMSA so that the gMSA cannot be used for login. For a disabled gMSA, you can use the Console to re-enable that gMSA.

To disable or re-enable a gMSA

1. Right-click the gMSA you want to administer and click **Properties**.
2. In the **Properties** dialog, click the **Account** tab, and examine the **Account is disabled** check box:
   - If the check box is not selected, then the gMSA is enabled for logon. You can disable the gMSA by selecting the **Account is disabled** check box.
   - If the check box is selected, then the gMSA is disabled. You can re-enable the gMSA by clearing the **Account is disabled** check box.

Alternatively, you can use the **Disable Account** or **Enable Account** command on the gMSA object to disable or re-enable the gMSA.

Group management

Groups are Active Directory objects used to collect users, contacts, computers, and other groups into manageable units. There are three kinds of groups:

- **Security groups**: Used to manage user and computer access to shared network resources. When assigning permissions to access resources, administrators assign permissions to security groups rather than to individual users.
- **Distribution groups**: Used as email distribution lists. Distribution groups have no security function.
- **Query-Based Distribution groups**: Used also as email distribution lists but the difference is that members of such a group are not specified statically. Membership of these groups is built in dynamic manner using LDAP queries.

In this document, security and distribution groups are collectively referred to as groups. As for Query-based distribution groups, these are considered a separate category of groups.

Each group has a scope: universal, global, or domain local.

- **Universal**: These groups can include groups and accounts from any domain in the domain tree or forest, and can be granted permissions in any domain in the domain tree or forest.
- **Global**: These groups can only include groups and accounts from the domain in which the group is defined. Global groups can be granted permissions in any domain in the forest.
- **Domain local**: These groups can include groups and accounts from other domains. These groups can only be granted permissions within the domain in which the group is defined.

A group can be a member of another group. This is referred to as group nesting. Group nesting increases the number of affected member accounts and thus consolidates group management. Accounts that reside in a group nested within another group are indirect members of the nesting group.

Active Roles provides the facility to perform administrative tasks such as create copy, rename, modify, and delete groups. It can also be used to add and remove members from groups and perform Exchange tasks on groups.

The following section describes how to use the Active Roles Console to manage groups. You can also use the Active Roles Web Interface to perform the group management tasks.

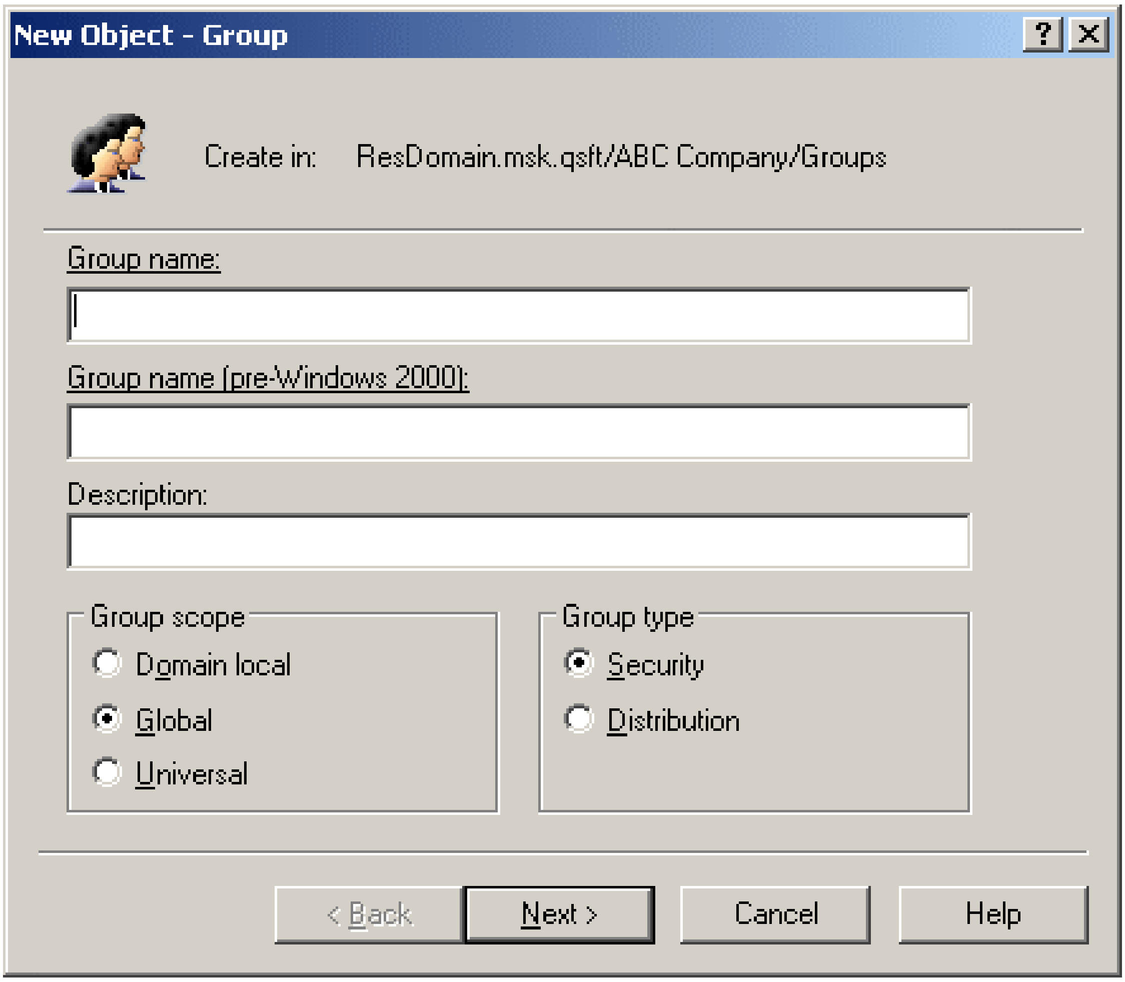
Creating a group

You can create new Active Directory groups with the Active Roles Console.

To create a group

1. In the **Console tree**, locate and select the folder in which you want to add the group.
2. Right-click the folder, point to **New** and click **Group** to start the **New Object - Group** wizard.
3. Follow the wizard pages to specify properties of the new group, such as the group name, pre-Windows 2000 group name, description, scope, type, membership list, and Exchange address settings.

Figure 11: Creating a group



New Object - Group

Create in: ResDomain.msk.qsft/ABC Company/Groups

Group name:

Group name (pre-Windows 2000):

Description:

Group scope
- ○ Domain local
- ● Global
- ○ Universal

Group type
- ● Security
- ○ Distribution

4. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the

wizard.

5. After setting any additional properties, click **Finish** on the completion page of the wizard.

> NOTE: Consider the following when creating a group:
>
> - The behavior of the wizard pages may vary depending on the configuration of Active Roles policies. To determine whether a given item on a page is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the wizard pages. For more information, see Getting policy-related information.
>
>   The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.
> - You can also start the **New Object - Group** wizard by clicking on the toolbar.
> - To create a group, you can also copy a previously created group. For more information, see Copying a group.
> - A new user account with the same name as a previously deleted user account does not automatically assume the permissions and group memberships of the previously deleted group. To duplicate a deleted group, all permissions and memberships must be manually recreated.

Finding a group

You can find Active Directory (AD) groups with the Active Roles Console.

To find a group

1. In the **Console tree**, locate the container you want to search.
2. In the details pane, right-click the container, then click **Find**.
3. In the **Find** window, select **Groups** from the **Find** list, specify your search criteria, and start the search.

   In the search results list, you can right-click groups and use commands on the shortcut menu to perform management tasks.

You can list the Active Directory (AD) groups in which an AD user is a member with the Active Roles Console.

To find groups in which a user is a member

1. In the **Console tree**, locate and select the folder that contains the user account.
2. In the details pane, right-click the user account, then click **Properties**.
3. Click the **Member Of** tab.

> NOTE: Consider the following when finding groups in which a user is a member:

- The **Member Of** tab for a user displays a list of groups in the domain where the user’s account is located. Active Roles does not display groups that reside in trusted domains.
- On the **Member Of** tab, you can select the **Show nested groups** check box in order for the list to also include the groups to which the user belongs because of group nesting.

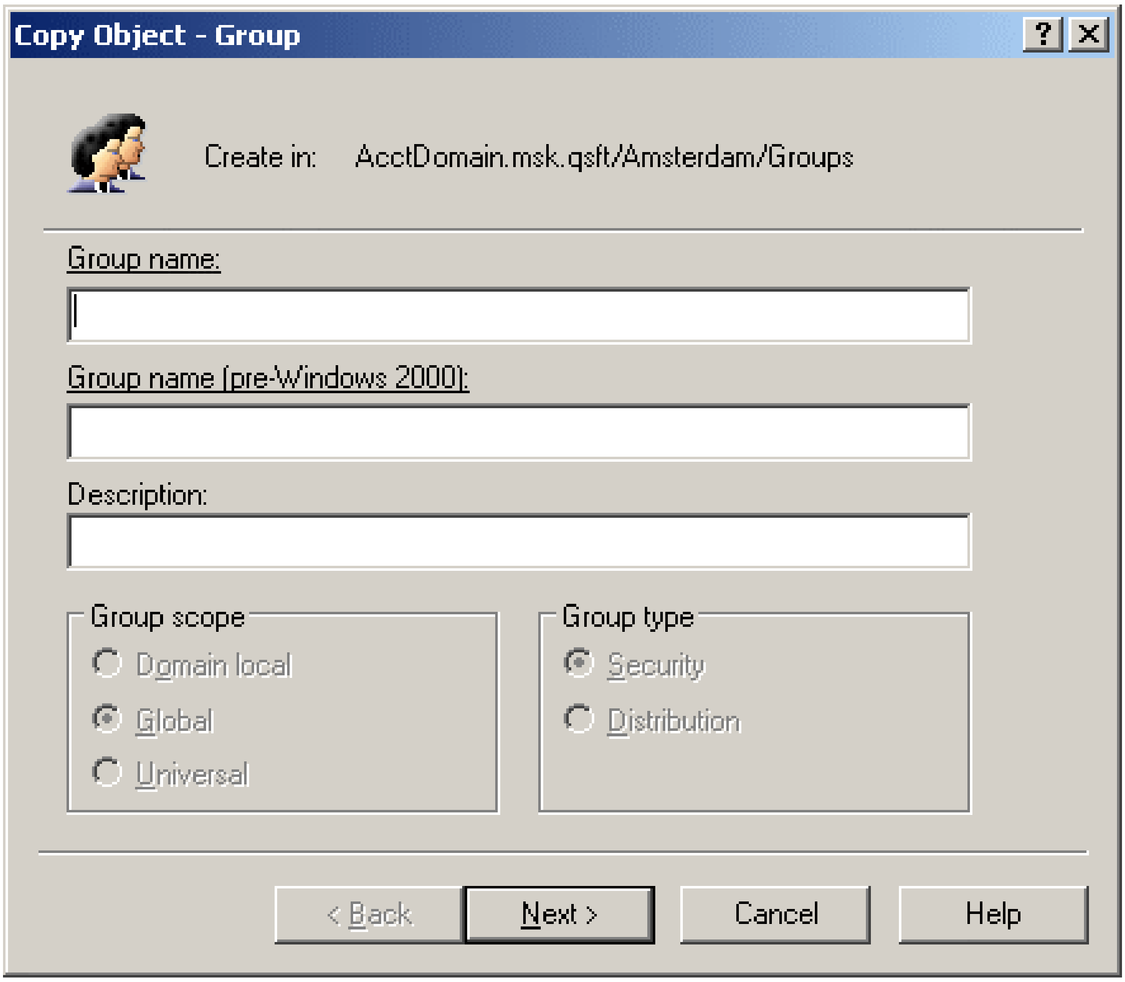
Copying a group

You can copy Active Directory groups with the Active Roles Console.

To copy a group

1. In the **Console tree**, locate and select the folder that contains the group that you want to copy.
2. In the details pane, right-click the group you want to copy, then click **Copy** to start the **Copy Object - Group** wizard.
3. Follow the wizard pages to specify properties of the new group, such as the group name, pre-Windows 2000 name, description, group scope, and group type.

Figure 12: Copying a group



Copy Object - Group

Create in: AcctDomain.msk.qsft/Amsterdam/Groups

Group name:

Group name (pre-Windows 2000):

Description:

Group scope: ○ Domain local ● Global ○ Universal

Group type: ● Security ○ Distribution

4. (Optional) If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the wizard.
5. After setting any additional properties for the copy of the group, click **Finish** on the completion page of the wizard.

> NOTE: Consider the following when copying a group:
>
> - The behavior of the wizard pages may vary depending on the configuration of Active Roles policies. To determine whether a given item on a page is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the wizard pages. For more information, see Getting policy-related information.
>
>   The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.

- By default, some common properties are carried over to the copied group from the original group. Thus, the group membership list is copied from the original group, and can be modified in the **Copy Object - Group** wizard.
- The group scope and group type are also copied from the original group, but these properties cannot be modified in the **Copy Object - Group** wizard. You can change these properties after the copy of the group is created. For instructions, see Changing group type and group scope.
- To locate the group that you want to copy, use the **Find** feature of Active Roles. Once you found the group, you can start the **Copy Object - Group** wizard from the **Find** dialog by right-clicking the group in the list of search results and clicking **Copy**.

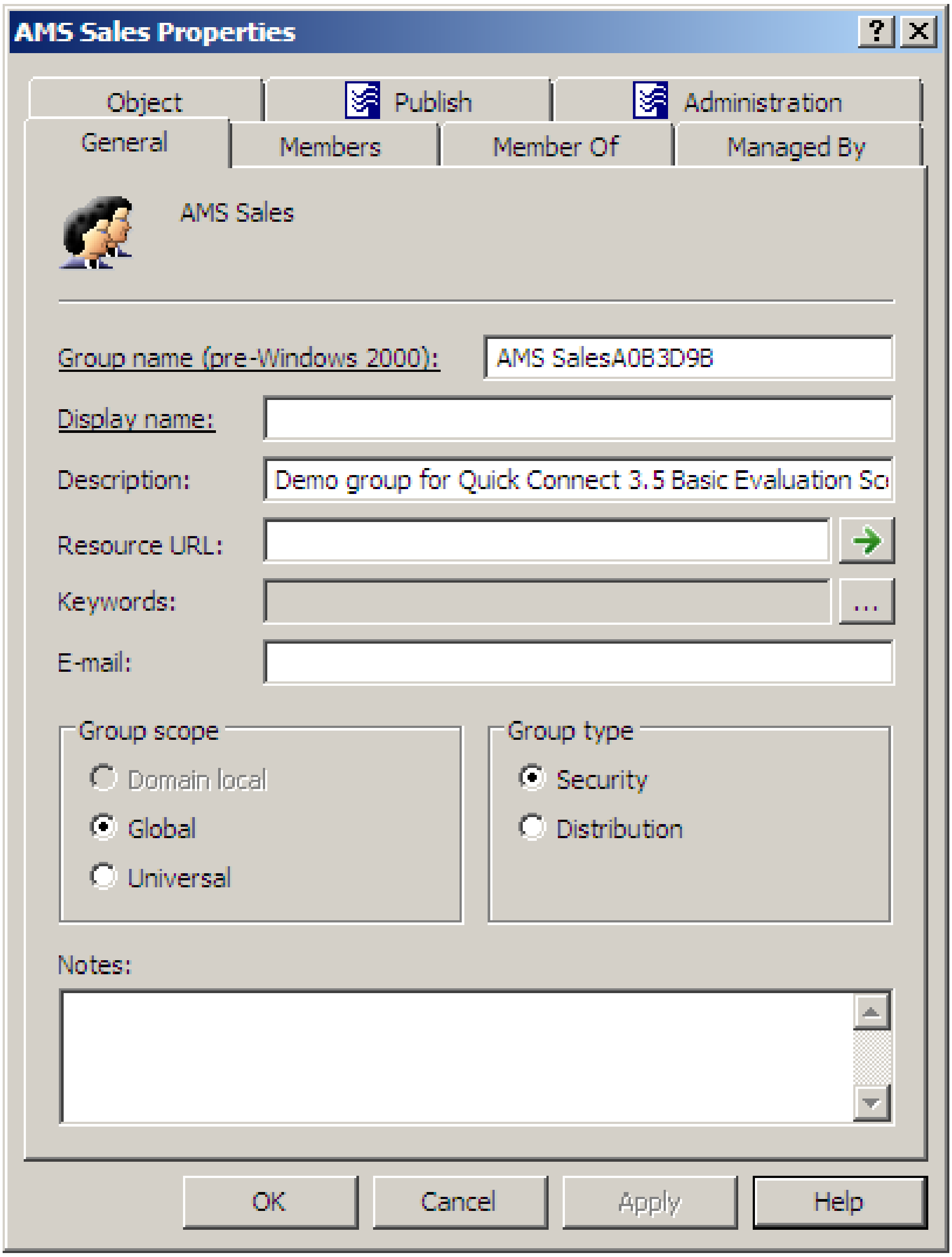
Modifying group properties

You can modify the properties of Active Directory groups with the Active Roles Console.

To modify group properties

1. In the **Console tree**, locate and select the folder that contains the group you want to modify.
2. In the details pane, right-click the group you want to modify, then click **Properties**.

Figure 13: Modifying group properties



AMS Sales

Group name (pre-Windows 2000): AMS SalesA0B3D9B

Display name:

Description: Demo group for Quick Connect 3.5 Basic Evaluation Sc

Resource URL:

Keywords:

E-mail:

Group scope

○ Domain local

● Global

○ Universal

Group type

● Security

○ Distribution

Notes:

3. Use the tabs in the **Properties** dialog to view or modify properties of the group.
4. If you want to view or modify additional properties (those for which the tabs in the **Properties** dialog do not provide data entries), navigate to the **Object** tab and click

Advanced Properties.

5. After setting all the properties you want, click **OK**.

> NOTE: Consider the following when modifying group properties:
>
> - The behavior of the user interface elements in the **Properties** dialog may vary depending on the configuration of Active Roles policies. To determine whether a given item on a tab is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click the underlined text labels to examine the policies that govern the behavior of the user interface elements. For more information, see Getting policy-related information.
>
>   The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.
> - To modify properties for multiple objects, press and hold **Ctrl**, then click each object. Right-click the selection, then click **Properties**.
> - You can also access the **Advanced Properties** dialog for an object by right-clicking the account and selecting **All Tasks** > **Advanced Properties**.
> - To locate the object that you want to modify, use the **Find** function of Active Roles. Once you found the object, open the **Properties** page by right-clicking the object, and clicking **Properties**.

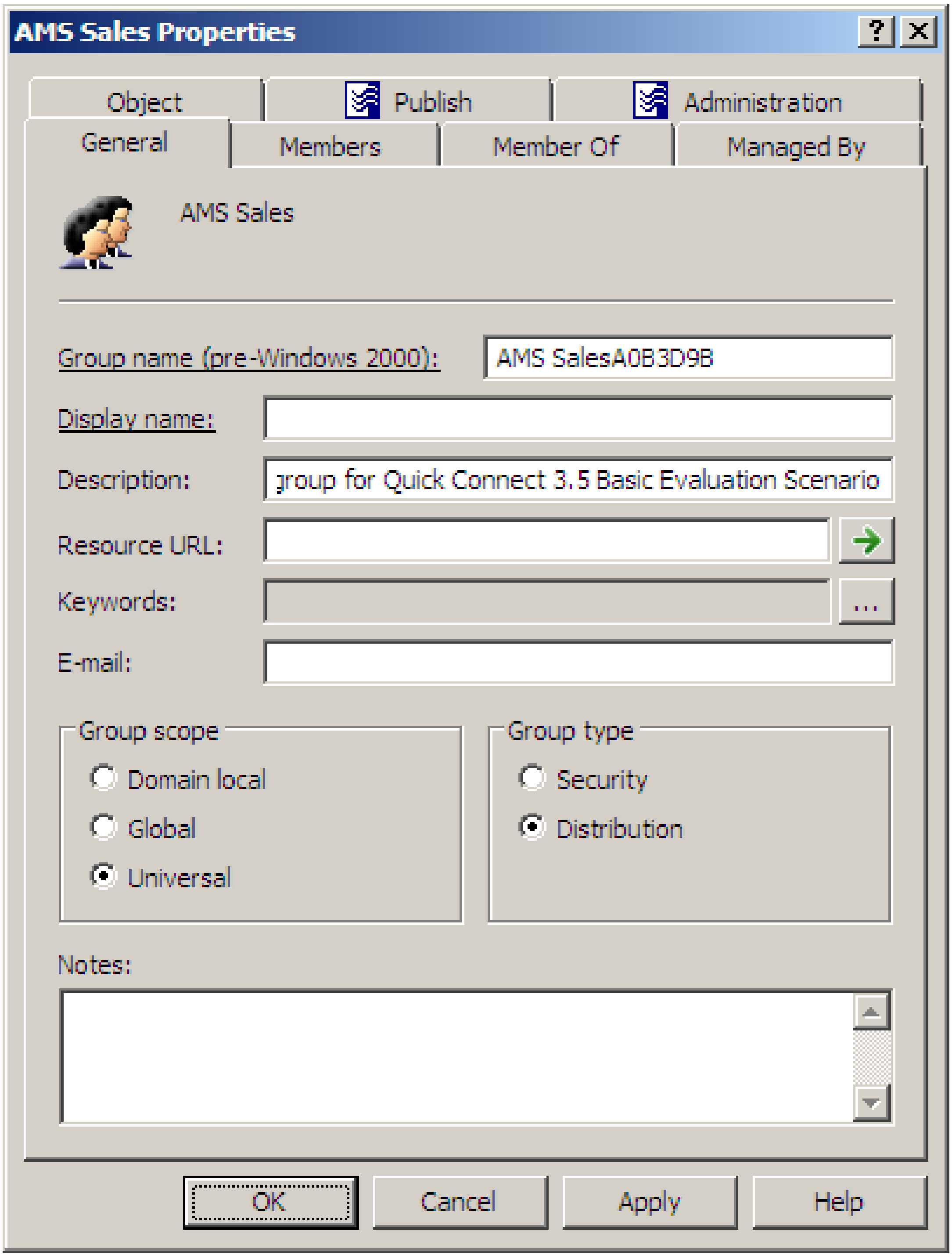
Changing group type and group scope

You can change the group type (security or distribution) of existing groups with the Active Roles Console.

To convert a group to another group type

1. In the **Console tree**, locate and select the folder that contains the group you want to modify.
2. In the details pane, right-click the group you want to modify, then click **Properties**.
3. On the **General** tab in the **Properties** dialog, under **Group type**, select the group type (**Security** or **Distribution**) you want to specify for the group.

Figure 14: Changing group type and group scope



AMS Sales

Group name (pre-Windows 2000): AMS SalesA0B3D9B

Display name:

Description: group for Quick Connect 3.5 Basic Evaluation Scenario

Resource URL:

Keywords:

E-mail:

Group scope

○ Domain local
○ Global
● Universal

Group type

○ Security
● Distribution

Notes:

You can change the scope (domain local, global, universal) of a group with the Active Roles Console.

To change the group scope

1. In the **Console tree**, locate and select the folder that contains the group you want to modify.
2. In the details pane, right-click the group you want to modify, then click **Properties**.
3. On the **General** tab in the **Properties** dialog, under **Group scope**, click the group scope you want for this group.

For information about possible scope settings, see Group management.

> NOTE: Active Roles supports the following group scope changes:
>
> - **Global to universal**: You can perform this scope change only if the modified group is not a member of another global group.
> - **Domain local to universal**: You can perform this scope change only if the modified group does not have another domain local group as a member.
> - **Universal to global**: You can perform this scope change only if the modified group does not have another universal group as a member.
> - **Universal to domain local**: You can perform this scope change without any restictions.

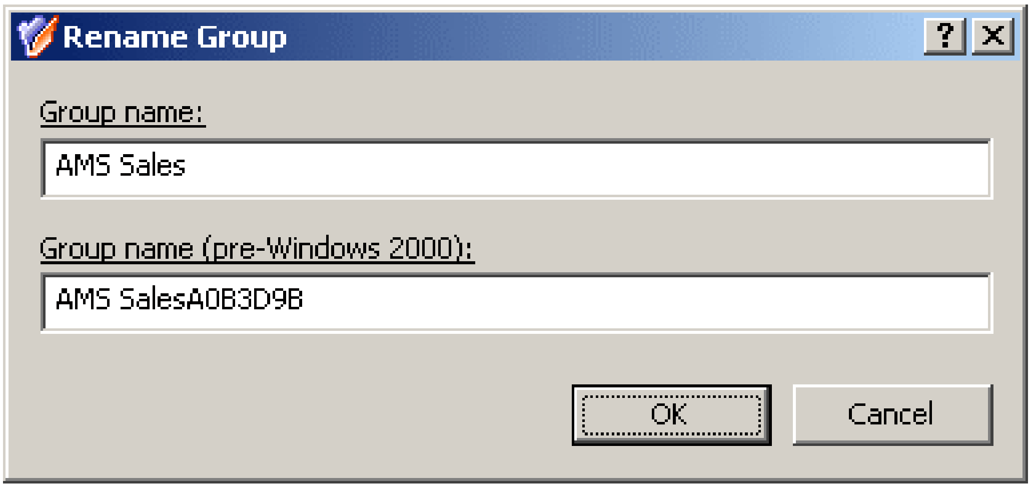
Renaming a group

You can rename Active Directory groups with the Active Roles Console.

To rename a group

1. In the **Console tree**, locate and select the folder that contains the group you want to rename.
2. In the details pane, right-click the group and click **Rename**.
3. Type a new name (or clear the existing name), then press **Enter** to display the **Rename Group** dialog.

Figure 15: Rename Group



Rename Group

Group name:

AMS Sales

Group name (pre-Windows 2000):

AMS SalesA0B3D9B

4. Use the **Rename Group** dialog to modify (if needed) the group name and the group name (pre-Windows 2000).
5. When finished, click **OK**.

NOTE: Consider the following when renaming an object:

- The behavior of the dialog may vary depending on the configuration of Active Roles policies. To determine whether a given item in the dialog is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the dialog. For more information, see Getting policy-related information.
- To locate the object you want to rename, use the **Find** function of Active Roles. Once you found the object, rename it by selecting it in the list of search results, right-clicking it, clicking **Rename**, then specifying the new name. To apply the new name, press **Enter**.

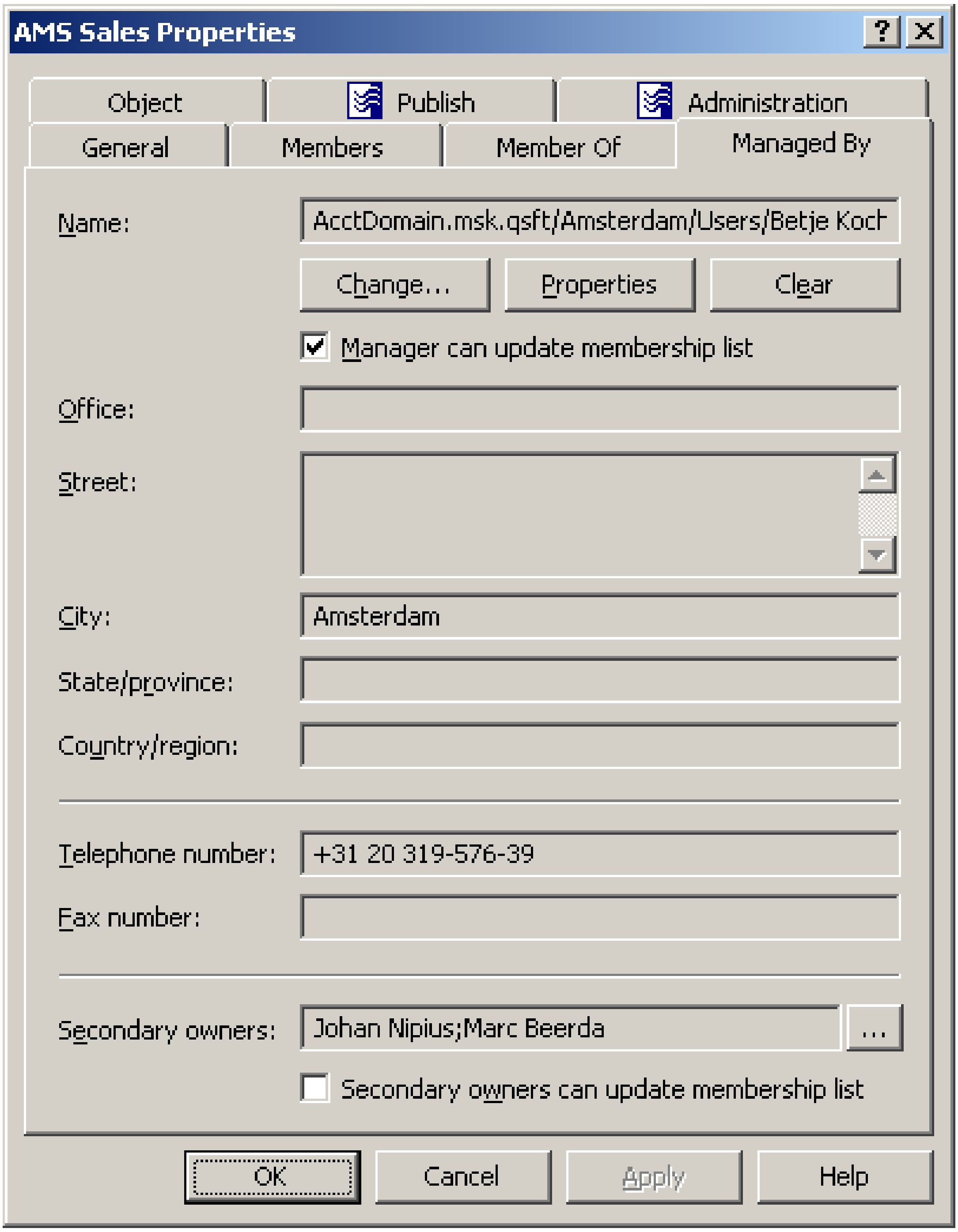
Assigning a manager to a group

You can assign a manager to a group with the Active Roles Console.

To assign a manager to a group

1. In the **Console tree**, locate and select the folder that contains the group you want to assign a manager to.
2. In the details pane, right-click the group, then click **Properties**.
3. On the **Managed By** tab in the **Properties** dialog, click **Change** under the **Name** box.

Figure 16: Assigning a manager to a group



AMS Sales Properties

Name: AcctDomain.msk.qsft/Amsterdam/Users/Betje Koch

☑ Manager can update membership list

Office:

Street:

City: Amsterdam

State/province:

Country/region:

Telephone number: +31 20 319-576-39

Fax number:

Secondary owners: Johan Nipius;Marc Beerda

☐ Secondary owners can update membership list

4. Use the **Select Objects** dialog to locate and select the user or contact you want to be responsible for the group - the manager of the group.

5. (Optional) To authorize the assigned manager to add or remove members from the group, select the **Manager can update membership list** check box.

NOTE: Consider the following when assigning a manager to a group:

- To assign additional managers to the group, click the button next to the **Secondary owners** box. Secondary owners can be given the same rights over the group as the manager. For example, selecting the check box beneath the **Secondary owners** box gives the secondary owners the authority to add or remove members from the group.
- It is possible to assign the management of the group to another group: select a group in the **Select Objects** dialog that you use to specify the manager or a secondary owner. This enables every member of the group to act as the manager or secondary owner.
- To locate the group you want to modify, use the **Find** function of Active Roles. Once you found the group, open its **Properties** dialog by right-clicking the group in the list of search results, then clicking **Properties**.

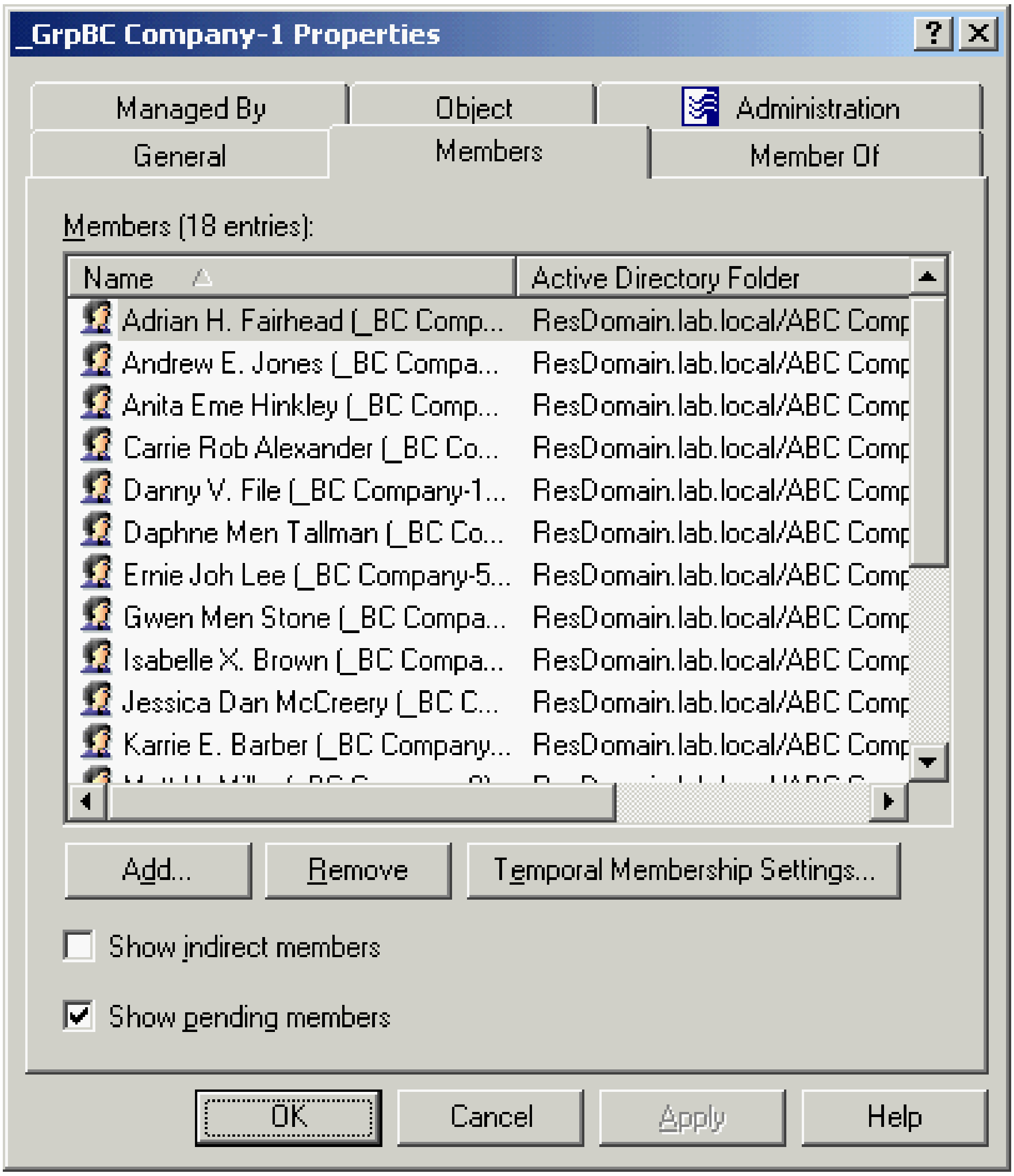
Adding members to a group

Depending on its scope, a group may contain members (users, groups, computers, contacts) from anywhere in the forest, or only members from its own domain.

To add a member to a group

1. In the **Console tree**, locate and select the folder that contains the group to which you want to add a member.
2. In the details pane, right-click the group, then click **Properties**.
3. On the **Members** tab in the **Properties** dialog, click **Add**.

Figure 17: Adding members to a group



Members (18 entries):

Name	Active Directory Folder
Adrian H. Fairhead (_BC Comp...	ResDomain.lab.local/ABC Comp
Andrew E. Jones (_BC Compa...	ResDomain.lab.local/ABC Comp
Anita Eme Hinkley (_BC Comp...	ResDomain.lab.local/ABC Comp
Carrie Rob Alexander (_BC Co...	ResDomain.lab.local/ABC Comp
Danny V. File (_BC Company-1...	ResDomain.lab.local/ABC Comp
Daphne Men Tallman (_BC Co...	ResDomain.lab.local/ABC Comp
Ernie Joh Lee (_BC Company-5...	ResDomain.lab.local/ABC Comp
Gwen Men Stone (_BC Compa...	ResDomain.lab.local/ABC Comp
Isabelle X. Brown (_BC Compa...	ResDomain.lab.local/ABC Comp
Jessica Dan McCreery (_BC C...	ResDomain.lab.local/ABC Comp
Karrie E. Barber (_BC Company...	ResDomain.lab.local/ABC Comp

☐ Show indirect members

☑ Show pending members

4. In the **Select Objects** dialog, type the name of the directory object, such as a user or computer, that you want to add to the group, or select and add the object from the list, then click **OK**.

NOTE: Consider the following when adding members to a group:

- In addition to users and computers, you can also add contacts and other groups to a group.
- In the **Select Objects** dialog, you can select objects from the list or type object names. Click **Check Names** to verify the names you type. If Active Roles cannot

find an object, it prompts you to correct the name.

- On the **Members** tab, you can manage user accounts and other objects directly from the list of members. To manage a group member, right-click the member and use commands on the shortcut menu.
- When you select multiple groups, the **Members** tab lists the objects that belong to each of the selected groups. If a given object does not belong to one of the selected groups, then that object does not appear in the list.
- The **Members** tab displays a list of objects that belong to the group. You can select the **Show indirect members** check box for the **Members** list to also display the objects that belong to the group indirectly (because of group nesting). If that check box is cleared, the **Members** list displays only those objects that were added to the group directly.
- The **Add** button appears on the **Members** tab only if the group is a basic group. For a dynamic group, use the **Membership Rules** tab to populate the group. For details, see Administering dynamic (rule-based) groups.
- The **Temporal Membership Settings** button can be used to specify the date and time when the object should be added or removed from the selected groups. For more information about this feature, see Using temporal group memberships.
- Depending on the scope of a group, the group can hold members from anywhere in the forest or only from its own domain. For more information, see Group management.

Removing members from a group

You can remove members from Active Directory groups with the Active Roles Console.

To remove a member from a group

1. In the **Console tree**, locate and select the folder that contains the group from which you want to remove a member.
2. In the details pane, right-click the group, then click **Properties**.
3. On the **Members** tab in the **Properties** dialog, click the member you want to remove, then click **Remove**.

NOTE: Consider the following when removing members from a group:

- The **Members** tab displays a list of objects that belong to the group. You can select the **Show indirect members** check box for the **Members** list to also display the objects that belong to the group indirectly (because of group nesting). If that check box is cleared, the **Members** list displays only those objects that were added to the group directly.
- With the **Show indirect members** check box selected, the **Members** list also includes the objects that belong to the group indirectly. If you select such an object

from the list, the **Remove** button is unavailable. An object can be removed from only those groups of which the object is a direct member.

- The **Remove** button appears on the **Members** tab only if the group is a static group. For a dynamic group, use the **Membership Rules** tab to add or remove members from the group. For more information, see Administering dynamic (rule-based) groups.

Performing Exchange tasks on a group

You can perform Exchange-related tasks (for example, creating or deleting email addresses) on Active Directory (AD) groups with the Active Roles Console.

To perform Exchange tasks on a group

1. In the **Console tree**, locate and select the folder that contains the group you want to perform Exchange tasks on.
2. In the details pane, right-click the group, then click **Exchange Tasks** to start the Exchange Task Wizard.
3. On the **Available Tasks** page of the wizard, select the task you want to perform.

   The following tasks are available, depending on the selected group:

   - **Establish E-mail Address**: The group has no email address established.
   - **Delete E-mail Addresses**: The group has an email address established.
4. On the next page of the wizard, do one of the following, depending on the selected task:
   - **Establish E-mail Addresses**: Modify the alias of the group, if needed. By default, the alias is the same as the name of the group.
   - **Delete E-mail Addresses**: Confirm the deletion of the email addresses.
5. On the completion page of the wizard, review the results of the task. To view the progress report, click **Back**. To close the wizard, click **Finish**.

NOTE: Consider the following when performing Exchange tasks on a group:

- You can perform Exchange tasks on multiple objects at a time. To do so, start the Exchange Task Wizard by selecting the objects, right-clicking the selection, and clicking **Exchange Tasks**.
- To locate the objects on which you want to perform Exchange tasks, use the **Find** function of Active Roles. Once you found the objects, start the Exchange Task Wizard by selecting the objects in the list of search results, right-clicking the selection, and clicking **Exchange Tasks**.

Moving a group

You can move groups from one Active Directory container to another with the Active Roles Console.

To move a group

1. In the **Console tree**, locate and select the folder that contains the group you want to move.
2. In the details pane, right-click the group and click **Move** to display the **Move** dialog.
3. In the **Move** dialog, select the folder to which you want to move the group, then click **OK**.

> NOTE: Consider the following when moving an object:
>
> - With Active Roles, directory objects can only be moved within the same domain. This means that the folder to which you want to move the object must belong to the same domain as the object.
> - You can move multiple objects at a time with the **Move** dialog. To open the dialog, select the objects, right-click the selection, and click **Move**. To select multiple objects, press and hold **Ctrl**, then click each object.
> - To locate the object that you want to move, use the **Find** function of Active Roles. Once you found the accounts, open the **Move** dialog by right-clicking the object, and clicking **Move**.
> - The Console provides the drag-and-drop function for moving objects. To move objects, you can drag the selection from the details pane to a destination container in the **Console tree**.

Exporting and importing groups

With the Active Roles Console, you can export groups to an XML file and then import them from that file to populate a container in a different domain. The export and import operations provide a way to relocate groups between domains.

To export groups, select them, right-click the selection, and select **All Tasks** > **Export**. In the **Export Objects** dialog, specify the file where you want to save the data, and click **Save**.

To import groups, right-click the container where you want to place the groups, and then click **Import**. In the **Import Directory Objects** dialog, select the file to which the groups were exported, and click **Open**.

Deleting a group

You can delete Active Directory groups with the Active Roles Console.

To delete a group

1. In the **Console tree**, locate and select the folder that contains the group you want to delete.
2. In the details pane, right-click the group, then click **Delete**.

NOTE: Consider the following when deleting a group:

- Deleting a group is a destructive operation that cannot be undone. Once a group is deleted, all permissions and memberships associated with that group are lost. Creating a new group with the same name as the deleted group does not automatically assign the permissions and memberships of the previously deleted group. Instead, you must manually re-create all permissions and memberships.
- You can delete multiple objects at the same time by selecting the objects, right-clicking the selection, and clicking **Delete**. To select multiple objects, press and hold **Ctrl**, then click each object. If you select multiple objects, clicking **Delete** displays a dialog. To delete all the selected objects, select the **Apply to all items** check box, then click **Yes**.
- As the confirmation message indicates, you can also deprovision groups instead of deleting them. Deprovisioning refers to a set of Active Roles actions that prevents using the group. Active Roles comes with a default policy to automate some commonly-used deprovisioning tasks, and allows administrators to adjust the deprovision policies as needed.
- To deprovision a group, right-click the group in the details pane, and click **Deprovision**.
- To locate groups for deletion or deprovisioning, use the **Find** function of Active Roles. Once you found the groups, delete or deprovision them by selecting the accounts in the list of search results, right-clicking the selection, and clicking **Delete** or **Deprovision**.
- When attempting to delete an object, you may receive an error message that access is denied to the object. This can typically occur if the object is protected from deletion. To remove this protection, navigate to the **Properties** > **Object** tab of the object you want to delete, then clear the **Protect object from accidental deletion** check box. After that, try deleting the object again.

Deprovisioning a group

Active Roles provides the ability to deprovision rather than delete groups. Deprovisioning a groups refers to a set of actions that are performed by Active Roles to prevent the use of the group.

The **Deprovision** command on a group updates the group object in Active Directory as prescribed by the deprovisioning policies. Active Roles comes with a default policy to automate some commonly-used deprovisioning tasks, and allows the administrator to configure and apply additional policies.

You can deprovision Active Directory groups with the Active Roles Console.

To deprovision a group

1. In the **Console tree**, locate and select the folder that contains the group you want to deprovision.
2. In the details pane, right-click the group, then click **Deprovision**.
3. Wait while Active Roles updates the group.

> NOTE: Consider the following when deprovisioning a group:
>
> - You can deprovision multiple groups at a time. Select two or more groups, right-click the selection, then click **Deprovision**.
> - The **Deprovision** command is also available in the Active Roles Web Interface.
> - When you click the **Deprovision** command, the operation progress and results are displayed. When the operation is completed, Active Roles displays the operation summary, and allows you to examine operation results in detail.
> - On a deprovisioned group, you can use the **Deprovisioning Results** command to view a report that lists the actions taken during the deprovisioning operation. For each action, the report informs about success or failure of the action. In the event of a failure, the report provides a description of the error situation.
> - If a deprovisioned group needs to be restored (for example, if a group has been deprovisioned by mistake), the group can be reset to the state it was in before the deprovisioning occurred. This can be accomplished by using the **Undo Deprovisioning** command on the deprovisioned group.

Restoring a deprovisioned group

Active Roles provides the ability to restore deprovisioned groups. The purpose of this operation, referred to as the Undo Deprovisioning operation, is to roll back the changes that were made to a group by the Deprovision operation. When a deprovisioned group needs to be restored (for example, if a group has been deprovisioned by mistake), the Undo Deprovisioning operation allows the group to be restored to the state it was in before the changes were made.

You can restore previously deprovisioned Active Directory groups with the Active Roles Console.

To restore a deprovisioned group

1. In the **Console tree**, locate and select the folder that contains the group you want to restore.
2. In the details pane, right-click the group, then click **Undo Deprovisioning**.
3. Wait while Active Roles restores the group.
4. When you click the **Undo Deprovisioning** command, the operation progress and results are displayed. When the operation is completed, Active Roles displays the operation summary, and allows you to examine the operation results in detail. You can view a report that lists the actions taken during the restore operation. For each action, the report informs about success or failure of the action. In the event of a failure, the report provides a description of the error situation.

Administering a query-based distribution group

A query-based distribution group is a type of distribution group introduced in Exchange Server. The difference from the usual distribution group is that members of a query-based group are not statically placed into it. Email is propagated among the members of the group, but only among those of them who is currently in the state to comply with the specified LDAP query of this distribution group.

You can create new query-based distribution groups with the Active Roles Console.

To create a query-based distribution group

1. In the **Console tree**, right-click the folder in which you want to add the group, and select **New** > **Query-based Distribution Group**.
2. In **Query-based Distribution Group name**, type a name for the group, then click **Next**.
3. The box under **Apply filter to recipients in and below** displays the container to search for recipients. Click **Change** to select the container that contains the recipients you want the group to include.

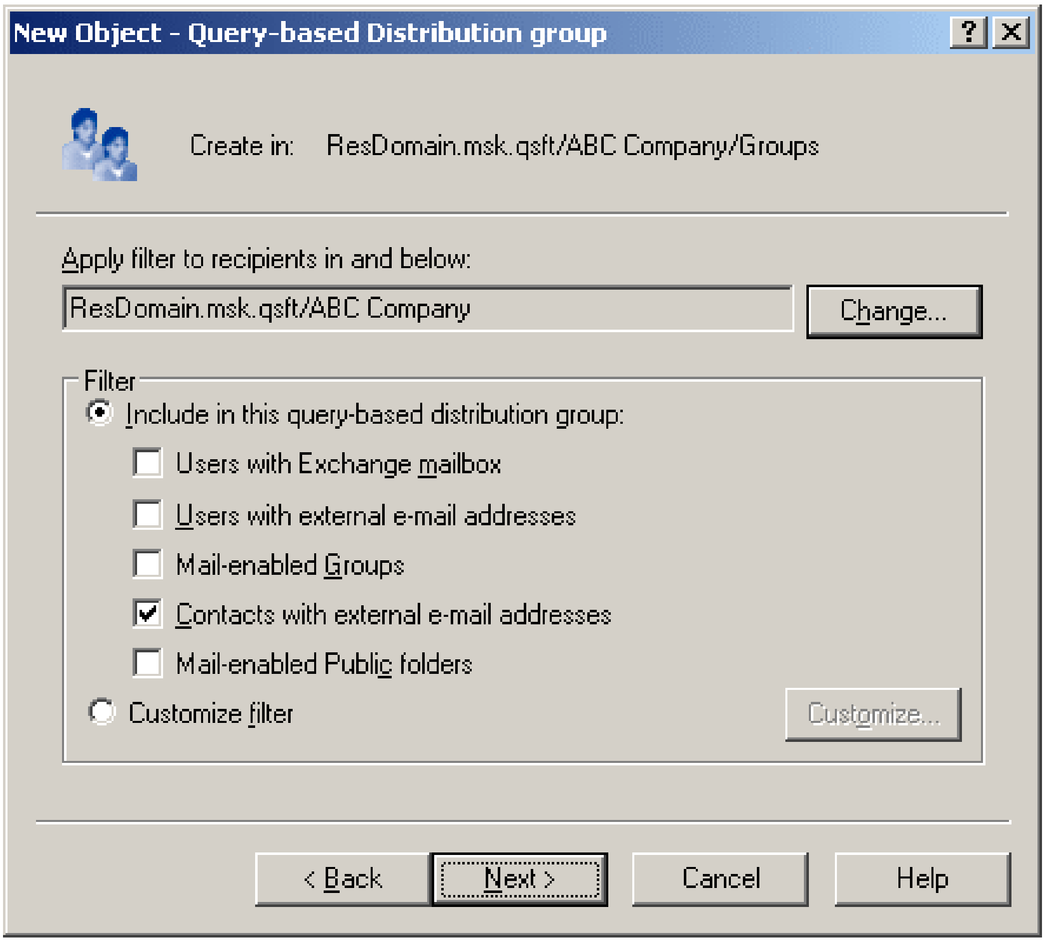
   > TIP: The query returns only recipients in the selected container and its sub-containers. To get the results you want, you may have to select a parent container or create multiple queries.

4. Under **Filter**, do one of the following:
   - Click **Include in this query-based distribution group**, then click each item you want to include in the criteria for membership in the query-based distribution group. The following criteria are pre-defined:

- **Users with Exchange mailbox**
- **Users with external e-mail addresses**
- **Mail-enabled Groups**
- **Contacts with external e-mail addresses**
- **Mail-enabled Public folders**

- To create your own criteria for the query, click **Customize filter** > **Customize.** This displays the **Custom Search** window where you can specify your search criteria.

Figure 18: Administering query-based distribution groups



New Object - Query-based Distribution group

Create in: ResDomain.msk.qsft/ABC Company/Groups

Apply filter to recipients in and below:

ResDomain.msk.qsft/ABC Company

Filter

● Include in this query-based distribution group:

□ Users with Exchange mailbox

□ Users with external e-mail addresses

□ Mail-enabled Groups

☑ Contacts with external e-mail addresses

□ Mail-enabled Public folders

○ Customize filter

5. Click **Next** to see a summary of the query-based distribution group you are about to create.
6. Click **Finish** to create the query-based distribution group. The new query-based distribution group is displayed in the details pane.
7. Right-click the query-based distribution group you just created and click **Properties**.

8. On the **Preview** tab, click **Start** to view the query results and verify that the correct recipients are included in the group.

> NOTE: Consider the following when administering a query-based distribution group:
>
> - A query-based distribution group provides the same functionality as a standard distribution group. However, instead of adding or removing members to or from the group manually, it is populated dynamically via an LDAP query. For example, you can configure a query-based distribution group to include all full-time employees of your organization.
> - When creating a query-based distribution group, One Identity recommends using the **Preview** button to:
>   - Verify the validity and the expected results of the query before applying it.
>   - Determining how long it takes for the query to run, allowing you to fine-tune the query or rework it into smaller queries to improve performance.
>
>   Specifying an LDAP filter string with bad formatting or an incorrect LDAP syntax will result in the query-based distribution group not working correctly. Also, if users send an email to an incorrectly configured query-based distribution group, they will receive a non-delivery report.

Administering dynamic (rule-based) groups

Active Roles can automatically keep group membership lists up to date, so that you do not need to add and remove members manually. To automate the maintenance of group membership lists, Active Roles uses the following features:

- A rule-based mechanism that automatically adds and removes objects to groups whenever object attributes change in Active Directory.
- Flexible membership criteria that enable both query-based and static group population.

In Active Roles, rules-based groups are referred to as dynamic groups. The groups that have no membership rules specified are referred to as basic groups. Any security or distribution group can be converted to a dynamic group by adding membership rules.

You can create a dynamic group by managing a basic group as follows: right-click the group, click **Convert to Dynamic Group**, select a rule type, and then configure a rule. For details, see *Adding a membership rule to a dynamic group* in the *Active Roles Administration Guide*.

When you convert a basic group to a dynamic group, the group loses all members that were added to the group when it was basic. This is because the membership list of a dynamic group is entirely under the control of membership rules.

Once membership rules are added to a group, the group only includes the objects that comply with the membership rules. Active Roles overrides any changes made directly to the membership list by any administrative tool.

> NOTE: In the Active Roles Console, dynamic groups are marked with this icon: . Also, a special note on the **General** tab makes it possible to distinguish between dynamic groups and basic groups when using administrative tools other than Active Roles.

For dynamic groups, the **Properties** dialog includes the **Membership Rules** tab. The **Members** tab for a dynamic group cannot be used to manage the membership list. It is only used to display a list of group members.

You can return a dynamic group to basic state as follows: right-click the group and click **Convert to Basic Group**. Then, click **Yes** to confirm the conversion. This operation removes all membership rules from the group. The group membership list remains intact as of the time of the conversion.

For more information about dynamic groups, refer to *Dynamic Groups* in the *Active Roles Administration Guide*.

Using temporal group memberships

By using temporal group memberships, you can manage group memberships of objects such as user or computer accounts that need to be members of particular groups for only a certain time period. This feature of Active Roles gives you flexibility in deciding and tracking what objects need group memberships and for how long.

This section guides you through the tasks of managing temporal group memberships in the Active Roles Console. If you are authorized to view and modify group membership lists, then you can add, view and remove temporal group members as well as view and modify temporal membership settings on group members.

Adding temporal members

A temporal member of a group is an object, such as a user, computer or group, scheduled to be added or removed from the group. You can add and configure temporal members using the Active Roles Console.

To add temporal members to a group

1. In the Active Roles Console, right-click the group, then click **Properties**.
2. On the **Members** tab in the **Properties** dialog, click **Add**.
3. In the **Select Objects** dialog, click **Temporal Membership Settings**.
4. In the **Temporal Membership Settings** dialog, choose the appropriate options, then click **OK**:

    - To have the temporal members added to the group on a certain date in the future, select **On this date** under **Add to the group**, and choose the date and time you want.
    - To have the temporal members added to the group at once, select **Now** under **Add to the group**.
    - To have the temporal members removed from the group on a certain date, select **On this date** under **Remove from the group**, and choose the date and time you want.
    - To retain the temporal members in the group for indefinite time, select **Never** under **Remove from the group**.

5. In the **Select Objects** dialog, type or select the names of the objects you want to make temporal members of the group, and click **OK**.
6. Click **Apply** in the **Properties** dialog for the group.

> NOTE: Consider the following when adding temporal members:
>
> - To add temporal members of a group, you must be delegated the authority to add or remove members from the group. The appropriate authority can be delegated by applying the **Groups - Add/Remove Members** Access Template.
> - You can also make an object a temporal member of a particular group (or groups) by modifying the properties of the object rather than the group(s). To do so, open the **Properties** dialog of the object, then click **Member Of** > **Add**. Finally, in the **Select Objects** dialog, specify the temporal membership settings and the name(s) of the group(s) in which you want to configure the temporal membership.

Viewing temporal members

The list of group members displayed by the Active Roles Console makes it possible to distinguish between regular group members and temporal group members. It is also possible to hide or display so-called pending members, the temporal members that are scheduled to be added to the group in the future but are not actual members of the group so far.

To view temporal members of a group

1. In the Active Roles Console, right-click the group, then click **Properties**.
2. Examine the list on the **Members** tab in the **Properties** dialog:
    - An icon of a small clock overlays the icon for the temporal members.
    - If the **Show pending members** check box is selected, the list also includes the temporal members that are not yet added to the group. The icons identifying such members are shown in orange.

The list of group memberships for a particular object makes it possible to distinguish between the groups in which the object is a regular member and the groups in which the object is a temporal member. It is also possible to hide or display so-called pending group memberships, the groups to which the object is scheduled to be added in the future.

To view groups in which an object is a temporal member

1. In the Active Roles Console, right-click the group, then click **Properties**.
2. Examine the list on the **Member Of** tab in the **Properties** dialog:
   - An icon of a small clock overlays the icon for the groups in which the object is a temporal member.
   - If the **Show pending group memberships** check box is selected, the list also includes the groups to which the object is scheduled to be added in the future. The icons identifying such groups are shown in orange.

Rescheduling temporal group memberships

The temporal membership settings on a group member include the start time and end time settings.

The start time setting specifies when the object is to be actually added to the group. This can be specific date and time or an indication that the object should be added to the group right away.

The end time setting specifies when the object is to be removed from the group. This can be specific date and time or an indication that the object should not be removed from the group.

You can view or modify both the start time and end time settings using the Active Roles Console.

To view or modify the start or end time setting for a member of a group

1. In the Active Roles Console, right-click the group, then click **Properties**.
2. In the list on the **Members** tab in the **Properties** dialog, click the member and then click **Temporal Membership Settings**.
3. Use the **Temporal Membership Settings** dialog to view or modify the start or end time settings.

The **Temporal Membership Settings** dialog provides the following options:

- **Add to the group** > **Now**: Indicates that the object should be added to the group at once.
- **Add to the group** > **On this date**: Indicates the date and time when the object should be added to the group.
- **Remove from the group** > **Never**: Indicates that the object should not be removed from the group.
- **Remove from the group** > **On this date**: Indicates the date and time when the object should be removed from the group.

Regular members have the **Add to group** and **Remove from group** options set to `Already added` and `Never`, respectively. You can set a particular date for any of these options in order to convert a regular member to a temporal member.

NOTE: Consider the following when rescheduling temporal group memberships:

- You can view or modify the start time and end time settings by managing an object rather than groups in which the object has memberships. Open the **Properties** dialog for that object, and on the **Member Of** tab, select the group for which you want to manage the object's start or end time setting and click **Temporal Membership Settings**.
- On the **Members** or **Member Of** tab, you can change the start or end time setting for multiple members or groups at a time. From the list on the tab, select two or more items and click **Temporal Membership Settings**. Then, in the **Temporal Membership Settings** dialog, select check boxes to indicate the settings to change and make the changes you want.

Removing temporal members

You can remove temporal group members in the same way as regular group members. Removing a temporal member of a group deletes the temporal membership settings for that object with respect to that group. As a result, the object will not be added to the group. If the object already belongs to the group at the time of removal, then it is removed from the group.

To remove a temporal member of a group

1. In the Active Roles Console, right-click the group, then click **Properties**.
2. On the **Members** tab in the **Properties** dialog, click the member, click **Remove**, then click **Apply**.

NOTE: You can remove an object that is a temporal member of a group by managing the object rather than the group. Open the **Properties** dialog for that object, and on the **Member Of** tab, select the group from the list and click **Remove**.

5

Computer account management

Computer accounts are Active Directory objects used to represent physical computers. Computer accounts allow computers to join the domain, and control their access to resources on the network. The operating system uses computer account information to determine access permissions for a computer.

Active Roles provides the facility to perform administrative tasks such as create, modify, and delete computer accounts. Active Roles can also be used to disable and enable accounts, add and remove accounts from groups, and reset accounts.

The following section describes how to use the Active Roles Console to manage computer accounts. You can also use the Active Roles Web Interface to perform management tasks on computer accounts.

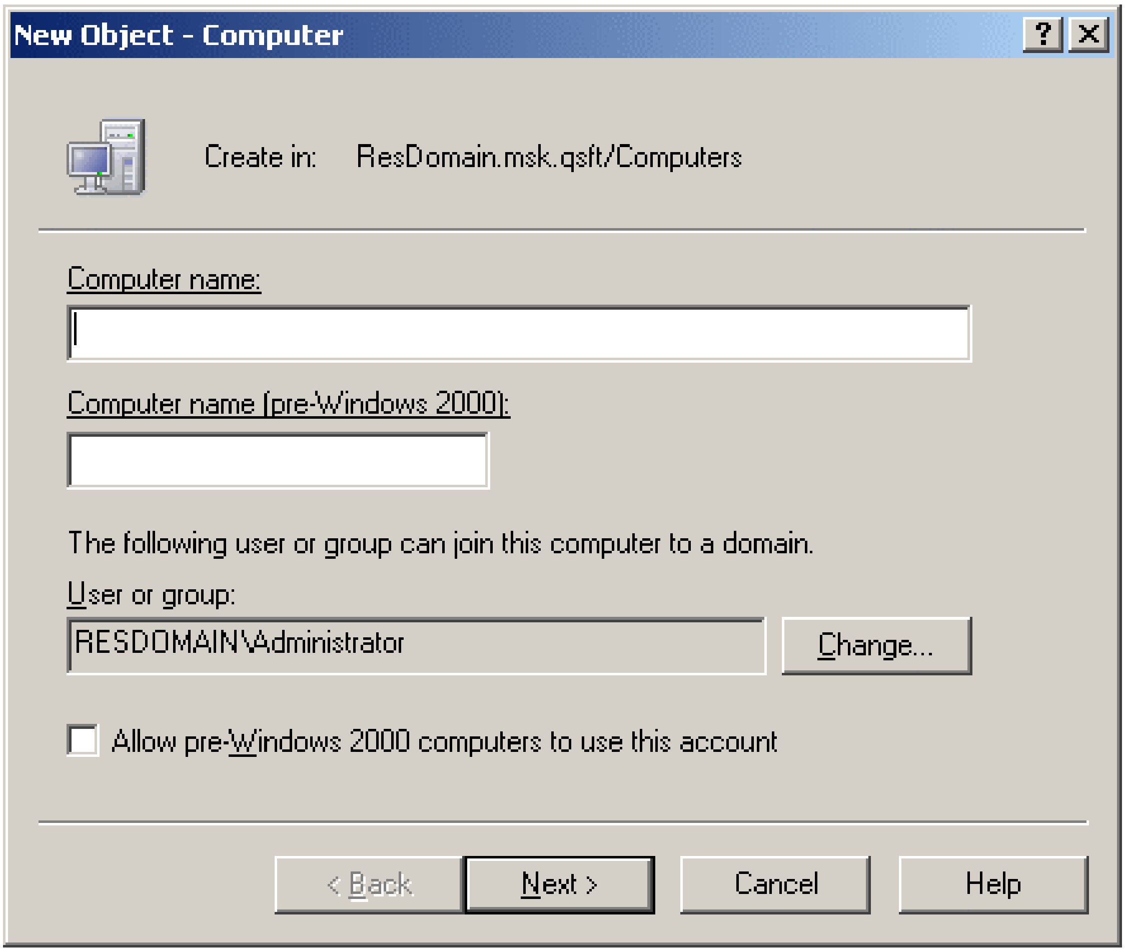
Creating a computer account

You can create new computer accounts with the Active Roles Console.

To create a computer account

1. In the **Console tree**, locate and select the folder in which you want to add the computer account.
2. Right-click the folder, point to **New** and click **Computer** to start the **New Object - Computer** wizard.
3. Follow the wizard pages to specify properties of the new computer account, such as the computer name and pre-Windows 2000 computer name.

Figure 19: Creating a computer account



New Object - Computer

Create in: ResDomain.msk.qsft/Computers

Computer name:

Computer name (pre-Windows 2000):

The following user or group can join this computer to a domain.

User or group: RESDOMAIN\Administrator

□ Allow pre-Windows 2000 computers to use this account

4. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the wizard.
5. After setting any additional properties, click **Finish** on the completion page of the wizard.

NOTE: Consider the following when creating a computer account:

- In the wizard, some property labels may be displayed as hyperlinks. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed. For more information, see Getting policy-related information.

  The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.

- Normally, the rights of a domain administrator are required to join a computer to the domain through the use of an existing, newly created computer account. If you want to authorize a certain user or group to perform this task, you can do so when creating the computer account: Under **The following user or group can join this computer to a domain**, click **Change**, then select the user or group you want.

- If the computer to be associated with the computer account you are creating is running a pre-Windows 2000 operating system, select the **Allow pre-Windows 2000 computers to use this account** check box.

Finding a computer account

To find a computer account, right-click the container you want to search and click **Find**. In the **Find** window, select **Computers** from the **Find** list, specify your search criteria, and start the search. In the search results list, you can right-click computer accounts and use commands on the shortcut menu to perform management tasks.

For step-by-step instructions on how to search for computer accounts, see Searching for a computer.

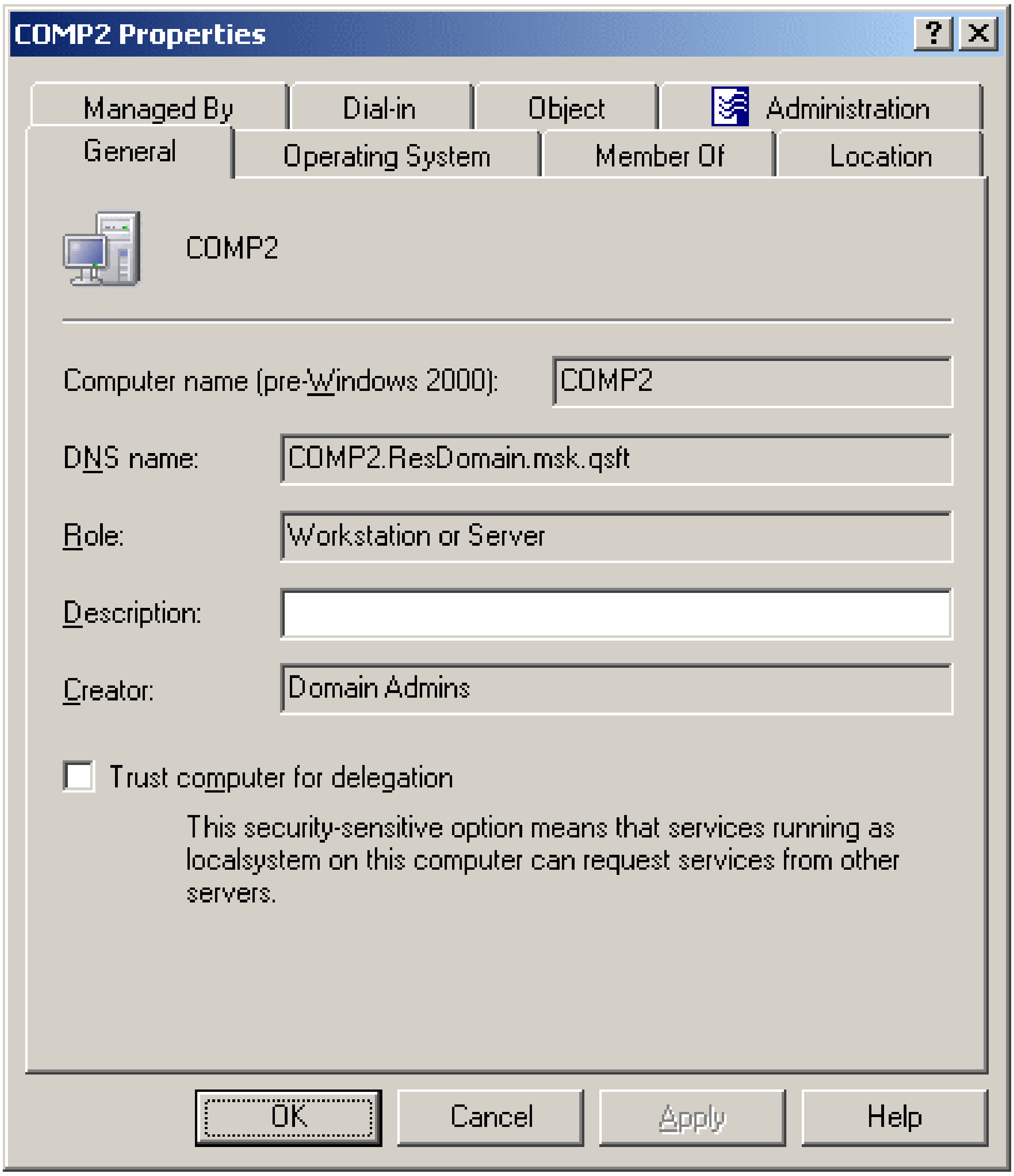
Modifying computer account properties

You can modify the properties of computer accounts with the Active Roles Console.

To modify computer account properties

1. In the **Console tree**, locate and select the folder that contains the computer account that you want to modify.
2. In the details pane, right-click the computer account you want to modify, then click **Properties**.
3. Use the tabs in the **Properties** dialog to view or modify properties of the computer account.

Figure 20: Properties



COMP2 Properties

COMP2

Computer name (pre-Windows 2000): COMP2

DNS name: COMP2.ResDomain.msk.qsft

Role: Workstation or Server

Description:

Creator: Domain Admins

□ Trust computer for delegation

This security-sensitive option means that services running as localsystem on this computer can request services from other servers.

4. If you want to view or modify additional properties (those for which the tabs in the **Properties** dialog do not provide data entries), navigate to the **Object** tab and click **Advanced Properties**.
5. After setting all the properties you want, click **OK**.

NOTE: Consider the following when modifying object properties:

- In the wizard, some property labels may be displayed as hyperlinks. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed. For more information, see Getting policy-related information.

The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.

- To modify properties for multiple objects, press and hold **Ctrl**, then click each object. Right-click the selection, then click **Properties**.
- You can use the **Properties** dialog to view or modify any property of the object by navigating to the **Object** tab and clicking **Advanced Properties**. In the **Advanced Properties** window you can manage all properties, including those that cannot be accessed via the **Properties** dialog itself.

  You can also display the **Advanced Properties** window by right-clicking the object and selecting **All Tasks** > **Advanced Properties**.
- To locate the object that you want to modify, use the **Find** function of Active Roles. Once you found the object, open the **Properties** page by right-clicking the object, and clicking **Properties**.

Blocking and unblocking a computer account

A computer account can be blocked as a security measure to prevent users from logging on to the computer, instead of deleting the computer account.

You can block and unblock computer accounts with the Active Roles Console.

To block a computer account

1. In the **Console tree**, locate and select the folder that contains the computer account you want to block.
2. In the details pane, right-click the computer account and click **Disable Account**.

NOTE: Consider the following when blocking a computer account:

- When you block a computer account, the computer cannot authenticate to the domain until the account has been unblocked.
- The **Disable Account** command is displayed if the account is unblocked; otherwise, the **Enable Account** command is displayed on the menu. By using the **Enable Account** command you can change the status of the blocked account.

The **Enable Account** option appears only for blocked computer accounts. Blocked computer accounts are marked with the icon.

To unblock a blocked computer account

1. In the **Console tree**, locate and select the folder that contains the computer account you want to unblock.
2. In the details pane, right-click the computer account and click **Enable Account**.

> NOTE: The **Enable Account** command appears if the account is blocked; otherwise, the **Disable Account** command appears on the menu.

Resetting a computer account

A computer account is normally reset if the computer has been taken offline and completely reinstalled. Resetting the account allows the (rebuilt) computer to rejoin the domain using the same name. If the computer account is reset whenever the computer has not been reinstalled, the computer cannot authenticate in the domain.

To reset a computer account, right-click the account, and click **Reset Account**. This command resets the computer account password.

> NOTE: You cannot reset the password of Domain Controllers (DCs) with the **Reset Account** command.

Adding a computer account to a group

You can add Active Directory computer accounts to a group with the Active Roles Console.

To add a computer account to a group

1. In the **Console tree**, locate and select the folder that contains the computer account you want to add to a group.
2. In the details pane, right-click the object, then click **Add to a Group**.
3. Use the **Select Objects** dialog to locate and select the group to which you want to add the computer account (you can select more than one group).

> NOTE: Consider the following when adding an object to a group:
>
> - In the **Select Objects** dialog, you can select groups from the list or type group names, separating them with semicolons. Click **Check Names** to verify the names you type. If Active Roles cannot find a group, it prompts you to correct the name.
> - You can add multiple objects to a group at a time: Select the objects, right-click the selection, and click **Add to a Group**. To select multiple objects, press and hold down **Ctrl**, then click each object.
>
>   When you select multiple objects, the **Member Of** tab lists the groups to which all the selected objects belong. If one of the objects does not belong to a given group, that group does not appear in the list.

- You can also add or remove objects from groups by using the **Properties** dialog: Select one or more objects, right-click the selection, click **Properties**, and go to the **Member Of** tab in the **Properties** dialog.
- On the **Member Of** tab, you can manage groups directly from the list of groups. To manage a group, right-click it, and use commands on the shortcut menu.
- The **Member Of** tab lists the groups to which the object belongs. If the **Show nested groups** check box is selected, the list also includes the groups to which the object belongs owing to group nesting.
- You can also add the object to groups by clicking **Add** on the **Member Of** tab. This displays the **Select Objects** dialog, allowing you to select the groups to which you want to add the object.
- The **Temporal Membership Settings** button can be used to specify the date and time when the object should be added or removed from the selected groups. For more information about this feature, see Using temporal group memberships.
- By adding an object to a group, you can assign permissions to all of the objects in that group and filter Group Policy settings on all objects in that group.
- To locate objects you want to add to a certain group, use the **Find** function of Active Roles. Once you found the objects, select the accounts in the list of search results, right-click the selection, and click **Add to a Group**.

Removing a computer account from a group

You can remove computer accounts from Active Directory groups with the Active Roles Console.

To remove a computer account from a group

1. In the **Console tree**, locate and select the folder that contains the computer account you want to remove from a group.
2. In the details pane, right-click the computer account, then click **Properties**.
3. On the **Member Of** tab in the **Properties** dialog, clear the **Show nested groups** check box, select the group from which you want to remove the computer account, and click **Remove**.

NOTE: Consider the following when removing an object from a group:

- If you have not cleared the **Show nested groups** check box, the list on the **Member Of** tab also includes the groups to which the object belongs indirectly, that is, because of group nesting. If you select such a group from the list, the **Remove** button is unavailable. An object can be removed only from those groups of which the object is a direct member.

- You cannot remove objects from their primary groups. Instead, you can change the primary group of an object. To do so, on the **Member Of** tab, select a different group from the list, then click **Set Primary Group**.

Moving a computer account

You can move computer accounts from one Active Directory container to another with the Active Roles Console.

To move a computer account

1. In the **Console tree**, locate and select the folder that contains the computer account you want to move.
2. In the details pane, right-click the computer account and click **Move** to display the **Move** dialog.
3. In the **Move** dialog, select the folder to which you want to move the computer account, then click **OK**.

NOTE: Consider the following when moving an object:

- With Active Roles, directory objects can only be moved within the same domain. This means that the folder to which you want to move the object must belong to the same domain as the object.
- You can move multiple objects at a time with the **Move** dialog. To open the dialog, select the objects, right-click the selection, and click **Move**. To select multiple objects, press and hold **Ctrl**, then click each object.
- To locate the object that you want to move, use the **Find** function of Active Roles. Once you found the accounts, open the **Move** dialog by right-clicking the object, and clicking **Move**.
- The Console provides the drag-and-drop function for moving objects. To move objects, you can drag the selection from the details pane to a destination container in the **Console tree**.

Exporting and importing a computer account

With the Active Roles Console, you can export computer accounts to an XML file and then import them from that file to populate a container in a different domain. The export and import operations provide a way to relocate computer accounts between domains.

To export computer accounts, select them, right-click the selection, and select **All Tasks** > **Export**. In the **Export Objects** dialog, specify the file where you want to save the data, and click **Save**.

To import computer accounts, right-click the container where you want to place the accounts, and then click **Import**. In the **Import Directory Objects** dialog, select the file to which the computer accounts were exported, and click **Open**.

Deleting a computer account

You can delete Active Directory computer accounts with the Active Roles Console.

To delete a computer account

1. In the **Console tree**, locate and select the folder that contains the computer account you want to delete.
2. In the details pane, right-click the computer account, then click **Delete**.

> NOTE: Consider the following when deleting a computer account:
>
> - Deleting an account is a destructive operation that cannot be undone. Once an account is deleted, the permissions and memberships associated with that account are also permanently deleted. Because the security ID (SID) for each account is unique, a new account with the same name as the previously deleted account does not automatically receive the permissions and memberships that the previously deleted account had. To duplicate a deleted account, you must recreate all permissions and memberships manually.
> - You can delete multiple objects at the same time by selecting the objects, right-clicking the selection, and clicking **Delete**. To select multiple objects, press and hold **Ctrl**, then click each object. If you select multiple objects, clicking **Delete** displays a dialog. To delete all the selected objects, select the **Apply to all items** check box, then click **Yes**.
> - To locate the objects for deletion, use the **Find** function of Active Roles. Once you found the objects, delete them by selecting the objects in the list of search results, right-clicking the selection, and clicking **Delete**.
> - When attempting to delete an object, you may receive an error message that access is denied to the object. This can typically occur if the object is protected from deletion. To remove this protection, navigate to the **Properties** > **Object** tab of the object you want to delete, then clear the **Protect object from accidental deletion** check box. After that, try deleting the object again.

Managing a remote computer

The Active Roles Console allows you to open the Computer Management console from which you can administer a remote computer. Computer Management combines several administration utilities into a single console, providing easy access to the computer’s administrative properties and tools. You must have administrative rights on the computer to view certain information or to modify computer properties using Computer Management.

To manage a remote computer

1. In the **Console tree**, locate and select the folder that contains the computer account of the computer you want to manage.
2. In the details pane, right-click the computer account, then click **Manage** to open the Computer Management console.

> NOTE: To locate the computer account of the computer you want to manage, use the **Find** function of Active Roles. Once you found the computer account, right-click the computer account in the list of search results, then click **Manage**.

Using a remote desktop connection

From the Active Roles Console, you can access a computer through Remote Desktop Connection. The **Connect via RDP** command on a computer object allows you to establish a Remote Desktop Connection session to the computer represented by that computer object in Active Directory.

By supporting Remote Desktop Connection, Active Roles enables you to access a remote computer from your computer running the Active Roles Console. However, the object representing the remote computer must be available in the Console. This requires that the remote computer be a member of one of the domains managed by Active Roles. Additionally, the commonly-known requirements must be met that apply to Remote Desktop Connection: The remote computer must have Remote Desktop enabled, it must be available on the network, and it must be configured so that the user has permission to connect.

To access a computer through Remote Desktop Connection

1. In the Active Roles Console, locate the desired computer object.
2. Right-click the computer object and click **Connect via RDP**.

Viewing BitLocker recovery passwords

Active Roles allows you to locate and view BitLocker recovery passwords that are stored in Active Directory. This tool helps to recover data on a drive that has been encrypted by using BitLocker. You can examine a computer object’s property pages to view the corresponding BitLocker recovery passwords. Additionally, you can perform a domain-wide search for a BitLocker recovery password.

Administrators can configure BitLocker Drive Encryption to back up recovery information for BitLocker-protected drives to Active Directory. Recovery information includes the recovery password for each BitLocker-protected drive, and the information required to identify which computers and drives the recovery information applies to. Backing up recovery passwords for BitLocker-protected drives allows administrators to recover the drive if it is locked, thereby ensuring that authorized persons can always access encrypted data belonging to the enterprise.

To view BitLocker recovery passwords, you must have been granted the appropriate permissions in Active Roles. The following Access Template provides sufficient permissions to view BitLocker recovery passwords:

- Computer Objects - View BitLocker Recovery Keys
- In addition, viewing BitLocker recovery passwords in a given Active Directory domain requires the following:
  - The domain must be configured to store BitLocker recovery information. For more information, see Backing Up BitLocker and TPM Recovery Information to AD DS.
  - The computers protected by BitLocker must be joined to the domain.
  - BitLocker Drive Encryption must have been enabled on the computers.

The following procedures describe the most common tasks that apply to locating and viewing BitLocker recovery passwords.

To view the BitLocker recovery passwords for a computer

1. In the Active Roles Console, locate the desired computer object.
2. Right-click the computer object, then click **Properties**.
3. In the **Properties** dialog, click the **BitLocker Recovery** tab to view the BitLocker recovery passwords that are associated with the computer you selected.

To copy the BitLocker recovery password for a computer

1. Follow the steps in the previous procedure to view the BitLocker recovery passwords.
2. On the **BitLocker Recovery** tab of the **Properties** dialog, perform the following steps:
   a. In the **BitLocker Recovery Passwords** list, click the desired password ID.
   b. Right-click in the **Details** box, click **Select All**, then click **Copy**.
3. Press **Ctrl+V** to paste the copied text to a destination location, such as a text file or spreadsheet.

You can use the Active Roles Web Interface to view the BitLocker recovery passwords for a computer. To do so, select the computer object, then choose the **BitLocker Recovery** command.

To locate a BitLocker recovery password

1. In the Active Roles Console or Web Interface, select the domain object, then choose the **Find BitLocker Recovery Password** command.
2. On the **Find BitLocker Recovery Password** page, type the first eight characters of the BitLocker recovery key identification in the **Password ID (first 8 characters)** box, then click **Search**.

You can also search for a BitLocker recovery password in all managed domains by choosing the **Find BitLocker Recovery Password** command on the **Active Directory** node in the Active Roles Console or Web Interface.

6

Organizational Unit management

Organizational Units (OUs) are containers in Active Directory. OUs can contain user accounts, groups, computer accounts, and other OUs. An object can be included in only one OU.

When you expand the **Active Directory** node in the Active Roles Console, the Console tree displays icons representing domains. You can double-click a domain icon to see containers that are defined in the domain. OUs are marked with the following icon: 📁

When you select an OU in the **Console tree**, the details pane lists objects included in the OU, and the **Action** menu provides commands to create new objects in the OU, search for objects in the OU, and manage OU properties.

The following section guides you through the Active Roles Console to manage Organizational Units. You can also use the Active Roles Web Interface to perform management tasks on Organizational Units.

Creating an Organizational Unit

You can create new Active Directory Organizational Units (OUs) with the Active Roles Console.

To create an Organizational Unit

1. In the **Console tree**, locate and select the folder in which you want to add the OU.
2. Right-click the folder, point to **New** and click **Organizational Unit** to start the **New Object - Organizational Unit** wizard.
3. (Optional) Select the **Protect container from accidental deletion** check box.
4. Follow the wizard pages to specify properties of the new OU, such as the name of the OU.
5. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the wizard.

6. After setting any additional properties, click **Finish** on the completion page of the wizard.

> NOTE: Consider the following when creating an Organizational Unit:
>
> - To create an OU, you can also click the domain node or folder in which you want to add the OU, then click 📁 on the toolbar.
> - By selecting the **Protect container from accidental deletion** check box you ensure that the newly created OU cannot be deleted, whether using Active Roles or other tools for Active Directory administration. When somebody attempts to delete an OU for which this check box is selected, the operation returns an error indicating that access is denied. For an existing OU, you can view or change this setting on the **Object** tab in the **Properties** dialog.

Finding an Organizational Unit

To find an Organizational Unit, select the domain you want to search, and click **Find**. In the **Find** window, select **Organizational Units** from the **Find** list, specify your search criteria, and start the search. In the search results list, you can right-click Organizational Units and use commands on the shortcut menu to perform management tasks.

For step-by-step instructions on how to search for Organizational Units, see Searching for an Organizational Unit.

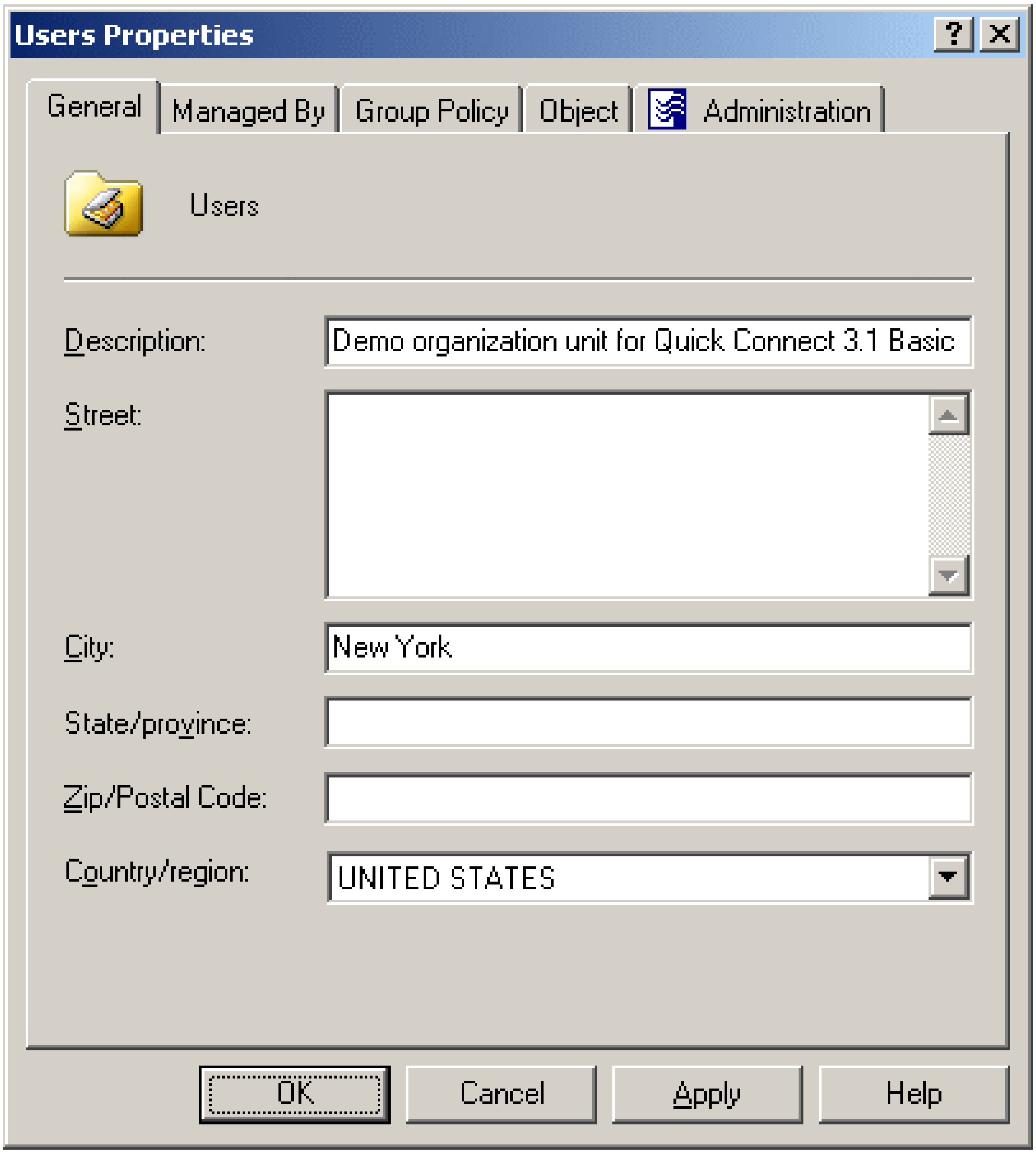
Modifying Organizational Unit properties

You can modify the properties of Active Directory Organizational Units (OUs) with the Active Roles Console.

To modify Organizational Unit properties

1. In the **Console tree**, locate the OU you want to modify.
2. Right-click the OU, then click **Properties**.

Figure 21: Modifying Organizational Unit properties



Description: Demo organization unit for Quick Connect 3.1 Basic

Street:

City: New York

State/province:

Zip/Postal Code:

Country/region: UNITED STATES

3. Use the tabs in the **Properties** dialog to view or modify properties of the OU.
4. If you want to view or modify additional properties (those for which the tabs in the **Properties** dialog do not provide data entries), navigate to the **Object** tab and click **Advanced Properties**.
5. After setting all the properties you want, click **OK**.

NOTE: Consider the following when modifying object properties:

- In the wizard, some property labels may be displayed as hyperlinks. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed. For more information, see Getting policy-related information.

The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.

- To modify properties for multiple objects, press and hold **Ctrl**, then click each object. Right-click the selection, then click **Properties**.
- You can use the **Properties** dialog to view or modify any property of the object by navigating to the **Object** tab and clicking **Advanced Properties**. In the **Advanced Properties** window you can manage all properties, including those that cannot be accessed via the **Properties** dialog itself.

  You can also display the **Advanced Properties** window by right-clicking the object and selecting **All Tasks** > **Advanced Properties**.
- To locate the object that you want to modify, use the **Find** function of Active Roles. Once you found the object, open the **Properties** page by right-clicking the object, and clicking **Properties**.

Renaming an Organizational Unit

You can rename Active Directory Organizational Units (OUs) with the Active Roles Console.

To rename an Organizational Unit

1. In the **Console tree**, locate the OU you want to rename.
2. Right-click the OU, then click **Rename**.
3. Type a new name, then press **Enter**.

NOTE: Consider the following when renaming an object:

- The behavior of the dialog may vary depending on the configuration of Active Roles policies. To determine whether a given item in the dialog is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the dialog. For more information, see Getting policy-related information.
- To locate the object you want to rename, use the **Find** function of Active Roles. Once you found the object, rename it by selecting it in the list of search results, right-clicking it, clicking **Rename**, then specifying the new name. To apply the new name, press **Enter**.

Moving an Organizational Unit

You can move Organizational Units (OUs) from one Active Directory container to another with the Active Roles Console.

To move an Organizational Unit

1. In the **Console tree**, locate and select the folder that contains the OU you want to move.
2. In the details pane, right-click the OU and click **Move** to display the **Move** dialog.
3. In the **Move** dialog, select the folder to which you want to move the OU, then click **OK**.

> NOTE: Consider the following when moving an object:
>
> - With Active Roles, directory objects can only be moved within the same domain. This means that the folder to which you want to move the object must belong to the same domain as the object.
> - You can move multiple objects at a time with the **Move** dialog. To open the dialog, select the objects, right-click the selection, and click **Move**. To select multiple objects, press and hold **Ctrl**, then click each object.
> - To locate the object that you want to move, use the **Find** function of Active Roles. Once you found the accounts, open the **Move** dialog by right-clicking the object, and clicking **Move**.
> - The Console provides the drag-and-drop function for moving objects. To move objects, you can drag the selection from the details pane to a destination container in the **Console tree**.

Deleting an Organizational Unit

You can delete Active Directory Organizational Units (OUs) with the Active Roles Console.

To delete an Organizational Unit

1. In the **Console tree**, locate the OU you want to delete.
2. Right-click the Organizational Unit, and click **Delete**.

> NOTE: Consider the following when deleting an Organizational Unit:
>
> - If the selected OU contains any objects, the Active Roles Console will prompt you to confirm the deletion of those objects. You can either cancel or confirm the deletion of the OU along with every object it contains.
> - You can delete multiple objects at the same time by selecting the objects, right-clicking the selection, and clicking **Delete**. To select multiple objects, press and

hold **Ctrl**, then click each object. If you select multiple objects, clicking **Delete** displays a dialog. To delete all the selected objects, select the **Apply to all items** check box, then click **Yes**.

- When attempting to delete an object, you may receive an error message that access is denied to the object. This can typically occur if the object is protected from deletion. To remove this protection, navigate to the **Properties** > **Object** tab of the object you want to delete, then clear the **Protect object from accidental deletion** check box. After that, try deleting the object again.

Contact management

A contact is an Active Directory object that holds email and telephone information about an individual, without giving that person a security account on the network.

Contacts do not have a security identifier, unlike user accounts and groups. Contacts are used to add members to distribution lists or groups without granting them access to network resources.

You can use Active Roles to create, modify, and delete contacts. You can also perform Exchange-related tasks such as establishing email addresses for contacts.

The following section describes how to use the Active Roles Console to manage contacts. You can also use the Active Roles Web Interface to perform contact management tasks.

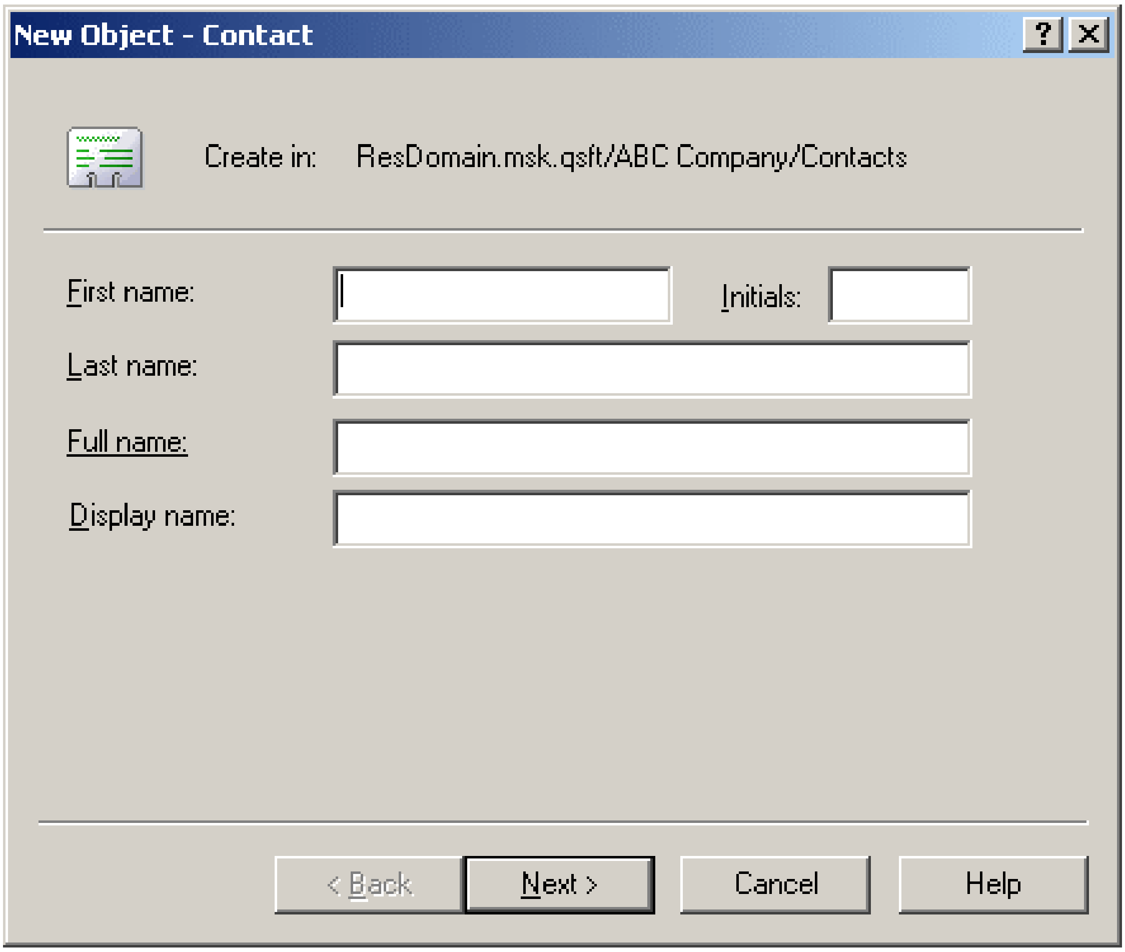
Creating a contact

You can create new Active Directory contacts with the Active Roles Console.

To create a contact

1. In the **Console tree**, locate and select the folder in which you want to add the contact.
2. Right-click the folder, point to **New** and click **Contact** to start the **New Object - Contact** wizard.
3. Follow the wizard pages to specify properties of the new contact, such as the contact’s first name, last name, full name, display name, and Exchange email address settings.

Figure 22: Creating a contact


New Object - Contact

Create in: ResDomain.msk.qsft/ABC Company/Contacts

First name:

Initials:

Last name:

Full name:

Display name:

4. If you want to set values for additional properties (those for which the wizard pages do not provide data entries), click **Edit Attributes** on the completion page of the wizard.
5. After setting any additional properties, click **Finish** on the completion page of the wizard.

NOTE: In the wizard, some property labels may be displayed as hyperlinks. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed. For more information, see Getting policy-related information.

Finding a contact

To find a contact, right-click the container you want to search and click **Find**. In the **Find** window, select **Contacts** from the **Find** list, specify your search criteria, and start the search. In the search results list, you can right-click contacts and use commands on the shortcut menu to perform management activities.

For step-by-step instructions on how to search for contacts, see Searching for a user, contact, or group.

Modifying contact properties

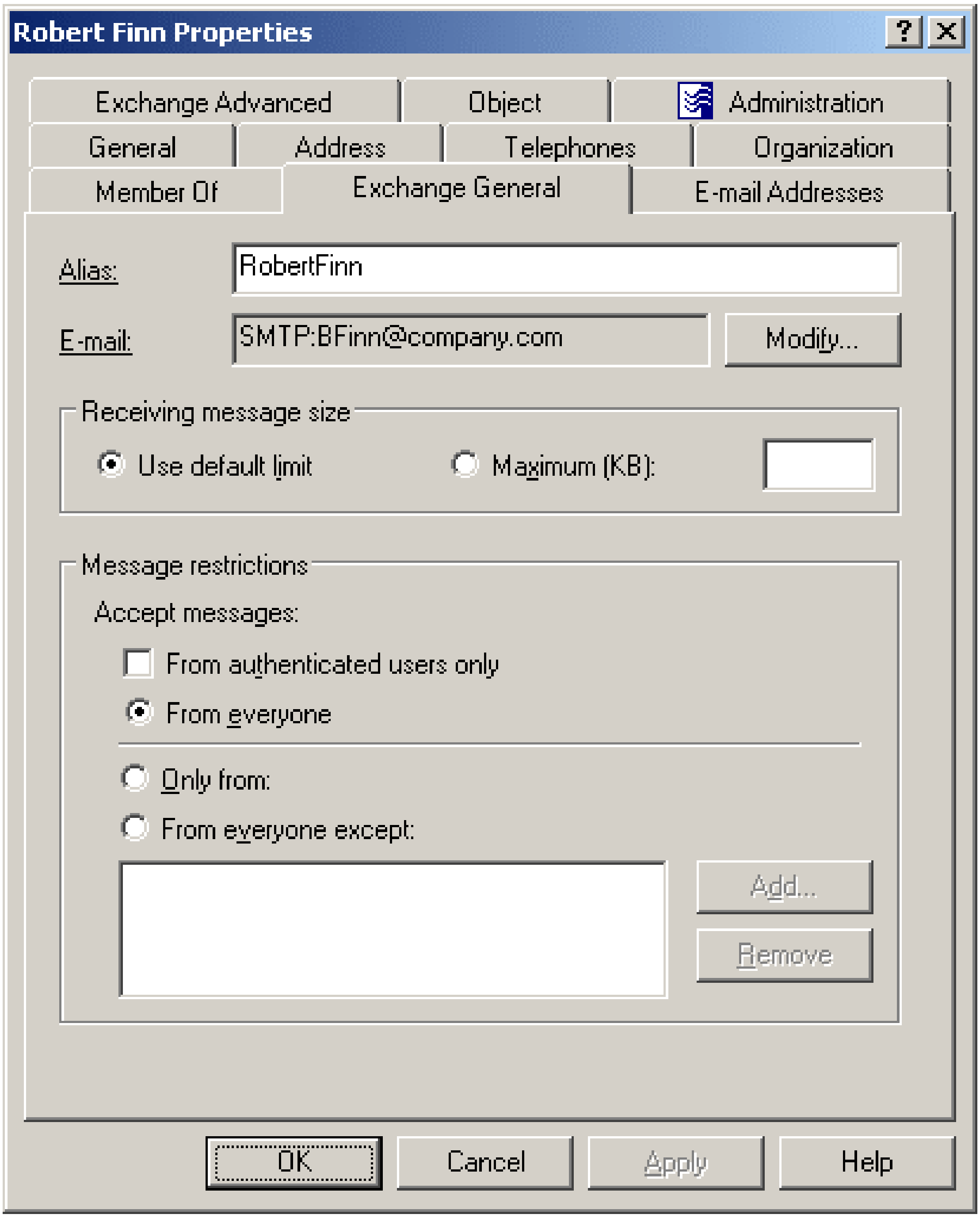
You can modify the properties of Active Directory contacts with the Active Roles Console.

To modify contact properties

1. In the **Console tree**, locate and select the folder that contains the contact you want to modify.
2. In the details pane, right-click the contact you want to modify, then click **Properties**.
3. Use the tabs in the **Properties** dialog to view or modify properties of the contact.
4. If you want to view or modify additional properties (those for which the tabs in the **Properties** dialog do not provide data entries), navigate to the **Object** tab and click **Advanced Properties**.
5. After setting all the properties you want, click **OK**.

> NOTE: Consider the following when modifying object properties:
>
> - In the wizard, some property labels may be displayed as hyperlinks. The hyperlink indicates that Active Roles enforces certain policy restrictions on the property. To examine policy details, click the hyperlink: the policy information is displayed. For more information, see Getting policy-related information.
>
>   The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.
> - To modify properties for multiple objects, press and hold **Ctrl**, then click each object. Right-click the selection, then click **Properties**.
> - You can use the **Properties** dialog to view or modify any property of the object by navigating to the **Object** tab and clicking **Advanced Properties**. In the **Advanced Properties** window you can manage all properties, including those that cannot be accessed via the **Properties** dialog itself.
>
>   You can also display the **Advanced Properties** window by right-clicking the object and selecting **All Tasks** > **Advanced Properties**.
> - To locate the object that you want to modify, use the **Find** function of Active Roles. Once you found the object, open the **Properties** page by right-clicking the object, and clicking **Properties**.

Figure 23: Modifying contact properties



Alias: RobertFinn

E-mail: SMTP:BFinn@company.com

Receiving message size

● Use default limit ○ Maximum (KB):

Message restrictions

Accept messages:

□ From authenticated users only

● From everyone

○ Only from:

○ From everyone except:

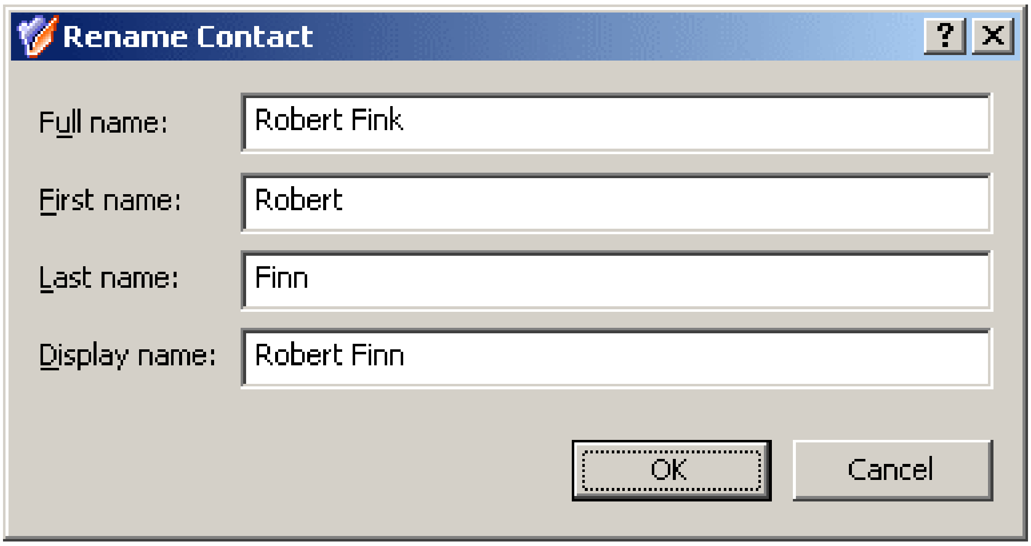
Renaming a contact

You can rename Active Directory contacts with the Active Roles Console.

To rename a contact

1. In the **Console tree**, locate and select the folder that contains the contact you want to rename.
2. In the details pane, right-click the contact and click **Rename**.
3. Type a new name (or clear the existing name), then press **Enter** to display the **Rename User** dialog.

   Figure 24: Rename Contact

   Rename Contact

   Full name: Robert Fink

   First name: Robert

   Last name: Finn

   Display name: Robert Finn

4. Use the **Rename Contact** dialog to modify (if needed) the naming properties of the user account such as the user full name, first name, last name, display name.
5. When finished, click **OK**.

> NOTE: Consider the following when renaming an object:
>
> - The behavior of the dialog may vary depending on the configuration of Active Roles policies. To determine whether a given item in the dialog is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the dialog. For more information, see Getting policy-related information.
> - To locate the object you want to rename, use the **Find** function of Active Roles. Once you found the object, rename it by selecting it in the list of search results, right-clicking it, clicking **Rename**, then specifying the new name. To apply the new name, press **Enter**.

Adding a contact to a group

You can add Active Directory contacts to a group with the Active Roles Console.

To add a contact to a group

1. In the **Console tree**, locate and select the folder that contains the contact you want to add to a group.
2. In the details pane, right-click the contact, then click **Add to a Group**.
3. Use the **Select Objects** dialog to locate and select the group to which you want to add the contact (you can select more than one group).

> NOTE: Consider the following when adding an object to a group:
>
> - In the **Select Objects** dialog, you can select groups from the list or type group names, separating them with semicolons. Click **Check Names** to verify the names you type. If Active Roles cannot find a group, it prompts you to correct the name.
> - You can add multiple objects to a group at a time: Select the objects, right-click the selection, and click **Add to a Group**. To select multiple objects, press and hold down **Ctrl**, then click each object.
>
>   When you select multiple objects, the **Member Of** tab lists the groups to which all the selected objects belong. If one of the objects does not belong to a given group, that group does not appear in the list.
> - You can also add or remove objects from groups by using the **Properties** dialog: Select one or more objects, right-click the selection, click **Properties**, and go to the **Member Of** tab in the **Properties** dialog.
> - On the **Member Of** tab, you can manage groups directly from the list of groups. To manage a group, right-click it, and use commands on the shortcut menu.
> - The **Member Of** tab lists the groups to which the object belongs. If the **Show nested groups** check box is selected, the list also includes the groups to which the object belongs owing to group nesting.
> - You can also add the object to groups by clicking **Add** on the **Member Of** tab. This displays the **Select Objects** dialog, allowing you to select the groups to which you want to add the object.
> - The **Temporal Membership Settings** button can be used to specify the date and time when the object should be added or removed from the selected groups. For more information about this feature, see Using temporal group memberships.
> - By adding an object to a group, you can assign permissions to all of the objects in that group and filter Group Policy settings on all objects in that group.
> - To locate objects you want to add to a certain group, use the **Find** function of Active Roles. Once you found the objects, select the accounts in the list of search results, right-click the selection, and click **Add to a Group**.

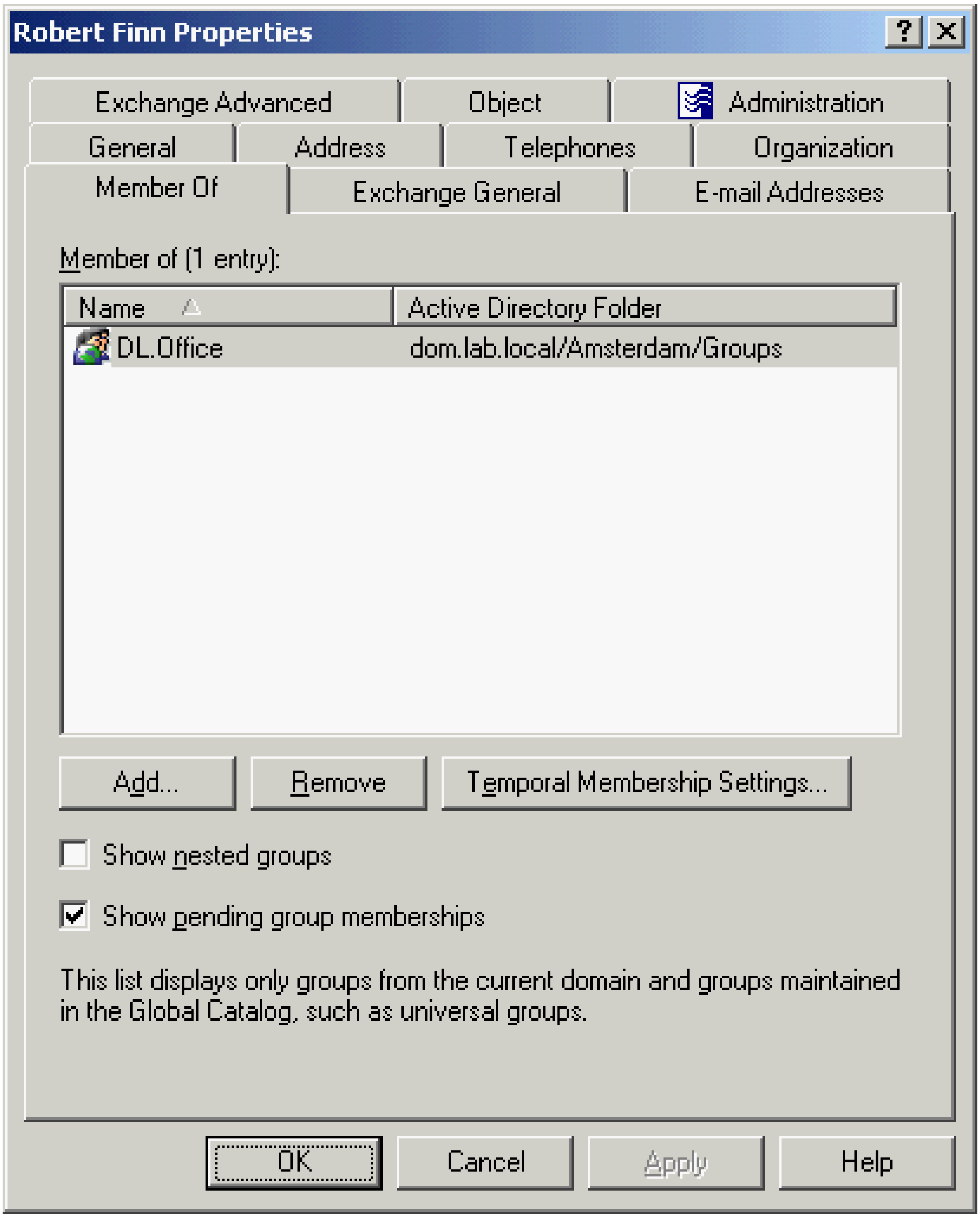
Removing a contact from a group

You can remove contacts from Active Directory groups with the Active Roles Console.

To remove a contact from a group

1. In the **Console tree**, locate and select the folder that contains the contact you want to remove from a group.
2. In the details pane, right-click the contact, then click **Properties**.
3. On the **Member Of** tab in the **Properties** dialog, clear the **Show nested groups** check box, select the group from which you want to remove the contact, and click **Remove**.

Figure 25: Adding and removing contacts from groups



Robert Finn Properties

Member of (1 entry):

Name	Active Directory Folder
DL.Office	dom.lab.local/Amsterdam/Groups

□ Show nested groups

☑ Show pending group memberships

This list displays only groups from the current domain and groups maintained in the Global Catalog, such as universal groups.

NOTE: Consider the following when removing an object from a group:

- If you have not cleared the **Show nested groups** check box, the list on the **Member Of** tab also includes the groups to which the object belongs indirectly, that is, because of group nesting. If you select such a group from the list, the **Remove** button is unavailable. An object can be removed only from those groups of which the object is a direct member.

- You cannot remove objects from their primary groups. Instead, you can change the primary group of an object. To do so, on the **Member Of** tab, select a different group from the list, then click **Set Primary Group**.

Performing Exchange tasks on a contact

You can perform Exchange-related tasks (for example, creating or deleting email addresses) on Active Directory contacts with the Active Roles Console.

To perform Exchange tasks on a contact

1. In the **Console tree**, locate and select the folder that contains the contact you want to perform Exchange tasks on.
2. In the details pane, right-click the contact, then click **Exchange Tasks** to start the Exchange Task Wizard.
3. On the **Available Tasks** page of the wizard, select the task you want to perform.

   The following tasks are available, depending on the selected group:

   - **Establish E-mail Addresses**: The contact has no email address established. Establishes an external email address for the selected contact to include the address in the Exchange address list.
   - **Delete E-mail Addresses**: The contact has an email address established.
4. On the next page of the wizard, do one of the following, depending on the selected task:
   - **Establish E-mail Addresses**: Specify the contact’s alias and external email address.
   - **Delete E-mail Addresses**: Confirm the operation.
5. On the completion page of the wizard, review the results of the task. To view the progress report, click **Back**. To close the wizard, click **Finish**.

NOTE: Consider the following when performing Exchange tasks on a contact:

- You can perform Exchange tasks on multiple objects at a time. To do so, start the Exchange Task Wizard by selecting the objects, right-clicking the selection, and clicking **Exchange Tasks**.
- To locate the objects on which you want to perform Exchange tasks, use the **Find** function of Active Roles. Once you found the objects, start the Exchange Task Wizard by selecting the objects in the list of search results, right-clicking the selection, and clicking **Exchange Tasks**.

Moving a contact

You can move contacts from one Active Directory container to another with the Active Roles Console.

To move a contact

1. In the **Console tree**, locate and select the folder that contains the contact you want to move.
2. In the details pane, right-click the contact and click **Move** to display the **Move** dialog.
3. In the **Move** dialog, select the folder to which you want to move the contact, then click **OK**.

> NOTE: Consider the following when moving an object:
>
> - With Active Roles, directory objects can only be moved within the same domain. This means that the folder to which you want to move the object must belong to the same domain as the object.
> - You can move multiple objects at a time with the **Move** dialog. To open the dialog, select the objects, right-click the selection, and click **Move**. To select multiple objects, press and hold **Ctrl**, then click each object.
> - To locate the object that you want to move, use the **Find** function of Active Roles. Once you found the accounts, open the **Move** dialog by right-clicking the object, and clicking **Move**.
> - The Console provides the drag-and-drop function for moving objects. To move objects, you can drag the selection from the details pane to a destination container in the **Console tree**.

Exporting and importing a contact

With the Active Roles Console, you can export contacts to an XML file, then import them from that file to populate a container in a different domain. The export and import operations provide a way to relocate contacts between domains.

To export a contact

1. In the **Console tree**, locate and select the folder that contains the contact you want to export.
2. In the details pane, right-click the contact and click **All Tasks** > **Export** to display the **Export Objects** dialog.
3. In the **Export Objects** dialog, specify the file where you want to save the data, and click **Save**.

To import a contact

1. In the **Console tree**, locate and select the folder where you want to import the contact.
2. Click **Import**.
3. In the **Import Directory Objects** dialog, select the file that contains the contact you want to import, and click **Open**.

Deleting a contact

You can delete Active Directory user accounts with the Active Roles Console.

To delete a contact

1. In the **Console tree**, locate and select the folder that contains the contact you want to delete.
2. In the details pane, right-click the contact, then click **Delete**.
3. To confirm the deletion, click **Yes**.

> NOTE: Consider the following when deleting a contact:
>
> - Deleting a contact is a destructive operation that cannot be undone. Also, if you recreate the contact with the same name later, the contact will not receive automatically the same distribution group and security group memberships that the deleted contact had. Instead, you must assign the previous memberships manually.
> - You can delete multiple objects at the same time by selecting the objects, right-clicking the selection, and clicking **Delete**. To select multiple objects, press and hold **Ctrl**, then click each object. If you select multiple objects, clicking **Delete** displays a dialog. To delete all the selected objects, select the **Apply to all items** check box, then click **Yes**.
> - When attempting to delete an object, you may receive an error message that access is denied to the object. This can typically occur if the object is protected from deletion. To remove this protection, navigate to the **Properties** > **Object** tab of the object you want to delete, then clear the **Protect object from accidental deletion** check box. After that, try deleting the object again.

8

Exchange recipient management

You can perform the following Exchange recipient management tasks in the Active Roles Console.

- Creating an Exchange mailbox
- Performing Exchange tasks
- Managing Exchange-related properties
- Managing Unified Messaging users

Creating an Exchange mailbox

When creating a user account, the Active Roles Console provides the option to create a user mailbox for that user. User mailboxes are the most commonly used mailbox type, and it is typically the mailbox type that is assigned to users in an Exchange organization.

Additionally, the Console provides a number of commands for creating special-purpose mailboxes in an Exchange organization where Exchange is deployed. On a container, such as an Organizational Unit, each of these commands creates an inactive user account along with a special-purpose mailbox associated with that account:

- **New** > **Room Mailbox**: Creates a mailbox that is assigned to a meeting location, such as a conference room, auditorium, or training room. Room mailboxes can be included as resources in meeting requests, providing a simple and efficient way of organizing meetings for your users.
- **New** > **Equipment Mailbox**: Creates a mailbox that is assigned to a non-location specific resource, such as a portable computer projector, microphone, or a company car. Equipment mailboxes can be included as resources in meeting requests, providing a simple and efficient way of utilizing resources for your users.
- **New** > **Linked Mailbox**: Creates a mailbox that is assigned to an individual user in a separate, trusted forest. Linked mailboxes may be necessary for organizations that choose to deploy Exchange in a resource forest. The resource forest scenario allows an organization to centralize Exchange in a single forest, while allowing access to the Exchange organization with user accounts in one or more trusted forests.

- **New** > **Shared Mailbox**: Creates a mailbox that is not primarily assigned to a single user and is generally configured to allow login access for multiple users. The user account associated with a shared mailbox must be an inactive account. You can also specify a list of the mailbox users each of which will have full access to the shared mailbox.

Creating a user mailbox

When configuring a new user account, you can also create a mailbox for it. To create a user mailbox for an existing user account, use the **Exchange Tasks** command on that account. For more information, see Performing Exchange tasks on a user account.

> NOTE: You can only create mailboxes for users. You cannot create mailboxes for contacts.

To create a new user mailbox

1. In the **Console tree**, locate and select the folder in which you want to add the user account.
2. Right-click the folder, then click **New** > **User**.
3. Follow the wizard pages to specify properties of the new user account, such as the user first name, last name, full name, display name, login name, pre-Windows 2000 login name, and password.
4. When prompted for the user alias and mailbox location, accept or change the default alias setting, and select the mailbox database to hold the mailbox data. Optionally, specify a retention policy, Exchange ActiveSync mailbox policy, or address book policy for this mailbox.
5. Click **Finish** on the completion page of the wizard.

> NOTE: The behavior of the wizard pages may vary depending on the configuration of Active Roles policies. To determine whether a given item on a page is under the control of a certain policy, observe the text label next to the item: the underlined text label indicates that some policy restrictions are in effect. Click underlined text labels to examine the policies that govern the behavior of the wizard pages. For more information, see Getting policy-related information.The policy information is also displayed whenever you supply a property value that violates a policy restriction. The wizard cannot proceed until you enter an acceptable value.

Creating a room or equipment mailbox

You can create a room or equipment mailbox along with a new inactive user account that will be associated with the mailbox. To create a room or equipment mailbox associated with an existing inactive user account, use the **Exchange Tasks** command on that account. For more information, see Performing Exchange tasks on a user account.

To create a new room or equipment mailbox

1. In the **Console tree**, locate and select the folder in which you want to add the user account.
2. Right-click the folder, point to **New**, then click one of the following:
    - To create a room mailbox, click **Room Mailbox**.
    - To create an equipment mailbox, click **Equipment Mailbox**.
3. Follow the wizard pages to specify properties of the new user account, such as the user first name, last name, full name, display name, login name, pre-Windows 2000 login name, and password.
4. When prompted for the user alias and mailbox location, accept or change the default alias setting, and select the mailbox database to hold the mailbox data. Optionally, specify a retention policy, Exchange ActiveSync mailbox policy, or address book policy for this mailbox.
5. (Optional) When prompted for the resource mailbox settings, specify the resource capacity and select the resource custom properties to add to the mailbox.

    After the mailbox is created, you can view or change these settings in the **Properties** > **Resource Information** tab of the user account associated with the mailbox.
6. Click **Finish** on the completion page of the wizard.

Creating a linked mailbox

You can create a linked mailbox along with a new inactive user account that will be associated with the mailbox. To create a linked mailbox associated with an existing inactive user account, use the **Exchange Tasks** command on that account. For more information, see Performing Exchange tasks on a user account.

To create a new linked mailbox

1. In the **Console tree**, locate and select the folder in which you want to add the user account.
2. Right-click the folder, then select **New** > **Linked Mailbox**.
3. Follow the wizard pages to specify properties of the new user account, such as the user first name, last name, full name, display name, login name, pre-Windows 2000 login name, and password.
4. When prompted for the user alias and mailbox location, accept or change the default alias setting, and select the mailbox database to hold the mailbox data. Optionally, specify a retention policy, Exchange ActiveSync mailbox policy, or address book policy for this mailbox.
5. When prompted for the linked master account, click **Browse** and select the user from a trusted forest or domain to which you want to assign the mailbox.

After the mailbox has been created, you can view or change this setting on the **Master Account** tab in the **Properties** dialog for the user account associated with the mailbox.

6. Click **Finish** on the completion page of the wizard.

Creating a shared mailbox

You can create a shared mailbox along with a new inactive user account that will be associated with the mailbox. To create a shared mailbox associated with an existing inactive user account, use the **Exchange Tasks** command on that account. For more information, see Performing Exchange tasks on a user account.

To create a new shared mailbox

1. In the **Console tree**, locate and select the folder in which you want to add the user account.
2. Right-click the folder, then click **New** > **Shared Mailbox**.
3. Follow the wizard pages to specify properties of the new user account, such as the user first name, last name, full name, display name, login name, pre-Windows 2000 login name, and password.
4. When prompted for the user alias and mailbox location, accept or change the default alias setting, and select the mailbox database to hold the mailbox data. Optionally, specify a retention policy, Exchange ActiveSync mailbox policy, or address book policy for this mailbox.
5. (Optional) When prompted to specify the users who will have full access to the shared mailbox, click **Add**, then select the users you want.

   After the mailbox is created, you can add or remove mailbox users in the **Properties** > **Mailbox Sharing** tab of the user account associated with the mailbox.
6. Click **Finish** on the completion page of the wizard.

Managing Exchange-related properties

For Exchange recipients (mail-enabled users, contacts and groups, and mailbox-enabled users) the **Properties** dialog includes the following tabs for managing Exchange-related properties:

- Exchange General tab
- Exchange Advanced tab
- E-mail Addresses tab
- Mail Flow Settings tab

- Mailbox Settings tab
- Mailbox Features tab
- Calendar Settings tab
- Resource Information tab
- Master Account tab
- Mailbox Sharing tab

Exchange General tab

For a mailbox-enabled user account, you can use the **Exchange General** tab to:

- Identify the mailbox type.
- Identify the Organizational Unit of the mailbox user account.
- Identify who last logged on to the mailbox.
- Identify the number of items held in the mailbox, and the size of the mailbox.
- Identify the mailbox database and server.
- Identify the archive database is an archive is enabled for the mailbox.
- View the date and time that the configuration of the mailbox was last modified.
- View or change the alias.
- Hide the mailbox from Exchange address lists.
- View or change custom attributes.

For a mail-enabled user account or contact, you can use the **Exchange General** tab to:

- View or change the alias.
- View or change the option to use MAPI rich text format.
- Hide the user or contact from Exchange address lists.
- View or change custom attributes.

For a mail-enabled (distribution) group, you can use the **Exchange General** tab to:

- View or change the alias and display name.
- View or change custom attributes.

Exchange Advanced tab

For a mailbox-enabled user account, you can use the **Exchange Advanced** tab to:

- View or change the simple display name.

  The simple display name is used by systems that cannot interpret all of the characters in a normal display name.
- Downgrade high priority mail bound for X.400.

  Use this option to downgrade email that is set for high priority delivery to an X.400-type email address. The downgrade causes the outbound email to conform to original 1984 X.400 conventions.
- View or change the Internet Locator Service (ILS) settings.

  You can specify the Internet Locator Service (ILS) server and ILS account name for the mailbox.
- View or change mailbox rights.

  You can specify mailbox permissions, assign mailbox permissions to users and groups, and change inherited permissions.
- View mailbox move status.

  You can view status of mailbox move request, clear completed move request, or remove non-completed move request.

For a mail-enabled user or contact, you can use the **Exchange Advanced** tab to:

- View or change the simple display name.
- Downgrade high priority mail bound for X.400 (for a mail-enabled user).
- View or change the Internet Locator Service (ILS) settings.

For a mail-enabled (distribution) group, you can use the **Exchange Advanced** tab to:

- View or change the simple display name.
- Select the desired expansion server.

  You can select a server in your Exchange organization that will be responsible for expanding the membership list for this mail-enabled (distribution) group.
- Hide the group from Exchange address lists.
- Choose whether to send out-of-office messages to message originators
- Select delivery report options.

E-mail Addresses tab

For a mailbox-enabled user account or a mail-enabled (distribution) group, you can use the **E-mail Addresses** tab to:

- View, add, edit or remove email addresses.
- View or change the default reply address for each address type.
- Set the option to update email addresses based on e-mail address policy.

For a mail-enabled user account or contact, you can use the **E-mail Addresses** tab to:

- View, add, edit or remove email addresses.
- View or change the default reply address for each address type.
- View or change the external e-mail address.
- Set the option to update email addresses based on email address policy.

Mail Flow Settings tab

For a mailbox-enabled user account, you can use the **Mail Flow Settings** tab to:

- View or change delivery options. You can configure users to send messages on behalf of the mailbox user, specify a forwarding address for messages addressed to the mailbox, and limit the number of recipients to whom the mailbox user can send a message.
- View or change message size restrictions and message delivery restrictions. You can specify the maximum size of incoming and outgoing messages for the mailbox, and also specify sender allow or deny lists, that is email addresses from which the mailbox can or cannot receive email.

For a mail-enabled user account or contact, you can use the **Mail Flow Settings** tab to:

- View or change message size restrictions and message delivery restrictions. You can specify the maximum size of incoming messages for the mailbox-enabled user or contact, and also specify sender allow or deny lists for them, that is email addresses from which the user or contact can or cannot receive emails.

For a mail-enabled (distribution) group, you can use the **Mail Flow Settings** tab to:

- View or change message size restrictions and message delivery restrictions. You can specify the maximum size of incoming messages for the group, and also specify sender allow or deny lists, that is email addresses from which the group can or cannot receive emails.
- View or change the message moderation settings. You can configure whether messages sent to the (distribution) group must be approved by a moderator before they are delivered to the group members.

Mailbox Settings tab

For a user account that has a mailbox on Exchange 2016 or later, you can use the **Mailbox Settings** tab to:

- View or change the messaging records management settings. You can select or suspend retention policy for the mailbox, place the mailbox on litigation hold to preserve deleted mailbox items and to record change made to mailbox items, specify the messaging records management description URL, and provide mailbox comments.

- View or change storage quotas. You can specify storage limits that, when exceeded, result in the mailbox user being warned or prohibited from sending or receiving email. You can also select the number of days a deleted item is retained in the mailbox store before it is permanently deleted.
- View or change the archive quota. If archiving is enabled for the mailbox, you can view or change the archive size at which messages are no longer moved to the archive and a warning message is sent to the mailbox user.
- Apply a sharing policy to the mailbox. You can select the sharing policy you want to be associated with the mailbox. This enables the mailbox user to create sharing relationships with users in other external federated Exchange organizations or with individuals in non-Exchange organizations.
- Apply a role assignment policy to the mailbox. You can select the management role assignment policy you want to be associated with the mailbox. This policy controls what specific mailbox and distribution group configuration settings the mailbox user is allowed to modify.
- Apply an address book policy to the mailbox. You can select the address book policy you want to be associated with the mailbox. This policy defines the global address list and other address lists that the user will see in Outlook and Outlook Web App.

Mailbox Features tab

You can use the **Exchange Features** tab to manage a variety of mailbox features for the mailbox user. You can also change configuration settings for certain features by selecting a feature from the list, then clicking **Properties**.

The **Mailbox Features** tab includes the following settings:

- **Outlook Mobile Access**: Allows the user to browse the mailbox with a cell phone or other wireless devices.
- **Exchange ActiveSync**: Allows the user to access the mailbox from a mobile device.

  To apply an Exchange ActiveSync mailbox policy to the mailbox, select this setting, then click **Properties**.
- **Up-to-date Notifications**: Allows the user to apply notifications in order to keep the mailbox data on a mobile device always up to date.
- **IMAP4**: Allows the user to access the mailbox from an IMAP4 client such as Outlook Express.

  To configure the MIME format for messages retrieved from the server for the mailbox, select this setting, then click **Properties**. You can use the default protocol settings, or specify a custom setting that overrides the default protocol settings.
- **POP3**: Allows the user to access the mailbox from a POP3 client, such as Outlook Express. To configure the MIME format for the messages retrieved from the server for the mailbox, select this setting, then click **Properties**. You can use the default

protocol settings, or specify a custom setting that overrides the default protocol settings.

- **Outlook Web App**: Allows the user to access the mailbox from a web browser by using Microsoft Outlook Web App (formerly known as Outlook Web Access). To assign an Outlook Web App mailbox policy to the mailbox, select this setting, then click **Properties**. In Exchange 2016 or later, Outlook Web App mailbox policies can be used to manage access to Outlook Web App features, overriding the settings of the Outlook Web App virtual directory.
- **MAPI**: Allows the user to access the mailbox from a MAPI client such as Microsoft Outlook.
- **Archive**: If the mailbox is archive-enabled, you can view or change the archive properties. To enable or disable archiving for the mailbox, use the **Enable Archive** or **Disable Archive** task in the Exchange Task wizard. If an archive is enabled for the mailbox, click **Properties** to view or change the name of the archive associated with this mailbox.
- **Unified Messaging**: If the mailbox is enabled for Unified Messaging, you can view or change the Unified Messaging properties of the mailbox. To enable or disable the mailbox for Unified Messaging, use the **Enable Unified Messaging** or **Disable Unified Messaging** task in the Exchange Task wizard. If the mailbox is enabled for Unified Messaging, click **Properties** to view or change the Unified Messaging properties of this mailbox. For more information, see Managing Unified Messaging users.

Calendar Settings tab

You can use the **Calendar Settings** tab to view or change the Calendar Attendant settings for the mailbox. The tab is available on (disabled) user accounts associated with a room or equipment mailbox in Microsoft Exchange.

The Calendar Attendant processes meeting requests as they come in, even if users are not currently logged on by means of a client such as Outlook. When enabled, the Calendar Attendant updates the time of the meeting on an attendee’s calendar after receiving an update from the meeting organizer, and updates the attendee’s response on the meeting organizer’s calendar after receiving a response from the attendee.

The **Calendar Settings** tab provides the option to enable or disable the Calendar Attendant for the mailbox, and provides a number of options to control how the Calendar Attendant handles meeting requests and responses. If you enable the Calendar Attendant, the following options are available:

- **Remove meeting forward notifications to the Deleted Items folder**: This option causes the Calendar Attendant to delete notifications about forwarded meeting requests. Such a notification occurs when a meeting request created by the mailbox user is forwarded to a new recipient by one of the meeting attendees.
- **Remove old meeting requests and responses**: This option causes the Calendar Attendant to delete out-of-date meeting requests and responses from the **Inbox**

folder of the mailbox.

- **Mark new meeting requests as Tentative**: This option causes the Calendar Attendant to automatically place new meeting requests on the mailbox user’s calendar and mark them as tentative, without sending a reply to the meeting organizer.
- **Process meeting requests and responses originating outside the Exchange organization**: This option causes the Calendar Attendant to automatically process requests and responses from external senders who are not a member of your Exchange organization.

Resource Information tab

On the **Resource Information** tab, you can view or change the resource mailbox settings. This tab is available only for resource mailboxes. For instructions on how to create a resource mailbox, see Creating a room or equipment mailbox.

There are two types of resource mailboxes in Microsoft Exchange Server: room and equipment. Room mailboxes are assigned to a meeting location such as a conference room, auditorium, or training room. Equipment mailboxes are assigned to a resource that is not location specific, such as a portable computer projector, microphone, or company car.

The following fields provide users with general information about the resource:

- **Resource capacity**: Use this box on the **Resource Information** tab to type the capacity the resource can handle. For example, for a room mailbox, you can specify the number of people the room can accommodate. The value range is from `0` through `2,147,483,647`.
- **Resource custom properties**: Custom resource properties can help users select the most appropriate room or equipment by providing additional information about the resource. For example, suppose a custom property for room mailboxes called **Audio-Visual** is defined in your Exchange organization. You can add this property to the room mailboxes for the rooms that have audio-visual equipment. This allows users to identify which conference rooms have audio-visual equipment available.

  Click **Add** on the **Resource Information** tab to open a dialog allowing you to select custom properties. The dialog displays a list of all custom resource properties that are defined in your Exchange organization for the specific resource type (room or equipment). Select the custom resource properties you want to assign to this mailbox, and then click **OK**.

  Click **Remove** to remove custom resource property from the resource mailbox.

With the supported Exchange versions, the following additional options are available:

- **Enable the Resource Booking Attendant**: Select this check box to allow the Resource Booking Attendant to process resource booking requests and cancellations. When enabled, the Resource Booking Attendant uses the booking policies to determine whether incoming requests will be accepted or declined. If the Resource

Booking Attendant is not enabled, the resource mailbox's delegate must accept or decline all requests.

- **Resource policy**: Click this button to view or change the options that determine under which conditions the resource mailbox automatically accepts requests. For more information, see Resource Policy.
- **Resource information**: Click this button to view or change the options that specify the information that appears in the resource's calendar. For more information, see Resource Information.
- **Resource in-policy requests**: Click this button to specify the users who are allowed to submit requests within the resource's policy configuration. For more information, see Resource in-policy request.
- **Resource out-of-policy requests**: Click this button to specify the users who are allowed to submit requests that do not meet the resource's policy configuration. For more information, see Resource out-of-policy request.

Resource Policy

Use the **Resource Policy** dialog to specify under which conditions the resource mailbox automatically accepts requests:

- **Allow conflict meeting requests**: Select this check box to allow conflicting meeting requests to be scheduled by the Resource Booking Attendant.
- **Allow repeating meetings**: Select this check box to allow repeating or recurring meetings to be scheduled.
- **Allow scheduling only during working hours**: Select this check box to allow scheduling for the resource to occur during working hours. Users can set working hours by using Outlook or Outlook Web App.
- **Reject repeating meetings that have an end date beyond the booking window**: Select this check box to allow the Resource Booking Attendant to reject recurring meeting requests that are outside of the resources booking window.
- **Booking window (days)**: Use this box to specify the number of days that the resource can be booked in advance. For example, if the booking window is set for 90 days and a request is received for scheduling the resource 4 months from today's date, the Resource Booking Attendant rejects the request.
- **Maximum duration (minutes)**: Use this box to specify the maximum number of minutes that the resource can be scheduled for.
- **Maximum conflict instances**: Use this box to specify the maximum number of conflicts allowed for recurring meetings. If the number of instances for a recurring meeting in conflict exceeds this number, the recurring meeting request is declined.
- **Conflict percentage allowed**: Use this box to specify the conflict percentage threshold from recurring meetings. If the percentage of instances of a recurring meeting that conflicts with other meetings exceeds the threshold, the recurring meeting request is declined.

- **Specify delegates of this mailbox**: Click **Add** to add delegates who can control the scheduling options for the resource mailbox. Click **Remove** to remove delegates from this resource mailbox.
- **Forward meeting requests to delegates**: Select this check box to forward all meeting requests to the delegates.

Resource Information

Use the **Resource Information** dialog box to specify the meeting information that appears in the resource's calendar:

- **Delete attachments**: Select this check box to remove attachments from all incoming requests.
- **Delete comments**: Select this check box to remove any text in the message body of incoming requests.
- **Delete the subject**: Select this check box to remove the subject of all incoming requests.
- **Delete non-calendar items**: Select this check box to remove all non-calendar Outlook items received by the mailbox.
- **Add the organizer's name to the subject**: Select this check box to specify whether the resource requester's name is added to the subject of the request.
- **Remove the private flag on an accepted meeting**: Select this check box to clear the private flag for all incoming requests.
- **Send organizer information when a meeting request is declined because of conflicts**: Select this check box to send the meeting organizer information regarding declined requests.
- **Customize the response message that organizers will receive**: Select the **Add additional text** check box to customize the message that the requester receives when the meeting has been declined, and then type the additional information in the **Additional text** field.
- **Mark pending requests as Tentative on the calendar**: Select this check box to specify that all pending requests are marked as Tentative in the resource's calendar. The delegate can then accept or deny the request as needed.

Resource in-policy request

Use the **Resource In-Policy Requests** dialog box to specify the users who are allowed to submit requests within the resource policy's configuration:

- **Specify users who are allowed to submit in-policy meeting requests that will be automatically approved**: Click **All users** or **Selected recipients**. If you click **Selected recipients**, you need to click **Add** to select the recipients. You can also remove selected recipients by clicking **Remove**.

- **Specify who can submit in-policy meeting requests that are subject to approval by a resource mailbox delegate**: Click **All users** or **Selected recipients**. If you click **Selected recipients**, you need to click **Add** to select the recipients. You can also remove selected recipients by clicking **Remove**.

Resource out-of-policy request

Use the **Resource Out-of-Policy Requests** dialog to specify the users who are allowed to submit resource requests that do not meet the resource's policy configuration. Users who have permission to submit out-of-policy requests will not have their request denied, but the requests require approval by one of the resource's delegates:

- **All users**: Choose this option to allow all users to submit out-of-policy requests.
- **Selected recipients**: Choose this option to allow specific users to submit out-of-policy requests. If you choose this option, you need to click **Add** to select the users. You can also remove selected users by clicking **Remove**.

Master Account tab

Use the **Master Account** tab to view or change information about the master account for the linked mailbox. This tab is available only for linked mailboxes. For instructions on how to create a linked mailbox, see Creating a linked mailbox.

Linked mailboxes are mailboxes that are accessed by users in a separate, trusted forest. Linked mailboxes may be necessary for organizations that choose to deploy Exchange in a resource forest. The resource forest scenario allows an organization to centralize Exchange in a single forest, while allowing access to the Exchange organization with user accounts in one or more trusted forests. The linked master account is the user account that will be used to access the linked mailbox.

From the **Master Account** tab you can view the current master account or choose a different master account for the linked mailbox. Click **Browse** next to the **Linked master account** box and then use the **Select Objects** dialog to select the user account you want to be used to access this linked mailbox. Select a user account from a forest or domain trusted by the forest or domain where Exchange is deployed.

Mailbox Sharing tab

Use the **Mailbox Sharing** tab to view or change information about the users who have full access to the shared mailbox. This tab is available only for shared mailboxes. For instructions on how to create a shared mailbox, see Creating a shared mailbox.

Shared mailboxes are generally configured to allow login access for multiple users. Although it is possible to grant additional users, the login rights to any mailbox type, shared mailboxes are dedicated for this functionality. The user account that is associated with a shared mailbox must be a disabled account. From this page, you can grant permissions to all users that require access to the shared mailbox.

From this tab, you can view or change a list of mailbox users. These are the users who can log on to the shared mailbox and have full access to the mailbox contents. They can use the mailbox to send and receive messages, manage contacts, schedule meetings, and maintain a task list. You can add or remove mailbox users:

- Click **Add** on the **Mailbox Sharing** tab and then use the **Select Objects** dialog to select the users you want to have full access to the shared mailbox.
- If you want a certain user to no longer have access to the shared mailbox, select that user from the **Mailbox users** list and click **Remove**.

Managing Unified Messaging users

You can use Active Roles to configure Unified Messaging users. Unified Messaging is a technology in Microsoft Exchange Server that combines voice messaging and email messaging into one store, accessible from a telephone and a computer. Unified Messaging puts all email and voice messages into one Exchange mailbox that can be accessed from many different devices. Once a user has an Exchange mailbox, you can configure the user for Unified Messaging. This can be accomplished by using the Active Roles Console or Web Interface.

Enabling a user for Unified Messaging

When you enable a user for Unified Messaging (UM), Active Roles applies a default set of UM properties to the user, so that the user can use UM features. You have the option to add a Session Initiation Protocol (SIP) or E.164 address for the user. However, the user must still have an extension number configured.

You can configure the extension number automatically or manually when enabling the user for UM. An extension number is required for each UM-enabled user associated with a telephone extension, SIP Uniform Resource Identifier (URI), or E.164 dial plan. The extension number must be the correct number of digits, as specified in the UM dial plan for the UM mailbox policy. If the user is associated with an E.164 dial plan, you can manually configure an E.164 address for the user when you are enabling the user for UM. If you associate a user to a SIP URI or E.164 dial plan, you must manually enter an extension number and the SIP or E.164 address for the user.

To enable a user for Unified Messaging

1. Do one of the following, depending on whether you are using the Active Roles Console or Web Interface:

   a. In the Active Roles Console:

      1. Right-click the user, then click **Exchange Tasks**.
      2. Follow the steps in the Exchange Task wizard.
      3. On the **Available Tasks** page, click **Enable Unified Messaging**, then click **Next**.

   b. In the Web Interface, click the user, then click the **Enable Unified Messaging** command.

2. On the **Unified Messaging Mailbox Policy** page, complete the following field:

   a. **Unified Messaging mailbox policy**: Click **Browse** and select the UM mailbox policy that you want to associate with the user mailbox.

   UM mailbox policies define settings such as PIN policies and dialing restrictions. Each UM-enabled user must be associated with a certain UM mailbox policy.

3. Click **Next**.
4. On the **Unified Messaging PIN** page, complete the following fields:

   - **Automatically generate PIN to access Outlook Voice Access**: Select this option to automatically generate a new PIN for the UM-enabled user. This is the default setting. If you select this option, a PIN is automatically generated based on the PIN policies configured on the user's UM mailbox policy. The automatically generated PIN will be sent in an email message to the user's mailbox.
   - **Manually specify PIN**: Select this option to manually specify a new PIN for the UM-enabled user. The PIN you specify with this option will be sent in an email message to the user's mailbox.

     The PIN must comply with the PIN policies configured on the user's UM mailbox policy. For example, if the UM mailbox policy is configured to accept only PINs that contain five or more digits, you must specify a PIN at least five digits long.
   - **Require user to reset PIN on first telephone logon**: Select this check box to force the user to reset the UM PIN the first time that the user accesses the UM system from a telephone.

     > TIP: To help protecting mailbox data, One Identity recommends selecting this option, as changing the PIN after the first login is a security best practice.

5. Click **Next**.
6. On the **Extension Configuration** page, complete the following fields:

   - **Automatically-generated mailbox extension**: Select this option if you want the extension number for the user's mailbox to be automatically generated from the telephone number specified in Active Directory. This option is selected by default if the user's UM mailbox policy is associated with a Telephone Extension dial plan; otherwise, the option is unavailable. The automatically generated extension will be sent in an e-mail message to the user's mailbox.

The automatically generated extension will comply with the number of digits specified on the dial plan for the user's UM mailbox policy. For example, if the dial plan is configured to use 5-digit extension numbers, the UM server will take the last 5 digits of the user's telephone number and use those digits as the user's mailbox extension.

- **Manually-entered mailbox extension**: Select this option if you want to manually specify the extension number for the user's mailbox. The extension number you specify with this option will be sent in an email message to the user's mailbox.

  The extension must comply with the number of digits specified on the dial plan for the user's UM mailbox policy. For example, if the dial plan is configured to use 5-digit extension numbers, you should specify an extension containing exactly 5 digits.

- **Automatically-generated SIP resource identifier**: Select this option if you want the SIP resource identifier or SIP address for the user's mailbox to be automatically generated. If Microsoft Office Communications Server is deployed in your organization, then the user's SIP address is taken from the `msRTCSIP-PrimaryUserAddress` attribute in Active Directory. If this attribute is not populated, the user's primary SMTP address will be used for the SIP address, such as `sam.smith@company.com`.

  This option is available only if the user's UM mailbox policy is associated with a SIP URI dial plan. This option will be unavailable if the user's UM mailbox policy is associated with a Telephone Extension or E.164 dial plan.

  This option also requires that you manually enter a mailbox extension for the user. This extension number is used when the user accesses the mailbox via Outlook Voice Access. The number of digits in the extension number must match the number of digits configured on the SIP URI dial plan for the user's UM mailbox policy.

- **Manually-entered SIP resource identifier**: Select this option if you want to manually enter the SIP or E.164 address for the user. This option is available if the user's UM mailbox policy is associated with either a SIP URI or E.164 dial plan. This option will be unavailable if the user's UM mailbox policy is associated with a Telephone Extension dial plan.

  If the user's UM mailbox policy is associated with an E.164 dial plan, you have to enter an E.164 address for the user. The address must be in the correct E.164 format, such as `+14275551234`. If the user's UM mailbox policy is associated with a SIP URI dial plan, you have to enter a SIP address for the user. The address must be in the correct format, such as `sam.smith@company.com`.

  This option also requires that you manually enter a mailbox extension for the user. This extension number is used when the user accesses the mailbox via Outlook Voice Access. The number of digits in the extension number must match the number of digits configured on the dial plan for the user's UM mailbox policy.

7. Do one of the following, depending on whether you are using the Active Roles Console or Web Interface:
    - In the Active Roles Console, click **Next** and wait while Active Roles performs the task. Then, click **Finish** to complete the wizard.
    - In the Web Interface, click **Finish** and wait while Active Roles performs the task.

After you have enabled a user for UM, you may also want to view or change the UM-related properties of that user. For more information, see Viewing or changing the properties of a Unified Messaging-enabled user.

Viewing or changing the properties of a Unified Messaging-enabled user

You can use Active Roles to view or configure the Unified Messaging (UM) properties of a user who is enabled for UM. When you change a user's UM properties, you can control the user's access to various UM features. For example, you can enable or disable Automatic Speech Recognition (ASR) or fax receiving.

To view or change the UM properties of a UM-enabled user

1. Do one of the following, depending on whether you are using the Active Roles Console or Web Interface:
    a. In the Active Roles Console:
        i. Right-click the user, then click **Properties**.
        ii. In the **Properties** dialog, click the **Mailbox Features** tab.
        iii. On the **Mailbox Features** tab, click **Unified Messaging**, then click **Properties**.
    b. In the Web Interface:
        i. Click the user, then click the **Exchange Properties** command.
        ii. On the **Exchange Properties** page, click the **Mailbox Features** tab.
        iii. On the **Mailbox Features** tab, click **Unified Messaging**, then click **Properties**.
2. Use the **Unified Messaging Properties** dialog to view or change the following properties of the UM-enabled user:
    - **UM Mailbox Status**: This area shows the UM lockout status of the user's mailbox. Normally, the status is listed as **Not locked out**. The status of **Locked Out** indicates that the user is locked out of UM due to a number of attempts to enter an incorrect UM PIN in Outlook Voice Access.
    - **Unified Messaging mailbox policy**: This field shows the name of the UM mailbox policy associated with the UM-enabled user.

- **UM extensions**: This box displays the extension number and the Session Initiation Protocol (SIP) or E.164 address that are assigned to the UM-enabled user. The contents of this box depends upon the dial plan of the user's UM mailbox policy. With a Telephone Extension dial plan, only the extension number configured for the user appears in this box. With a SIP dial plan, the extension number and SIP address are listed. With an E.164 dial plan, the extension number and E.164 address are listed.
- **Enable for Automatic Speech Recognition**: When selected, this option indicates that the UM-enabled user can access the mailbox by means of Automatic Speech Recognition (ASR). This option is selected by default, which allows the user to use voice commands when accessing the mailbox via Outlook Voice Access. Even if enabled for ASR, the user must still use the keypad to enter the extension number and PIN.
- **Allow UM calls from non-users**: When selected, this option allows incoming calls from unauthenticated callers through an auto attendant to be transferred to the UM-enabled user. By default, this option is selected, allowing callers from outside your organization to be transferred to the user inside the organization.

  If this option is not selected, then an external caller who tries to transfer to the user receives the following response from the UM system: "I'm sorry, I am unable to transfer the call to this user." The caller is then transferred to the operator configured on the auto attendant.

  This option does not affect callers who have signed in to their mailbox using Outlook Voice Access and are sending a voice message to the user.
- **Allow the user to receive faxes**: When selected, this option allows the UM-enabled user to receive incoming faxes. By default, this option is selected. Unselect it if you do not want the user to receive incoming faxes.

  This option is also configured on UM dial plans. If you select this option for a UM-enabled user, but the dial plan is configured to disallow fax receiving, the UM-enabled user is unable to receive faxes.
- **Allow diverted calls without a caller ID to leave a message**: When selected, this option indicates that, for diverted calls without a caller ID, the caller is allowed to leave a message in the user's mailbox. By default, this option is selected, which makes it possible for the UM-enabled user to accept anonymous calls.
- **Allow users to configure call answering rules**: When selected, this option allows the UM-enabled user to create personal auto attendants. This option is available to users with mailbox on a server running an Exchange instance which does not hold the role of a UM server. If this option is disabled on the UM dial plan or on the UM mailbox policy, it is not available to UM-enabled users associated with that UM mailbox policy.
- **Personal operator extension**: Use this field to specify the operator extension number for the user. This enables incoming calls for the UM-enabled user to be forwarded to the extension number that you specify in this field. By

default, an extension number is not configured. The range for the extension number is from 1 through 20 characters.

Other types of operator extensions can be configured on dial plans and auto attendants. However, those extensions are normally meant for company-wide receptionists or operators. The personal operator extension setting could be used when an administrative assistant or personal assistant answers incoming calls before they are answered by the user.

Resetting the Unified Messaging PIN for a UM-enabled user

When a Unified Messaging-enabled (UM-enabled) user is locked out of the mailbox because of a number of attempts to enter an incorrect UM PIN in Outlook Voice Access, or the user forgot the PIN, you can use Active Roles to reset the user's PIN. When you reset a user's PIN, you can configure UM to automatically generate a PIN or you can manually specify the PIN. The new PIN is e-mailed to the user. If you prefer, you can specify additional PIN options when resetting the user's PIN.

To reset the Unified Messaging PIN for a UM-enabled user

1. Do one of the following, depending on whether you are using the Active Roles Console or Web Interface:
   - In the Active Roles Console:
     a. Right-click the user, then click **Exchange Tasks**.
     b. Follow the steps in the Exchange Task wizard.
     c. On the **Available Tasks** page, click **Reset Unified Messaging PIN**, then click **Next**.
   - In the Web Interface, click the user, then click the **Reset Unified Messaging PIN** command.
2. On the **Reset Unified Messaging PIN** page, complete the following fields:
   - **Automatically generate PIN to access Outlook Voice Access**: Select this option to automatically generate a new PIN for the UM-enabled user. This is the default setting. If you select this option, a PIN is automatically generated based on the PIN policies configured on the user's UM mailbox policy. The automatically generated PIN will be sent in an email message to the user's mailbox.
   - **Manually specify PIN**: Select this option to manually specify a new PIN for the UM-enabled user. The PIN you specify with this option will be sent in an email message to the user's mailbox.

     The PIN must comply with the PIN policies configured on the user's UM mailbox policy. For example, if the UM mailbox policy is configured to accept only PINs that contain five or more digits, you must specify a PIN at least five digits long.

- **Require user to reset PIN on first telephone logon**: Select this check box to force the user to reset the UM PIN the first time that the user accesses the UM system from a telephone.

  > TIP: To help protecting mailbox data, One Identity recommends selecting this option, as changing the PIN after the first login is a security best practice.

- **Require user to reset PIN at first logon**: Select this check box to force the user to change the UM PIN the first time that the user accesses the UM system from a telephone after you reset the PIN.

  > TIP: To help protecting mailbox data, One Identity recommends selecting this option, as changing the PIN after the first login is a security best practice.

3. Do one of the following, depending on whether you are using the Active Roles Console or Web Interface:

   - In the Active Roles Console, click **Next** and wait while Active Roles performs the task. Then, click **Finish** to complete the wizard.
   - In the Web Interface, click **Finish** and wait while Active Roles performs the task.

Disabling Unified Messaging for a user

You can disable Unified Messaging (UM) for a UM-enabled user, so that the user cannot use the UM features of Microsoft Exchange Server. However, even if UM is disabled for a user, its UM settings are kept, so you can reenable them later at any time.

To disable Unified Messaging for a user by using the Active Roles Console

1. Right-click the user, then click **Exchange Tasks**.
2. Follow the steps in the Exchange Task wizard.
3. On the **Available Tasks** page in the Exchange Task wizard, click **Disable Unified Messaging**, then click **Next**.

   > NOTE: This setting appears only for users who have UM enabled.

4. On the **Disable Unified Messaging** page in the Exchange Task wizard, click **Next** to confirm that you want to disable UM for the user.
5. Wait while Active Roles performs the task.
6. Click **Finish** on the completion page of the wizard.

> TIP: You can also disable UM for a UM-enabled user via the Active Roles Web Interface. To do so, in the Web Interface, click the user, then click **Disable Unified Messaging**. As with the Exchange Task wizard in the Active Roles Console, the **Disable Unified Messaging** command only appears for users who have UM enabled.

About us

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

Contacting us

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

Technical support resources

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

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

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