



Active Roles 8.0 LTS

# Built-in Access Templates Reference Guide

**Copyright 2024 One Identity LLC.**

**ALL RIGHTS RESERVED.**

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

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

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

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

Refer to our 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](http://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 Built-in Access Templates Reference Guide  
Updated - 15 November 2024, 17:16

For the most recent documents and product information, see [Online product documentation](#).

# Contents

<b>Introduction</b> .....	<b>5</b>
<b>About built-in Active Roles Access Templates</b> .....	<b>6</b>
<b>Active Directory</b> .....	<b>7</b>
Active Directory – General ATs .....	8
Active Directory – Advanced ATs .....	15
Active Directory – Best Practices ATs .....	25
Active Directory – DNS Admins Role ATs .....	26
Active Directory – Domain Configuration Operators Role ATs .....	27
Active Directory – Forest Configuration Operators Role ATs .....	30
Active Directory – Replication Management Admins Role ATs .....	34
Active Directory – Replication Monitoring Operators Role ATs .....	36
Active Directory – Service Admin Managers Role ATs .....	37
<b>AD LDS (ADAM)</b> .....	<b>39</b>
AD LDS (ADAM) – General ATs .....	39
<b>Azure</b> .....	<b>41</b>
Azure – General ATs .....	41
Azure – Special ATs .....	47
<b>Built-in Security</b> .....	<b>48</b>
Built-in Security – General ATs .....	48
<b>Computer Resources</b> .....	<b>51</b>
Computer Resources – General ATs .....	51
Computer Resources – Advanced ATs .....	52
<b>Configuration</b> .....	<b>56</b>
Configuration – General ATs .....	56
Configuration – Advanced ATs .....	58
<b>Exchange</b> .....	<b>61</b>
Exchange – General ATs .....	61
Exchange – Advanced ATs .....	64

<b>Skype for Business Server</b> .....	<b>70</b>
Skype for Business Server – General ATs .....	70
<b>Starling</b> .....	<b>72</b>
Starling – General ATs .....	72
<b>User Interfaces</b> .....	<b>73</b>
User Interfaces – General ATs .....	73
<b>User Self-management</b> .....	<b>74</b>
User Self-management – General ATs .....	74
<b>About us</b> .....	<b>76</b>
Contacting us .....	76
Technical support resources .....	76

# Introduction

This document lists the built-in Access Templates (ATs) installed with Active Roles 8.0 LTS.

# About built-in Active Roles Access Templates

To help delegating administrative permissions for Active Directory (AD), Azure Active Directory (Azure AD), Exchange, Starling, or other miscellaneous resources in your organization, the Active Roles Console provides a set of built-in Access Templates (ATs).

With ATs, you can simplify the delegation of administrative tasks by assigning low-level permissions to your organizational resources, allowing administrators to manage them in the scope of the assigned ATs as a single unit.

With the built-in ATs of the Active Roles Console, you can:

- Delegate the most typical administrative roles within your organization. For more information on how to assign ATs, see *Applying Access Templates* in the *Active Roles Administration Guide*.
- Create your own custom ATs by using the built-in ones as a baseline. For more information, see *Creating an Access Template* in the *Active Roles Administration Guide*.

# Active Directory

The **Configuration > Access Templates > Active Directory** container of the Active Roles Console contains Access Templates (ATs) for delegating Active Directory (AD) service and data management tasks, for example:

- User and group management.
- Computer, printer queue and shared folder object management.
- Forest and domain configuration management.

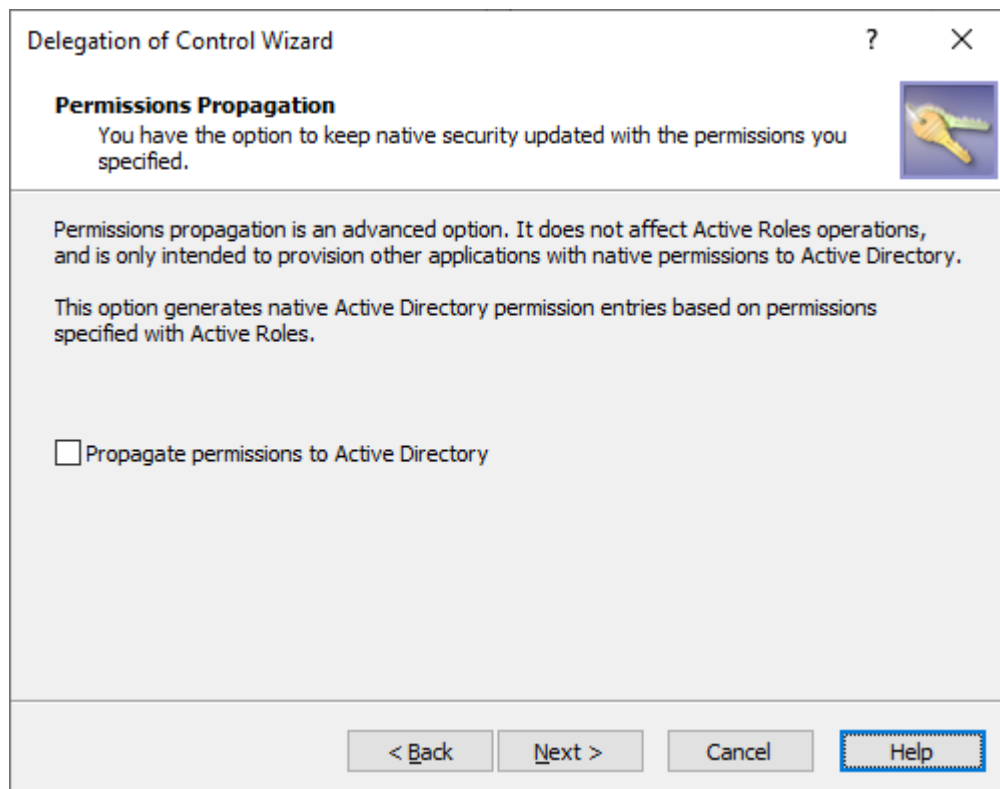
This container has two sub-containers:

- **Advanced** contains special AD ATs with very granular permissions. For more information, see [Active Directory – Advanced ATs](#).
- **Best Practices for Delegating Active Directory Administration** contains ATs for delegating service management to the most typical AD service management roles. For the list of these ATs, see [Active Directory – Best Practices ATs](#).
  - For more information about these best practices, their security sensitivity and impact, see the [Microsoft Windows Server documentation](#).
  - For more information on how to configure these ATs within the Active Roles Console, see the **Description** of the applicable AT.

**IMPORTANT:** Consider the following when configuring **Active Directory** ATs:

- To ensure that all appropriate permission entries are added to AD when configuring service management-specific ATs, always select the **Propagate permissions to Active Directory** option in the **Permissions Propagation** step of the **Delegation of Control Wizard**.

**Figure 1: Delegation of Control Wizard – Permissions propagation**



For more information on how to configure ATs for resource objects in your organization with the Active Roles Console, see *Applying Access Templates* in the *Active Roles Administration Guide*.

- Active Roles does not support configuring ATs for the *Schema* container. To do so, use native Microsoft tools, such as ADSI Edit.

## Active Directory – General ATs

To delegate data management tasks for the resources stored in your Active Directory AD environment, use the Access Templates (ATs) in the root of the **Configuration > Access Templates > Active Directory** container of the Active Roles Console. Such data management tasks include managing users, groups, printers, or computers.

**Table 1: Active Directory – General data management Access Templates**

Access Template	Description
<b>All Objects - Full Control</b>	Grants full permission to perform any administrative operation on any object in AD.

Access Template	Description
<b>All Objects - Read All Properties</b>	<p><b>TIP:</b> Use this AT to delegate complete permission to data administrators who are expected to carry out any and all AD content management tasks in your organization.</p> <p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>List directory objects.</li> <li>View all properties of any object in AD.</li> </ul>
<b>All Objects - View or Restore Deleted Objects</b>	<p>Grants the permission to view or restore AD objects deleted from a container.</p> <p><b>TIP:</b> Apply this AT to the container whose deleted objects the data administrators should be able to view or restore.</p> <p>For more information on how to configure ATs for resource objects in your organization with the Active Roles Console, see <i>Applying Access Templates</i> in the <i>Active Roles Administration Guide</i>.</p>
<b>Claim Types - Full Control</b>	<p>Grants full permission to:</p> <ul style="list-style-type: none"> <li>Create new claim types.</li> <li>Perform all administrative operations on existing claim types.</li> </ul> <p>Claim types determine the claims to issue for an AD security principal upon its authentication, and are used to define permissions when authoring claim-based access rules.</p>
<b>Claim Types - Modify All Properties</b>	<p>Grants permission to view or change all claim type properties.</p>
<b>Claim Types - Read All Properties</b>	<p>Grants permission to list claim types and view all claim type properties.</p>
<b>Computers - Create Computer Accounts</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>Create new computer accounts.</li> <li>View all properties of computer accounts.</li> </ul>
<b>Computers - Full Control</b>	<p>Grants full permission to:</p> <ul style="list-style-type: none"> <li>Create new computer accounts.</li> <li>Perform all administrative tasks on existing computer accounts.</li> </ul>
<b>Computers - Modify All Properties</b>	<p>Grants permission to view or change all properties of computer accounts.</p>

<b>Access Template</b>	<b>Description</b>
<b>Computers - Move Computer Accounts</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Move computer accounts.</li> <li>• View all properties of computer accounts.</li> </ul>
<b>Computers - Read All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• List computer accounts.</li> <li>• View all properties of computer accounts.</li> </ul>
<b>Computer - Reset Computer Accounts</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Reset computer accounts.</li> <li>• View all properties of computer accounts.</li> </ul>
<b>Contacts - Create Contacts</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Create new contacts.</li> <li>• View all contact properties.</li> </ul>
<b>Contacts - Full Control</b>	Grants full permission to: <ul style="list-style-type: none"> <li>• Create new contacts.</li> <li>• Perform all administrative operations on existing contacts.</li> </ul>
<b>Contacts - Modify All Properties</b>	Grants permission to view or modify all contact properties.
<b>Contacts - Modify Picture</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• View or change the image, that is, the thumbnailPhoto attribute.</li> <li>• View all contact properties.</li> </ul>
<b>Contacts - Read All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• List contacts.</li> <li>• View all contact properties.</li> </ul>
<b>Domains - Read All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• List domain objects.</li> <li>• View all properties of domain objects.</li> </ul>
<b>gMSA - Full Control</b>	Grants full permission to: <ul style="list-style-type: none"> <li>• Create new group Managed Service Accounts (gMSAs).</li> <li>• Perform all administrative operations on existing gMSAs.</li> </ul>

<b>Access Template</b>	<b>Description</b>
<b>gMSA - Modify All Properties</b>	Grants permission to view or change all gMSA properties.
<b>gMSA - Modify Membership Policy</b>	Grants permission to view or change the list of computers and computer groups allowed to use a specific gMSA.
<b>gMSA - Read All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• List gMSAs.</li> <li>• View all gMSA properties.</li> </ul>
<b>Groups - Add/Remove Members</b>	Grants permission to view or modify the members of groups.
<b>Groups - Create Groups</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Create new groups.</li> <li>• View all group properties.</li> </ul>
<b>Groups - Full Control</b>	Grants full permission to: <ul style="list-style-type: none"> <li>• Create new groups.</li> <li>• Perform all administrative operations on existing groups.</li> </ul>
<b>Groups - Manage Dynamic Groups</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Configure rule-based membership rules for dynamic groups.</li> <li>• View all group properties.</li> <li>• List groups in AD containers.</li> <li>• List AD containers.</li> </ul>
<b>Groups - Modify All Properties</b>	Grants permission to view or modify all group properties.
<b>Groups - Modify Picture</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• View or change the image, that is, the thumbnailPhoto attribute.</li> <li>• View all group properties.</li> </ul>
<b>Groups - Perform Deprovision Tasks</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Deprovision groups.</li> <li>• View all group properties.</li> </ul>

**TIP:** Use this AT to delegate group deprovisioning permissions to

Access Template	Description
<b>Groups - Perform Undo Deprovision Tasks</b>	<p data-bbox="448 297 1362 365">data administrators without also delegating group create and group delete permissions.</p> <p data-bbox="448 383 895 416">Grants the following permissions:</p> <ul data-bbox="496 439 868 517" style="list-style-type: none"> <li data-bbox="496 439 740 472">• Restore groups.</li> <li data-bbox="496 488 868 517">• View all group properties.</li> </ul> <p data-bbox="448 539 1362 607"><b>TIP:</b> Use this AT to delegate the permission of performing the <b>Undo Deprovisioning</b> command on groups only.</p>
<b>Groups - Read all Properties</b>	<p data-bbox="448 629 895 663">Grants the following permissions:</p> <ul data-bbox="496 685 868 763" style="list-style-type: none"> <li data-bbox="496 685 683 719">• List groups.</li> <li data-bbox="496 734 868 763">• View all group properties.</li> </ul>
<b>OUs - Create OUs</b>	<p data-bbox="448 786 895 819">Grants the following permissions:</p> <ul data-bbox="496 842 1050 920" style="list-style-type: none"> <li data-bbox="496 842 1050 875">• Create new Organizational Units (OUs).</li> <li data-bbox="496 891 831 920">• View all OU properties.</li> </ul>
<b>OUs - Full Control</b>	<p data-bbox="448 943 783 976">Grants full permission to:</p> <ul data-bbox="496 999 1134 1077" style="list-style-type: none"> <li data-bbox="496 999 751 1032">• Create new OUs.</li> <li data-bbox="496 1048 1134 1077">• Perform all administrative operations on OUs.</li> </ul>
<b>OUs - Modify All Properties</b>	<p data-bbox="448 1099 1166 1133">Grants permission to view or modify all OU properties.</p>
<b>OUs - Read All Properties</b>	<p data-bbox="448 1189 895 1223">Grants the following permissions:</p> <ul data-bbox="496 1245 831 1323" style="list-style-type: none"> <li data-bbox="496 1245 647 1279">• List OUs.</li> <li data-bbox="496 1294 831 1323">• View all OU properties.</li> </ul>
<b>Printers - Full Control</b>	<p data-bbox="448 1346 783 1379">Grants full permission to:</p> <ul data-bbox="496 1402 1385 1480" style="list-style-type: none"> <li data-bbox="496 1402 979 1435">• Create new printer queue objects.</li> <li data-bbox="496 1451 1385 1480">• Perform all administrative operations on existing printer queues.</li> </ul>
<b>Printers - Modify All Properties</b>	<p data-bbox="448 1503 1305 1536">Grants permission to view or modify all printer queue properties.</p>
<b>Printers - Read All Properties</b>	<p data-bbox="448 1615 895 1648">Grants the following permissions:</p> <ul data-bbox="496 1671 970 1749" style="list-style-type: none"> <li data-bbox="496 1671 874 1704">• List printer queue objects.</li> <li data-bbox="496 1720 970 1749">• View all printer queue properties.</li> </ul>
<b>Shared</b>	<p data-bbox="448 1771 783 1805">Grants full permission to:</p>

<b>Access Template</b>	<b>Description</b>
<b>Folders - Full Control</b>	<ul style="list-style-type: none"> <li>• Create new shared folder objects.</li> <li>• Perform all administrative operations on existing shared folders.</li> </ul>
<b>Shared Folders - Modify All Attributes</b>	Grants permissions to view or modify all shared folder properties.
<b>Shared Folders - Read All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• List shared folders.</li> <li>• View all shared folder properties.</li> </ul>
<b>Users - Create User Accounts</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Create new user accounts.</li> <li>• View all user account properties.</li> </ul>
<b>Users - Delete User Accounts</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Delete user accounts.</li> <li>• View all user account properties.</li> </ul>
<b>Users - Full Control</b>	Grants full permission to: <ul style="list-style-type: none"> <li>• Create new user accounts.</li> <li>• Perform all administrative operations on existing user accounts.</li> </ul>
<b>Users - Help Desk</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Reset user passwords.</li> <li>• Unlock user accounts.</li> <li>• Assign or remove digital (X.509) certificates from user accounts.</li> <li>• View all user account properties.</li> </ul> <p><b>TIP:</b> One Identity recommends using this AT to delegate permissions required for the day-to-day operations of your helpdesk service.</p>
<b>Users - Modify All Properties</b>	Grants permission to view or modify all user account properties.
<b>Users - Modify Personal Data</b>	Grants permission to manage the basic HR-related properties of user accounts.
<b>Users - Modify Picture</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• View or change the image, that is, the thumbnailPhoto attribute.</li> <li>• View all user account properties.</li> </ul>

Access Template	Description
<b>Users - Move User Accounts</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• Move user accounts.</li> <li>• View all user account properties.</li> </ul>
<b>Users - Pager &amp; Cell Phone Numbers</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• View and modify the mobile phone and pager number information of the user accounts.</li> <li>• View all user account properties.</li> </ul>
<b>Users - Perform Deprovision Tasks</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• Deprovision user accounts and other user-related resources.</li> <li>• View all user account properties.</li> </ul> <p><b>TIP:</b> Use this AT to delegate user deprovisioning permissions to data administrators without also delegating user create and user delete permissions.</p>
<b>Users - Perform Undo Deprovision Tasks</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• Restore user accounts.</li> <li>• View all user account properties.</li> </ul> <p><b>TIP:</b> Use this AT to delegate the permission of performing the <b>Undo Deprovisioning</b> command on user accounts only.</p>
<b>Users - Phone Number &amp; Address</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• Modify the address and telephone number properties of user accounts.</li> <li>• View all user account properties.</li> </ul>
<b>Users - Read All Properties</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• List user accounts.</li> <li>• View all user account properties.</li> </ul>
<b>Users and Groups - Basic Management</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• List groups and user accounts.</li> <li>• Add or remove users and groups to or from groups.</li> <li>• Reset user passwords.</li> <li>• View or modify the login-related properties of user accounts.</li> </ul>

# Active Directory – Advanced ATs

To delegate more granular data management permissions for the resources stored in your Active Directory (AD) environment, use the Access Templates (ATs) in the **Configuration > Access Templates > Active Directory > Advanced** container of the Active Roles Console.

These ATs contain more granular data management tasks for computer objects, contacts, domains, groups, Organizational Units (OUs), printers, shared folders and users.

**Table 2: Active Directory – Advanced data management Access Templates**

Access Template	Description
<b>Computer Objects – Create</b>	Grants permission to create computer objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Computer Objects – Delete</b>	Grants permission to delete computer objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Computer Objects – List</b>	Grants permission to list computer objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Computer Objects – Read/Write Account Restrictions</b>	Grants permission to view or modify properties that set account restrictions for computer objects (that is, the User-Account-Restrictions property set of computer objects). For more information on the affected properties, see <a href="#">User-Account-Restrictions property set</a> in the <i>Microsoft Active Directory Schema documentation</i> .
<b>Computer Objects – Read/Write General Information</b>	Grants permission to view or modify the following general information properties of computer objects: <ul style="list-style-type: none"> <li>• Computer name (pre-Windows 2000)</li> <li>• DNS name</li> <li>• Role</li> <li>• Description</li> <li>• Flags controlling password, lockout, and computer disable/enable behavior (that is, the <b>User Account Control</b> attribute)</li> </ul>
<b>Computer Objects – Read/Write Manager</b>	Grants permission to view or modify the person assigned to the management of the computer resource (that is, the <b>Managed By</b> attribute of the computer).   <b>NOTE:</b> This AT provides no additional permissions.
<b>Computer Objects –</b>	Grants permission to view or modify the personal information properties of computer objects (that is, the Personal-Information property set of computer objects).

Access Template	Description
<b>Read/Write Personal Information</b>	For more information on the affected properties, see <a href="#">Personal-Information property set</a> in the <i>Microsoft Active Directory Schema documentation</i> .
<b>Computer Objects – Read/Write Public Information</b>	Grants permission to view or modify the public information properties of computer objects (that is, the Public-Information property set of computer objects). For more information on the affected properties, see <a href="#">Public-Information property set</a> in the <i>Microsoft Active Directory Schema documentation</i> .
<b>Computer Objects - Reset Computer Accounts</b>	Grants permission to reset computer accounts. <b>  NOTE:</b> This AT provides no additional permissions.
<b>Computer Objects - View BitLocker Recovery Keys</b>	Grants the permission to search and view all properties of computer child objects that contain a Full Volume Encryption recovery password in their associated globally unique identifier (GUID). <b>  TIP:</b> Use this AT to delegate the task of retrieving BitLocker recovery keys stored in AD.
<b>Contacts – Create</b>	Grants permission to create contact objects. <b>  NOTE:</b> This AT provides no additional permissions.
<b>Contacts – Delete</b>	Grants permission to delete contact objects. <b>  NOTE:</b> This AT provides no additional permissions.
<b>Contacts – Read Group Membership</b>	Grants permission to view the list of groups to which the contact object belongs. <b>  NOTE:</b> This AT provides no additional permissions.
<b>Contacts – Read/Write Organizational Information</b>	Grants permission to view or modify the following organizational properties of the contact: <ul style="list-style-type: none"> <li>• Job title</li> <li>• Department</li> <li>• Company</li> <li>• Employee ID</li> <li>• Manager</li> <li>• Office location</li> </ul>
<b>Contacts – Read/Write Personal</b>	Grants permission to view or modify the personal information properties of contacts (that is, the Personal-Information property set of contacts).

Access Template	Description
<b>Information</b>	For more information on the affected properties, see <a href="#">Personal-Information property set</a> in the <i>Microsoft Active Directory Schema documentation</i> .
<b>Contacts – Read/Write Web Information</b>	Grants permission to view or modify the web-related information properties of contacts (that is, the Web-Information property set of contacts).  For more information on the affected properties, see <a href="#">Web-Information property set</a> in the <i>Microsoft Active Directory Schema documentation</i> .
<b>Contacts – Rename</b>	Grants permission to rename contact objects.    <b>NOTE:</b> This AT provides no additional permissions.
<b>Domains – Change PDC</b>	Grants permission to change the role owner of the Primary Domain Controller (PDC) Emulator.    <b>NOTE:</b> This AT provides no additional permissions.
<b>Domains – Delegate Control and Enforce Active Roles Server Policy</b>	Grants permission to apply Active Roles ATs and Policy Objects to domain objects.    <b>NOTE:</b> This AT provides no additional permissions.
<b>Domains – Generate Resultant Set of Policy (Logging)</b>	Grants permission to generate Group Policy Result data for the users and/or computers in a specific domain.
<b>Domains – Generate Resultant Set of Policy (Planning)</b>	Grants permission to generate Group Policy Modeling data for the users and/or computers in a specific domain. Administrators can use Group Policy modeling to troubleshoot Group Policy settings and testing GPOs before deploying them in a live environment.
<b>Domains – List</b>	Grants permission to list domain objects.    <b>NOTE:</b> This AT provides no additional permissions.
<b>Domains – Read/Write General Information</b>	Grants permission to view or modify the following general information properties of domain objects: <ul style="list-style-type: none"> <li>• Domain name (pre-Windows 2000)</li> <li>• Description</li> </ul>
<b>Domains – Read/Write Manager</b>	Grants permission to view or modify the person assigned to the management of a domain (that is, the <b>Managed By</b> attribute of the domain).    <b>NOTE:</b> This AT provides no additional permissions.

Access Template	Description
<b>Domains – Read/Write Other Domain Parameters</b>	<p>Grants permission to view or modify properties permitting control to a list of domain attributes (that is, the Domain-Other-Parameters property set of domains).</p> <p>For more information on the affected properties, see <a href="#">Domain-Other-Parameters property set</a> in the <i>Microsoft Active Directory Schema documentation</i>.</p>
<b>Domains – Read/Write Password &amp; Lockout Policies</b>	<p>Grants permission to view or modify lockout and password expiration related properties on the user accounts of a domain (that is, the Domain-Password property set of domains).</p> <p>For more information on the affected properties, see <a href="#">Domain-Password property set</a> in the <i>Microsoft Active Directory Schema documentation</i>.</p>
<b>Group Policy Container – Apply Group Policy</b>	<p>Grants the extended right used by the Group Policy engine (that is, the <i>Apply-Group-Policy</i> extended right) to determine if a Group Policy Object (GPO) applies to a user and/or computer.</p>
<b>Groups – Add/Remove Self As Member</b>	<p>Grants permission to enable updating group membership via Self-Membership validated write (that is, allowing users to add or remove their own account from the group).</p>
<b>Groups – Copy</b>	<p>Grants permission to copy groups.</p> <p>  <b>NOTE:</b> This AT provides no additional permissions.</p>
<b>Groups – Create</b>	<p>Grants permission to create groups.</p> <p>  <b>NOTE:</b> This AT provides no additional permissions.</p>
<b>Groups – Delete</b>	<p>Grants permission to delete groups.</p> <p>  <b>NOTE:</b> This AT provides no additional permissions.</p>
<b>Groups - Deprovision</b>	<p>Grants permission to deprovision groups.</p> <p>  <b>NOTE:</b> This AT provides no additional permissions.</p>
<b>Groups – List</b>	<p>Grants permission to list groups.</p> <p>  <b>NOTE:</b> This AT provides no additional permissions.</p>
<b>Groups – Manage Membership Rules</b>	<p>Grants permission to view or modify the criteria of rule-based group membership assignments within Active Roles.</p> <p>  <b>NOTE:</b> This AT provides no additional permissions.</p>
<b>Groups – Read Group Membership</b>	<p>Grants permission to view the list of groups to which a specific group belongs.</p> <p>  <b>NOTE:</b> This AT provides no additional permissions.</p>

Access Template	Description
<b>Groups – Read/Write E-mail Address</b>	Grants permission to view or modify the list of email addresses for a group.
<b>Groups – Read/Write General Information</b>	Grants permission to view or modify the following general information properties of groups: <ul style="list-style-type: none"> <li>• Group name (pre-Windows 2000)</li> <li>• Description</li> <li>• E-mail</li> <li>• Group scope</li> <li>• Group type</li> <li>• Notes</li> </ul>
<b>Groups – Read/Write Group Members</b>	Grants permission to add or remove members to or from a group.
<b>Groups – Read/Write Group Type and Scope</b>	Grants permission to view or modify the type and scope settings of a group.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Groups – Read/Write Manager</b>	Grants permission to view or modify the person assigned to manage a specific group (that is, the <b>Managed By</b> attribute of the group).
<b>Groups – Read/Write Phone and Mail Options</b>	Grants permission to view or modify the email-related information properties of a group (that is, the Email-Information property set of group objects). For more information on the affected properties, see <a href="#">Email-Information property set</a> in the <i>Microsoft Active Directory Schema documentation</i> .
<b>Groups – Rename</b>	Grants permission to rename groups.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Groups - Undo Deprovision</b>	Grants permission to restore (that is, perform the <b>Undo Deprovision</b> action) on groups.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Groups - Undo Deprovision - Deny</b>	Grants permission to deny the restoration of group objects (that is, performing the <b>Undo Deprovision</b> action on them).
<b>Objects - Deny Deletion</b>	Grants permission to deny the deletion and sub-tree deletion of a specific object.

Access Template	Description
	<b>NOTE:</b> This AT provides no additional permissions.
<b>Objects - Deny Deletion of Child Objects</b>	Grants permission to deny deleting all child objects from a specific AD container.   <b>NOTE:</b> This AT provides no additional permissions.
<b>OUs – Create</b>	Grants permission to create Organizational Units (OUs).   <b>NOTE:</b> This AT provides no additional permissions.
<b>OUs – Delegate Control and Enforce Active Roles Server Policy</b>	Grants permission to apply Active Roles ATs and Policy Objects to an OU.   <b>NOTE:</b> This AT provides no additional permissions.
<b>OUs – Delete</b>	Grants permission to delete OUs.   <b>NOTE:</b> This AT provides no additional permissions.
<b>OUs – Generate Resultant Set of Policy (Logging)</b>	Grants permission to generate Group Policy Results data for the users and computers within the specific OU.
<b>OUs – Generate Resultant Set of Policy (Planning)</b>	Grants permission to generate Group Policy Modeling data for the users and computers within the specific OU.
<b>OUs – List</b>	Grants permission to list OUs.   <b>NOTE:</b> This AT provides no additional permissions.
<b>OUs – Read/Write General Information</b>	Grants permission to view or modify the following general information properties of OUs: <ul style="list-style-type: none"> <li>• Description</li> <li>• Street</li> <li>• City</li> <li>• State/province</li> <li>• Zip/Postal Code</li> <li>• Country/region</li> </ul>
<b>OUs – Read/Write Manager</b>	Grants permission to view or modify the person assigned to manage a specific OU (that is, the <b>Managed By</b> attribute of the OU).
<b>OUs – Rename</b>	Grants permission to rename OUs.   <b>NOTE:</b> This AT provides no additional permissions.

Access Template	Description
<b>Printer Objects – Create</b>	Grants permission to create printer queue objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Printer Objects – Delete</b>	Grants permission to delete printer queue objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Printer Objects – List</b>	Grants permission to list printer queue objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Printer Objects – Read/Write General Information</b>	Grants permission to view or modify the following general information properties of printer queue objects: <ul style="list-style-type: none"> <li>• Location</li> <li>• Model</li> <li>• Description</li> <li>• Color</li> <li>• Staple</li> <li>• Double-sided</li> <li>• Printing speed</li> <li>• Maximum resolution</li> </ul>
<b>Printer Objects – Read/Write Manager</b>	Grants permission to view or modify the person assigned to manage a specific printer (that is, the <b>Managed By</b> attribute of the printer).
<b>Printer Objects – Rename</b>	Grants permission to rename printer queue objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Shared Folders – Create</b>	Grants permission to create shared folder objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Shared Folders – Delete</b>	Grants permission to delete shared folder objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Shared Folders – List</b>	Grants permission to list shared folder objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Shared Folders – Read/Write General Information</b>	Grants permission to view or modify the following general information properties of shared folders: <ul style="list-style-type: none"> <li>• Description</li> <li>• UNC name</li> </ul>
<b>Shared Folders –</b>	Grants permission to view or modify the person assigned to manage

Access Template	Description
<b>Read/Write Manager</b>	a specific shared folder (that is, the <b>Managed By</b> attribute of the shared folder).
<b>Shared Folders – Rename</b>	Grants permission to rename shared folder objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Users - Assign/Remove Digital Certificates</b>	Grants permission to assign or remove digital (X.509) certificates to or from AD users ( that is, read or write the userCertificate attribute of user objects).
<b>Users - Change Password (Extended Right)</b>	Grants permission to change the password of users (that is, grants the User-Change-Password extended right).
<b>Users - Copy</b>	Grants the permission to copy user objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Users - Create</b>	Grants permission to create user objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Users - Delete</b>	Grants permission to delete user objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Users - Deprovision</b>	Grants permission to deprovision user objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Users - Enable/Disable Account</b>	Grants permission to enable or disable user objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Users - List</b>	Grants permission to list user objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Users - Read Group Membership</b>	Grants permission to view the list of groups the selected user is a member of.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Users - Read/Write Account Information</b>	Grants permission to view or modify the following account information properties of user objects: <ul style="list-style-type: none"> <li>• User logon name</li> <li>• User logon name (pre-Windows 2000)</li> <li>• Logon Hours</li> <li>• Last Logon</li> <li>• Account is locked out</li> </ul>

Access Template	Description
<b>Users - Read/Write Account Restrictions</b>	<ul style="list-style-type: none"> <li>• Account options</li> <li>• Account expires</li> </ul> <p>Grants permission to view or modify the account restriction properties of user objects (that is, the User-Account-Restrictions property set of user objects).</p> <p>For more information on the affected properties, see <a href="#">User-Account-Restrictions property set</a> in the <i>Microsoft Active Directory Schema documentation</i>.</p>
<b>Users - Read/Write Dial-In Properties</b>	<p>Grants permission to view or modify the following dial-in specific properties of user objects:</p> <ul style="list-style-type: none"> <li>• Remote Access Permission (Dial-in or VPN)</li> <li>• Verify Caller-ID</li> <li>• Callback Options</li> <li>• Assign a Static IP Address</li> <li>• Apply Static Routes Settings</li> </ul>
<b>Users - Read/Write General Information</b>	<p>Grants permission to view or modify the general information properties of user objects (that is, the General-Information property set of user objects).</p> <p>For more information on the affected properties, see <a href="#">General-Information property set</a> in the <i>Microsoft Active Directory Schema documentation</i>.</p>
<b>Users - Read/Write Logon Information</b>	<p>Grants permission to view or modify the logon information properties of user objects (that is, the User-Logon property set of user objects).</p> <p>For more information on the affected properties, see <a href="#">User-Logon property set</a> in the <i>Microsoft Active Directory Schema documentation</i>.</p>
<b>Users - Read/Write Organizational Information</b>	<p>Grants permission to view or modify the following organization-related properties of user objects:</p> <ul style="list-style-type: none"> <li>• Title</li> <li>• Department</li> <li>• Company</li> <li>• Manager</li> <li>• Direct reports</li> <li>• Office (General tab)</li> </ul>

Access Template	Description
<b>Users - Read/Write Personal Information</b>	<p>Grants permission to view or modify the personal information properties of user objects (that is, the Personal-Information property set of user objects).</p> <p>For more information on the affected properties, see <a href="#">Personal-Information property set</a> in the <i>Microsoft Active Directory Schema documentation</i>.</p>
<b>Users - Read/Write Phone and Mail Options</b>	<p>Grants permission to view or modify the email-related information properties of user objects (that is, the Email-Information property set of user objects).</p> <p>For more information on the affected properties, see <a href="#">Email-Information property set</a> in the <i>Microsoft Active Directory Schema documentation</i>.</p>
<b>Users - Read/Write Profile Properties</b>	<p>Grants permission to view or modify the following profile-related properties of user objects:</p> <ul style="list-style-type: none"> <li>• User profile</li> <li>• Home folder</li> </ul>
<b>Users - Read/Write Public Information</b>	<p>Grants permission to view or modify the public information properties of user objects (that is, the Public-Information property set of user objects).</p> <p>For more information on the affected properties, see <a href="#">Public-Information property set</a> in the <i>Microsoft Active Directory Schema documentation</i>.</p>
<b>Users - Read/Write Web Information</b>	<p>Grants permission to view or modify the web-related information properties of user objects (that is, the Web-Information property set of user objects).</p> <p>For more information on the affected properties, see <a href="#">Web-Information property set</a> in the <i>Microsoft Active Directory Schema documentation</i>.</p>
<b>Users - Read/Write WTS Properties</b>	<p>Grants permission to view or modify the following user object properties describing Terminal Services-related information:</p> <ul style="list-style-type: none"> <li>• Terminal Services user profile</li> <li>• Terminal Services home folder</li> <li>• Allow login to the terminal server</li> <li>• Starting program</li> <li>• Client devices</li> <li>• Terminal Service timeout and reconnection settings</li> </ul>
<b>Users - Rename</b>	Grants permission to rename user objects.

Access Template	Description
	<b>NOTE:</b> This AT provides no additional permissions.
<b>Users - Reset Password (Extended Right)</b>	Grants permission to reset the password of user objects (that is, grants the User-Reset-Password extended right).   <b>NOTE:</b> This AT provides no additional permissions.
<b>Users - Run Check Policy (Extended Right)</b>	Grants permission to use the <b>Check Policy</b> action on user objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Users - Undo Deprovision</b>	Grants permission to restore user objects (that is, performing the <b>Undo Deprovision</b> action on them).
<b>Users - Undo Deprovision - Deny</b>	Grants permission to deny the restoration of user objects (that is, performing the <b>Undo Deprovision</b> action on them).
<b>Users - Unlock Account</b>	Grants permission to unlock user objects that get locked due to reaching the limit of failed login attempts set in your organization.
<b>Users - View Change History (Extended Right)</b>	Grants permission to use the <b>Change History</b> and <b>User Activity</b> actions on user objects.
<b>Users - View Delegated Rights (Extended Right)</b>	Grants permission to use the <b>Delegated Rights</b> action on user objects.
<b>Users - View Digital Certificates</b>	Grants permission to view the digital (X.509) certificates assigned to the AD user (that is, the permission to read the userCertificate attribute of user objects).
<b>Users - View Entitlement Profile (Extended Right)</b>	Grants permission to use the <b>Entitlement Profile</b> action on user objects to view the resources to which the selected user object is entitled.
<b>Users - Write Password</b>	Grants permission to set the password of user objects.   <b>NOTE:</b> This AT provides no additional permissions.

## Active Directory – Best Practices ATs

To delegate permissions for performing the most typical service management roles in your Active Directory environment, use the Access Templates (ATs) in the **Configuration > Access Templates > Active Directory > Best Practices for Delegating Active Directory Administration** container of the Active Roles Console.

The ATs that are available in this container are grouped into additional sub-containers, in accordance with the operator, administrator or manager roles that they are recommended to be used with.

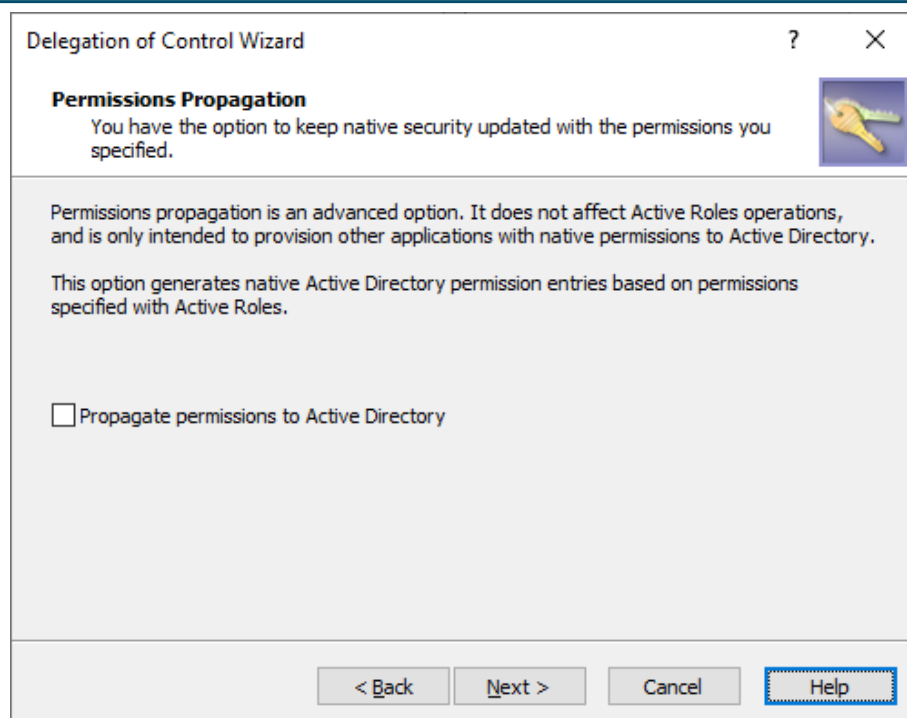
- For more information about these best practices, their security sensitivity and impact, see the [Microsoft Windows Server documentation](#).
- For more information on how to configure these ATs within the Active Roles Console, see the **Description** of the applicable AT.

## Active Directory – DNS Admins Role ATs

To delegate Microsoft Domain Name Server (DNS) management duties to administrators within your organization, use the Access Templates (ATs) available under the **Configuration > Access Templates > Active Directory > Best Practices for Delegating Active Directory Administration > DNS Admins Role** container of the Active Roles Console.

**Table 3: Active Directory – Best Practices for Delegating Active Directory Administration: DNS Admins Role Access Templates**

Access Template	Description
<b>DNS Admins - Microsoft DNS Management</b>	<p>Grants permission to perform management tasks on the Microsoft DNS servers within your organization.</p> <p>To delegate this AT, apply it on the following resources of your Active Directory tree in the Active Roles Console:</p> <ol style="list-style-type: none"> <li>1. <b>&lt;forest-root-domain&gt; &gt; ForestDnsZones &gt; MicrosoftDNS</b></li> <li>2. <b>&lt;domain&gt; &gt; System &gt; MicrosoftDNS</b></li> <li>3. <b>&lt;domain&gt; &gt; DomainDnsZones &gt; MicrosoftDNS</b></li> </ol> <p><b>IMPORTANT:</b> When configuring this AT, always select the <b>Propagate permissions to Active Directory</b> option in the <b>Permissions Propagation</b> step of the <b>Delegation of Control Wizard</b>.</p> <p><b>Figure 2: Delegation of Control Wizard – Permissions propagation</b></p>



For more information on how to configure ATs for resource objects in your organization with the Active Roles Console, see *Applying Access Templates* in the *Active Roles Administration Guide*.

## Active Directory – Domain Configuration Operators Role ATs

To delegate domain configuration duties to operators within your organization, use the Access Templates (ATs) available under the **Configuration > Access Templates > Active Directory > Best Practices for Delegating Active Directory Administration > Domain Configuration Operators Role** container of the Active Roles Console.

Domain configuration operators typically perform the following duties in an Active Directory (AD) organization:

- Create or remove replicas, that is, additional Domain Controllers (DC).
- Designate or dismiss a DC as a global catalog.
- Protect and manage the Organizational Unit (OU) of the default DC.
- Protect and manage the content stored in the **<domain> > System** container.
- Raise the domain functional level.

- Rename DCs.
- Restore the AD environment from backups.
- Transfer or seize the Relative Identifier (RID) master role.
- Transfer or seize the Primary Domain Controller (PDC) emulator master role.
- Transfer or seize the infrastructure master role.

**Table 4: Active Directory – Best Practices for Delegating Active Directory Administration: Domain Configuration Operators Role Access Templates**

<b>Access Template</b>	<b>Description</b>
<b>Domain Configuration Operators - Domain Controllers OU Management</b>	<p>Grants full permission to domain configuration, applied to all classes.</p> <p>To delegate this AT, select the trustee(s), then apply it to the <b>Domain Controllers</b> container of your AD environment:</p> <p><b>&lt;domain&gt; &gt; Domain Controllers</b></p>
<b>Domain Configuration Operators - Domain Management</b>	<p>Grants the following permissions, applied to all classes:</p> <ul style="list-style-type: none"> <li>• Add or remove replicas in the domain.</li> <li>• Modify the infrastructure master.</li> <li>• Modify the PDC.</li> <li>• Write the fsmoRoleOwner attribute.</li> <li>• Write the msDS-Behavior-Version attribute.</li> </ul> <p>To delegate this AT, select the trustee(s), then apply it on the root domain of your AD environment.</p>
<b>Domain Configuration Operators - Full Control for "Creator Owner"</b>	<p>Grants full permission in a Creator Owner role, applied to all classes.</p> <p>To delegate this AT, select the trustee(s) you want to assign as Creator Owner(s), then apply the AT to the site configuration container:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Sites</b></p>
<b>Domain Configuration Operators - Full Control on Computer Object</b>	<p>Grants full permission to perform domain configuration tasks on all computer objects.</p> <p>To delegate this AT, select the trustee(s), then apply the AT on the computer object that will be promoted to Domain Controller (DC).</p>
<b>Domain Configuration Operators - Infrastructure Master</b>	<p>Grants the following permissions, applied to all classes:</p> <ul style="list-style-type: none"> <li>• Write the fsmoRoleOwner attribute.</li> <li>• Modify the infrastructure master.</li> </ul>

Access Template	Description
<b>Management</b>	<p>To delegate this AT, select the trustee(s), then apply the AT to the AD infrastructure container:</p> <p><b>&lt;domain&gt; &gt; Infrastructure</b></p>
<b>Domain Configuration Operators - Replication Management</b>	<p>Grants the following domain-level configuration permissions:</p> <ul style="list-style-type: none"> <li>• Manage the replication topology, applied to all classes.</li> <li>• Replicate directory changes, applied to all classes</li> <li>• Monitor AD replication, applied to the Directory Management Domain (DMD).</li> <li>• Replicate all directory changes, applied to the DMD.</li> </ul> <p>To delegate this AT, select the trustee(s), then apply the AT to the following AD containers:</p> <ul style="list-style-type: none"> <li>• <b>&lt;domain&gt;</b></li> <li>• <b>&lt;forest-root-domain&gt; &gt; Configuration</b></li> </ul> <p><b>NOTE:</b> You must apply the permissions that are specified by this AT to the AD configuration schemas too. These are located in the following container:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Schema</b></p> <p>To apply the permissions to the <b>Schema</b> container, use native AD management tools, such as ADSI Edit.</p>
<b>Domain Configuration Operators - RID Master Management</b>	<p>Grants the following permissions, applied to all classes:</p> <ul style="list-style-type: none"> <li>• Modify the RID master.</li> <li>• Write the fSMORoleOwner attribute.</li> </ul> <p>To delegate this AT, select the trustee(s), then apply the AT to the AD RID manager container:</p> <p><b>&lt;domain&gt; &gt; System &gt; RID Managers</b></p>
<b>Domain Configuration Operators - Server Object Creation</b>	<p>Grants permission to create all server child objects in the domain, applied to all classes.</p> <p>To delegate this AT, select the trustee(s), then apply the AT to the AD server configuration container:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Sites &gt; &lt;site&gt; &gt; Servers</b></p>
<b>Domain Configuration Operators - Site</b>	<p>Grants permission to read all site objects in the domain, applied to all classes.</p> <p>To delegate this AT, select the trustee(s), then apply the AT to the AD</p>

Access Template	Description
<b>Objects - Read All Properties</b>	site configuration container: <b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Sites</b>
<b>Domain Configuration Operators - System Container Management</b>	Grants full permission to manage the AD <b>System</b> container, applied to all classes. To delegate this AT, select the trustee(s), then apply the AT to the AD system container of your domain: <b>&lt;domain&gt; &gt; System</b>

## Active Directory – Forest Configuration Operators Role ATs

To delegate forest configuration duties to operators within your organization, use the Access Templates (ATs) available under the **Configuration > Access Templates > Active Directory > Best Practices for Delegating Active Directory Administration > Forest Configuration Operators Role** container of the Active Roles Console.

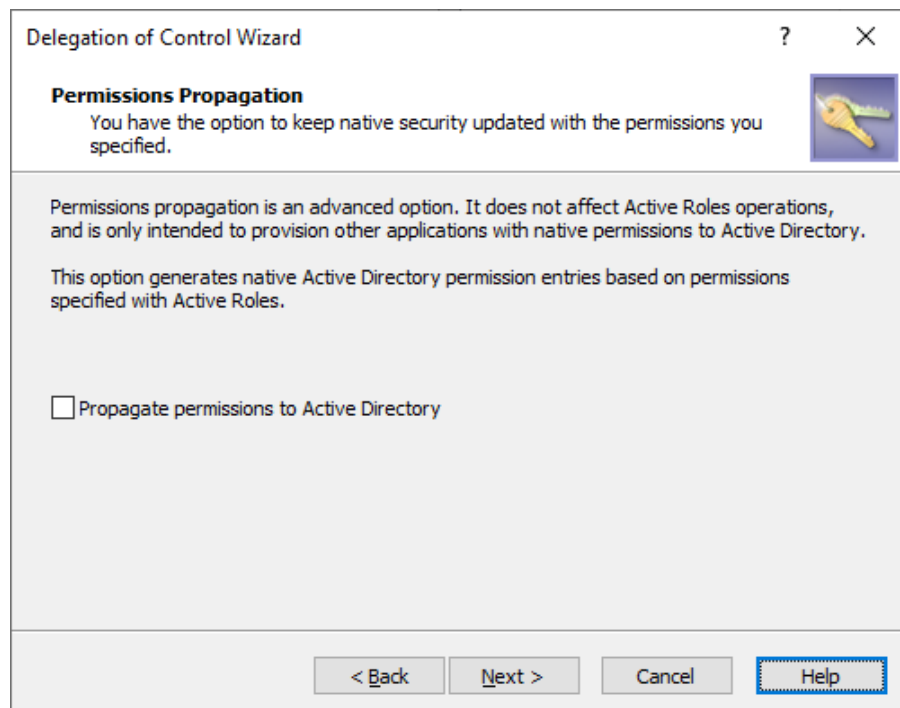
Forest configuration operators typically perform the following duties in an Active Directory (AD) organization:

- Add or remove top-level names and top-level name exclusions from a realm trust.
- Enable or disable placing name suffix (that is, top-level name) information on a realm trust.
- Modify the transitivity of a realm trust.
- Change trust direction.
- Create or delete trusts for all domains.
- Force the removal of a trust.
- Reset the trust passwords shared by a trust-pair.
- Create child domains in an existing domain tree.
- Demote the last Domain Controller (DC) in a child domain or forest-root domain.
- Transfer or seize the domain naming master role.
- Enable or disable name suffix routing for a specific suffix in a forest.
- Enable or the disable the Security Identifier (SID) history in outbound forest trusts.
- Enable or disable SID filtering.
- Enable selective authentication on an outbound forest or external trust.
- Raise the forest functional level.
- Manage all LDAP query policy-related administrative tasks.

**Table 5: Active Directory – Best Practices for Delegating Active Directory Administration: Forest Configuration Operators Role Access Templates**

Access Template	Description
<b>Forest Configuration Operators - Change Domain Master Management</b>	<p>Grants the following permissions, applied to all classes:</p> <ul style="list-style-type: none"> <li>• Modify the domain master.</li> <li>• Write the fsmoRoleOwner attribute.</li> </ul> <p>To delegate this AT, select the trustee(s), then apply it to the domain partitions container of your AD environment:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Partitions</b></p>
<b>Forest Configuration Operators - Change Schema Master Management</b>	<p>Grants permission to modify the schema master.</p> <p>To delegate this AT, select the trustee(s), then apply it to the domain schema container of your AD environment:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Schema</b></p> <p><b>IMPORTANT:</b> When configuring this AT, always select the <b>Propagate permissions to Active Directory</b> option in the <b>Permissions Propagation</b> step of the <b>Delegation of Control Wizard</b>.</p>

**Figure 3: Delegation of Control Wizard – Permissions propagation**



Access Template	Description
<b>Forest Configuration Operators - Computer Object Creation</b>	<p>For more information on how to configure ATs for resource objects in your organization with the Active Roles Console, see <i>Applying Access Templates</i> in the <i>Active Roles Administration Guide</i>.</p> <p>Grants permission to create computer objects in the forest, applied to all classes.</p> <p>To delegate this AT, select the trustee(s), then apply it to the <b>Domain Controllers</b> container of your AD environment:  <b>&lt;domain&gt; &gt; Domain Controllers</b></p> <p>This will apply the AT to every domain in your forest.</p>
<b>Forest Configuration Operators - Full Control for "Creator Owner"</b>	<p>Grants full permission to the Creator Owner role in your forest environment, applied to all classes.</p> <p>To delegate this AT, select the trustee(s) you want to assign as Creator Owner(s), then apply the AT to the site configuration container:  <b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Sites</b></p>
<b>Forest Configuration Operators - Full Control on Computer Object</b>	<p>Grants full permission to perform domain configuration tasks on all computer objects.</p> <p>To delegate this AT, select the trustee(s), then apply the AT on the computer object that will be promoted to Domain Controller (DC).</p>
<b>Forest Configuration Operators - NTDS Domain Controller Settings Management</b>	<p>Grants permission to write the queryPolicyObject attribute, applied to the NT Directory Services (NTDS) of the DC settings.</p> <p>To delegate this AT, select the trustee(s), then apply it to the DC NTDS settings container of your AD environment:  <b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Sites &gt; &lt;site&gt; &gt; Servers &gt; &lt;domain-controller&gt; &gt; NTDS Settings</b></p>
<b>Forest Configuration Operators - NTDS Site Settings Management</b>	<p>Grants permission to write the queryPolicyObject attribute, applied to the NTDS site settings.</p> <p>To delegate this AT, select the trustee(s), then apply it to the site NTDS settings container of your AD environment:  <b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Sites &gt; &lt;site&gt; &gt; NTDS Site Settings</b></p>
<b>Forest Configuration Operators - Query Policies</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• Create or delete Query Policy Objects, applied to all classes.</li> <li>• Write all properties of Query Policies.</li> </ul>

Access Template	Description
<b>Management</b>	<p>To delegate this AT, select the trustee(s), then apply it to the site NTDS query policies container of your AD environment:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Services &gt; Windows NT &gt; Directory Service &gt; Query-Policies</b></p>
<b>Forest Configuration Operators - Replication Management</b>	<p>Grants the following forest-level configuration permissions:</p> <ul style="list-style-type: none"> <li>• Manage the replication topology, applied to all classes.</li> <li>• Replicate directory changes, applied to all classes</li> <li>• Monitor AD replication, applied to the Directory Management Domain (DMD).</li> <li>• Replicate all directory changes, applied to the DMD.</li> </ul> <p>To delegate this AT, select the trustee(s), then apply the AT to the following AD container:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration</b></p> <p><b>NOTE:</b> You must apply the permissions that are specified by this AT to the AD configuration schemas too. These are located in the following container:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Schema</b></p> <p>To apply the permissions to the <b>Schema</b> container, use native AD management tools, such as ADSI Edit.</p>
<b>Forest Configuration Operators - Server Object Creation</b>	<p>Grants permission to create all server child objects in the forest, applied to all classes.</p> <p>To delegate this AT, select the trustee(s), then apply the AT to the AD server configuration container:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Sites &gt; &lt;site&gt; &gt; Servers</b></p>
<b>Forest Configuration Operators - Site Objects - Read All Properties</b>	<p>Grants permission to read all site objects in the forest, applied to all classes.</p> <p>To delegate this AT, select the trustee(s), then apply the AT to the AD site configuration container:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Sites</b></p>
<b>Forest Configuration Operators - Trust Relationship Management</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• Create or delete Trusted Domain objects, applied to all classes.</li> <li>• Write all properties of Trusted Domains.</li> </ul> <p>To delegate this AT, select the trustee(s), then apply it to the domain</p>

Access Template	Description
-----------------	-------------

system container of every domain in your forest:

**<domain> > System**

## Active Directory – Replication Management Admins Role ATs

To delegate replication management duties to administrators within your organization, use the Access Templates (ATs) available under the **Configuration > Access Templates > Active Directory > Best Practices for Delegating Active Directory Administration > Replication Management Admins Role** container of the Active Roles Console.

Replication management administrators typically perform the following duties in an Active Directory (AD) organization:

- Create, add, rename, or delete sites.
- Specify the location of a site.
- Create, add, or delete subnets.
- Specify the location of a subnet.
- Associate a subnet with a site.
- Create or delete site links.
- Add or remove sites to or from a site link.
- Modify the cost, replication period or replication schedule associated with a site link.
- Create or delete a site link bridge (object).
- Add or remove sites to or from a site link bridge.
- Create a single bridge for the entire network.
- Turn off the **Bridge all site links** option for IP/SMTP transport.
- Create or delete connections on demand.
- Take ownership of a Knowledge Consistency Checker (KCC) generated connection object.
- Manually set a schedule for connection objects.
- Enable or disable data compression for inter-site replication.
- Change the default setting for the intra-site replication schedule within a site.
- Designate or dismiss a preferred bridgehead server.
- Replace a failed preferred bridgehead server.
- Force replication or synchronization between two servers.

- Disable automatic topology generation or automatic cleanup for a site.
- Disable minimum hops topology for a site.
- Disable automatic stale server detection or automatic inter-site topology generation for a site.
- Disable inbound or outbound replication on a Domain Controller (DC).
- Enable reciprocal replication or change notification between sites (only for IP transport links).
- Force replication topology generation.

**Table 6: Active Directory – Best Practices for Delegating Active Directory Administration: Replication Management Admins Role Access Templates**

Access Template	Description
<b>Replication Management Admins - Inter-Site Transports Management</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• Create or delete Site Link objects, applied to all classes.</li> <li>• Write all properties of Site Links.</li> </ul> <p>To delegate this AT, select the trustee(s), then apply it to the inter-site transport container of the forest root domain:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Sites &gt; Inter-Site Transports</b></p>
<b>Replication Management Admins - Replication Topology Management</b>	<p>Grants permission to manage replication topology, applied to all classes.</p> <p>To delegate this AT, select the trustee(s), then apply it to the following AD containers:</p> <ul style="list-style-type: none"> <li>• <b>&lt;forest-root-domain&gt; &gt; Configuration</b></li> <li>• Every domain in the forest, including the forest root domain.</li> </ul> <p><b>NOTE:</b> You must apply the permissions that are specified by this AT to the AD configuration schemas too. These are located in the following container:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Schema</b></p> <p>To apply the permissions to the <b>Schema</b> container, use native AD management tools, such as ADSI Edit.</p>
<b>Replication Management Admins - Site Management</b>	<p>Grants the following permissions, applied to all classes:</p> <ul style="list-style-type: none"> <li>• Write all site properties.</li> <li>• Create or delete connection objects.</li> <li>• Create or delete site objects.</li> </ul> <p>To delegate this AT, select the trustee(s), then apply it to the site</p>

Access Template	Description
	configuration container of the forest root domain: <b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Sites</b>
<b>Replication Management Admins - Subnet Management</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Create or delete subnet objects, applied to all classes.</li> <li>• Write all subnet object properties.</li> </ul> <p>To delegate this AT, select the trustee(s), then apply it to the subnet configuration container of the forest root domain: <b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Sites &gt; Subnets</b></p>

## Active Directory – Replication Monitoring Operators Role ATs

To delegate replication monitoring duties to operators within your organization, use the Access Templates (ATs) available under the **Configuration > Access Templates > Active Directory > Best Practices for Delegating Active Directory Administration > Replication Monitoring Operators Role** container of the Active Roles Console.

Replication monitoring operators typically perform the following duties in an Active Directory (AD) organization:

- Check replication status.
- Get replication latency and summary information.
- Get the pending operations on a Domain Controller (DC).

**Table 7: Active Directory – Best Practices for Delegating Active Directory Administration: Replication Monitoring Operators Role Access Templates**

Access Template	Description
<b>Replication Monitoring Operators - Windows 2000</b>	Grants permission to manage replication topology, applied to all classes.  <b>NOTE:</b> Use this AT to configure replication monitoring in Windows 2000 AD environments.  To delegate this AT, select the trustee(s), then apply it to the following AD containers: <ul style="list-style-type: none"> <li>• <b>&lt;forest-root-domain&gt; &gt; Configuration</b></li> <li>• Every domain in the forest, including the forest root domain.</li> </ul>

Access Template	Description
<b>Replication Monitoring Operators - Windows Server 2003</b>	<p><b>NOTE:</b> You must apply the permissions that are specified by this AT to the AD configuration schemas too. These are located in the following container:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Schema</b></p> <p>To apply the permissions to the <b>Schema</b> container, use native AD management tools, such as ADSI Edit.</p> <p>Grants permission to monitor AD replication, applied to the Directory Management Domain (DMD).</p> <p><b>NOTE:</b> Use this AT to configure replication monitoring in Windows Server 2003 Active Directory environments.</p> <p>To delegate this AT, select the trustee(s), then apply it to the following AD containers:</p> <ul style="list-style-type: none"> <li>• <b>&lt;forest-root-domain&gt; &gt; Configuration</b></li> <li>• Every domain in the forest, including the forest root domain.</li> </ul> <p><b>NOTE:</b> You must apply the permissions that are specified by this AT to the AD configuration schemas too. These are located in the following container:</p> <p><b>&lt;forest-root-domain&gt; &gt; Configuration &gt; Schema</b></p> <p>To apply the permissions to the <b>Schema</b> container, use native AD management tools, such as ADSI Edit.</p>

## Active Directory – Service Admin Managers Role ATs

To delegate service administrator duties within your organization, use the Access Templates (ATs) available under the **Configuration > Access Templates > Active Directory > Best Practices for Delegating Active Directory Administration > Service Admin Managers Role** container of the Active Roles Console.

Service administrators typically manage and protect the following resources in a forest:

- All service administrator security groups.
- All service administrator accounts.

**Table 8: Active Directory – Best Practices for Delegating Active Directory Administration: DNS Admins Role Access Templates**

<b>Access Template</b>	<b>Description</b>
<b>Service Admin Managers - Admin SD Holder Management</b>	Grants full service administrator permissions, applied to all classes. To delegate this AT, select the trustee(s), then apply it to the <b>AdminSDHolder</b> container of every domain in your forest: <b>&lt;domain&gt; &gt; System &gt; AdminSDHolder</b>

# AD LDS (ADAM)

The **Configuration > Access Templates > AD LDS (ADAM)** container of the Active Roles Console contains Access Templates (ATs) for delegating Active Directory Lightweight Directory Services (AD LDS) data management tasks within your organization. These include managing AD LDS containers, groups, Organizational Units (OUs) and users.

## AD LDS (ADAM) – General ATs

To delegate data management tasks for the resources stored in your Active Directory Lightweight Directory Services (AD LDS) environment, use the Access Templates (ATs) in the root of the **Configuration > Access Templates > AD LDS (ADAM)** container of the Active Roles Console. Data management tasks include managing users, groups, printers, or computers.

**Table 9: AD LDS (ADAM) data management Access Templates**

Access Template	Description
<b>AD LDS Containers - Full Control</b>	Grants full permission to: <ul style="list-style-type: none"><li>• Create new AD LDS containers.</li><li>• Perform all administrative operations on existing AD LDS containers.</li></ul>
<b>AD LDS Containers - Modify All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"><li>• List all AD LDS containers.</li><li>• View or modify the properties of any AD LDS container.</li></ul>
<b>AD LDS Containers - Read All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"><li>• List all AD LDS containers.</li><li>• View the properties of any AD LDS container.</li></ul>
<b>AD LDS Groups - Add/Remove Members</b>	Grants the following permissions: <ul style="list-style-type: none"><li>• List all AD LDS groups.</li><li>• View or modify the members of AD LDS groups.</li></ul>
<b>AD LDS Groups - Full Control</b>	Grants full permission to: <ul style="list-style-type: none"><li>• Create new AD LDS groups.</li><li>• Perform all management tasks on existing AD LDS groups.</li></ul>

<b>Access Template</b>	<b>Description</b>
<b>AD LDS Groups - Modify All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List AD LDS groups.</li> <li>View or modify all properties of AD LDS groups.</li> </ul>
<b>AD LDS Groups - Read All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List AD LDS groups.</li> <li>View all properties of AD LDS groups.</li> </ul>
<b>AD LDS OUs - Full Control</b>	Grants full permission to: <ul style="list-style-type: none"> <li>Create new AD LDS Organizational Units (OUs).</li> <li>Perform all management tasks on existing AD LDS OUs.</li> </ul>
<b>AD LDS OUs - Modify All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List AD LDS OUs.</li> <li>View or modify all properties of AD LDS OUs.</li> </ul>
<b>AD LDS OUs - Read All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List AD LDS OUs.</li> <li>View all properties of AD LDS OUs.</li> </ul>
<b>AD LDS Users - Full Control</b>	Grants full permission to: <ul style="list-style-type: none"> <li>Create new AD LDS user accounts.</li> <li>Perform all management tasks on existing AD LDS user accounts.</li> </ul>
<b>AD LDS Users - Modify All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List AD LDS user accounts.</li> <li>View or modify all properties of AD LDS user accounts.</li> </ul>
<b>AD LDS Users - Read All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List AD LDS user accounts.</li> <li>View all properties of AD LDS user accounts.</li> </ul>
<b>All AD LDS Objects - Full Control</b>	Grants full permission to perform any management task on any AD LDS object.
<b>All AD LDS Objects - Read All Properties</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List all AD LDS objects.</li> <li>View all properties of any AD LDS object.</li> </ul>

The **Configuration > Access Templates > Azure** container of the Active Roles Console contains Access Templates (ATs) for managing Azure AD resources. These Azure AD resources include:

- Hybrid Azure configurations.
- Hybrid and cloud-only Azure users and guest users.
- Hybrid and cloud-only Azure contacts.
- Hybrid and cloud-only Azure groups.
- Microsoft 365 groups.

This container has a **Special** sub-container, containing an additional AT to facilitate searching for Azure resources in the Active Roles Web Interface. For more information, see [Azure – General ATs](#).

## Azure – General ATs

The **Configuration > Access Templates > Azure** container of the Active Roles Console contains Access Templates (ATs) to delegate Azure AD resource management tasks. Resource management tasks include searching, creating, reading, updating or deleting Azure tenants, users, guest users, groups and so on.

**Table 10: Azure AD data management Access Templates**

Access Template	Description
<b>Azure - Configuration Administrator</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Read and write Azure tenants.</li> <li>• Read and write Azure applications.</li> <li>• Read Azure health check reports.</li> <li>• Read Azure license reports.</li> <li>• Read Azure roles reports.</li> </ul>
<b>Azure - Contact Full Control</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Add and enable new Azure contacts.</li> <li>• View existing Azure contacts.</li> <li>• Update the properties of existing Azure contacts.</li> </ul>

Access Template	Description
<b>Azure - Full Control</b>	<p>Grants full permission to:</p> <ul style="list-style-type: none"> <li>• Read and write Azure configuration objects.</li> <li>• Read and write Azure user attributes.</li> <li>• Read and write Azure group attributes.</li> <li>• Read and write Azure M365 group objects.</li> </ul>
<b>Azure - Group Full Control</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• Add and enable new Azure groups.</li> <li>• View existing Azure groups.</li> <li>• Update the properties of existing Azure groups.</li> </ul>
<b>Azure - Health Check, O365 Roles Report and License Report</b>	<p>Grants permission to access the Azure health check, M365 roles and license reports.</p> <p><b>NOTE:</b> This Access Template must be applied on a <b>Configuration</b> container.</p>
<b>Azure - O365 Groups Full Control</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• Add and enable new Azure M365 groups.</li> <li>• View existing Azure M365 groups.</li> <li>• Update the properties of existing Azure M365 groups.</li> </ul>
<b>Azure - Read All Attributes</b>	<p>Grants permission to read all Azure attributes.</p> <p><b>NOTE:</b> This AT provides no additional permissions.</p>
<b>Azure - Read All Contact Attributes</b>	<p>Grants permission to read all Azure contact attributes.</p> <p><b>NOTE:</b> This AT provides no additional permissions.</p>
<b>Azure - Read All Group Attributes</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• List all Azure groups.</li> <li>• View all Azure group properties.</li> </ul>
<b>Azure - Read All O365 Group Attributes</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• List all Azure M365 groups.</li> <li>• View all Azure M365 group properties.</li> </ul>
<b>Azure - Read All User Attributes</b>	<p>Grants permission to read all Azure user and guest user attributes.</p> <p><b>NOTE:</b> This AT provides no additional permissions.</p>

Access Template	Description
<b>Azure - User Full Control</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Create new Azure user and guest user accounts.</li> <li>• Perform all administrative operations on existing Azure user and guest user accounts.</li> </ul>
<b>Azure Cloud Contact-Create Objects</b>	Grants permission to create cloud-only Azure contact accounts.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Cloud Contact - Delete Objects</b>	Grants permission to delete cloud-only Azure contact accounts.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Cloud Contact - Full Control</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Create new cloud-only Azure contact accounts.</li> <li>• Perform all administrative operations on existing cloud-only Azure contact accounts.</li> </ul>
<b>Azure Cloud Contact - Modify Objects</b>	Grants permission to modify cloud-only Azure contact accounts.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Cloud Contact - Read All Attributes</b>	Grants permission to read all cloud-only Azure contact attributes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Cloud User - Create Objects</b>	Grants permission to create cloud-only Azure user accounts.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Cloud User - Delete Objects</b>	Grants permission to delete cloud-only Azure user accounts.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Cloud User - Full Control</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Create new cloud-only Azure user accounts.</li> <li>• Perform all administrative operations on existing cloud-only Azure user accounts.</li> </ul>
<b>Azure Cloud User - Modify Objects</b>	Grants permission to modify cloud-only Azure user accounts.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Cloud User - Read All Attributes</b>	Grants permission to read all cloud-only Azure user attributes.   <b>NOTE:</b> This AT provides no additional permissions.

Access Template	Description
<b>Azure Create O365 Groups</b>	Grants permission to create M365 groups.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Distribution Groups - Create Objects</b>	Grants permission to create Azure distribution groups.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Distribution Groups - Delete Objects</b>	Grants permission to delete Azure distribution groups.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Distribution Groups - Full Control</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Add and enable new Azure distribution groups.</li> <li>• View existing Azure distribution groups.</li> <li>• Update the properties of existing Azure distribution groups.</li> </ul>
<b>Azure Distribution Groups - Modify Members</b>	Grants permission to modify the members of Azure distribution groups.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Distribution Groups - Modify Objects</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• List all Azure distribution groups.</li> <li>• Update all Azure distribution group properties.</li> </ul>
<b>Azure Distribution Groups - Read All Attributes</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• List all Azure distribution groups.</li> <li>• Read all Azure distribution group properties.</li> </ul>
<b>Azure Guest User - Create Objects</b>	Grants permission to create Azure guest user accounts.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Guest User - Delete Objects</b>	Grants permission to delete Azure guest user accounts.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Guest User - Full Control</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Create new Azure guest user accounts.</li> <li>• Perform all administrative operations on existing Azure guest user accounts.</li> </ul>

Access Template	Description
<b>Azure Guest User - Modify Objects</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List all Azure guest user accounts.</li> <li>Update all Azure guest user properties.</li> </ul>
<b>Azure Guest User - Read All Attributes</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List all Azure guest user accounts.</li> <li>Read all Azure guest user properties.</li> </ul>
<b>Azure Health Check Report</b>	Grants permission to access Azure health check reports. <b>NOTE:</b> This Access Template must be applied on a <b>Configuration</b> container.
<b>Azure License Report</b>	Grants permission to access Azure license reports. <b>NOTE:</b> This Access Template must be applied on a <b>Configuration</b> container.
<b>Azure Modify O365 Group Members</b>	Grants permission to modify the membership list of M365 groups.
<b>Azure O365 Roles Report</b>	Grants permission to access M365 roles reports. <b>NOTE:</b> This Access Template must be applied on a <b>Configuration</b> container.
<b>Azure Resource Mailboxes - Create Objects</b>	Grants permission to create Azure resource mailboxes. <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Resource Mailboxes - Delete Objects</b>	Grants permission to delete Azure resource mailboxes. <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Resource Mailboxes - Full Control</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>Add and enable new Azure resource mailboxes.</li> <li>View existing Azure resource mailboxes.</li> <li>Update the properties of existing Azure resource mailboxes.</li> </ul>
<b>Azure Resource Mailboxes - Modify Objects</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List all Azure resource mailboxes.</li> <li>Update the properties of Azure resource mailboxes.</li> </ul>

Access Template	Description
<b>Azure Resource Mailboxes - Read All Attributes</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List all Azure resource mailboxes.</li> <li>Read the properties of Azure resource mailboxes.</li> </ul>
<b>Azure Security Group - Create Objects</b>	Grants permission to create Azure security groups.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Security Group - Delete Objects</b>	Grants permission to delete Azure security groups.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Security Group - Full Control</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>Add and enable new Azure security groups.</li> <li>View existing Azure security groups.</li> <li>Update the properties of existing Azure security groups.</li> </ul>
<b>Azure Security Group - Modify Members</b>	Grants permission to modify the members of Azure security groups.
<b>Azure Security Group - Modify Objects</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List all Azure security groups.</li> <li>Update all Azure security group properties.</li> </ul>
<b>Azure Security Group - Read All Attributes</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List all Azure security groups.</li> <li>Read all Azure security group properties.</li> </ul>
<b>Azure Shared Mailboxes- Create Objects</b>	Grants permission to create Azure shared mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Shared Mailboxes - Delete Objects</b>	Grants permission to delete Azure shared mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Azure Shared Mailboxes - Full Control</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>Add and enable new Azure shared mailboxes.</li> <li>View existing Azure shared mailboxes.</li> <li>Update the properties of existing Azure shared mailboxes.</li> </ul>

Access Template	Description
<b>Azure Shared Mailboxes - Modify Members</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List all Azure shared mailboxes.</li> <li>Update all Azure shared mailbox properties.</li> </ul>
<b>Azure Shared Mailboxes - Read All Attributes</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>List all Azure shared mailboxes.</li> <li>Read all Azure shared mailbox properties.</li> </ul>

## Azure – Special ATs

The **Configuration > Access Templates > Azure > Special** container of the Active Roles Console contains Access Templates (ATs) to delegate miscellaneous Azure AD management permissions.

**Table 11: Azure AD special Access Templates**

Access Template	Description
<b>Azure Health Check Allow for Search</b>	Grants permission to read the Azure Health Check service so that the user(s) can search for Azure objects in the Active Roles Web Interface. <p><b>NOTE:</b> Make sure to grant this permission to non-administrator Active Roles users. Otherwise, they will be unable to perform searches on the Active Roles Web Interface.</p>

# Built-in Security

The **Configuration > Access Templates > Builtin** container of the Active Roles Console contains Access Templates (ATs) that you can use to:

- Delegate default security settings for your Active Roles server, covering both the various Active Roles components and the most common resource types managed in Active Roles.
- Use the default security ATs to configure your own security ATs.

## Built-in Security – General ATs

To delegate common Active Roles server security permissions for the resources and Active Roles components in your organization, use the Access Templates (ATs) in the root of the **Configuration > Access Templates > Builtin** container of the Active Roles Console.

**Table 12: Built-in security Access Templates**

Access Template	Description
<b>AR Server Security - Active Directory Container</b>	Grants the following permissions to ensure default security on the <b>Active Directory</b> container: <ul style="list-style-type: none"><li>• Read all domain properties.</li><li>• Write the LDAP server properties of the domain.</li><li>• List all Active Directory (AD) resources.</li><li>• Read all properties of AD resources.</li></ul>
<b>AR Server Security - Active Directory Container - Self</b>	Grants the following permissions to ensure default security on the <b>Active Directory</b> container for the security principal self: <ul style="list-style-type: none"><li>• Read the membership status of users (that is, their <b>Member Of</b> attribute).</li><li>• Read the object class of users (that is, their <b>objectClass</b> attribute).</li></ul>
<b>AR Server Security - AD LDS (ADAM) Container</b>	Grants the following permissions to ensure default security on the <b>AD LDS (ADAM)</b> container: <ul style="list-style-type: none"><li>• List all Active Directory Lightweight Directory Services (AD LDS) resources.</li><li>• Read all properties of AD LDS resources.</li></ul>

Access Template	Description
<b>AR Server Security - Application Configuration Objects</b>	<ul style="list-style-type: none"> <li>• Read all properties of <b>crossRefContainers</b>.</li> </ul> <p>Grants the following permissions to ensure default security on application configuration objects:</p> <ul style="list-style-type: none"> <li>• List and read all properties of <b>Schema Cache</b> containers.</li> <li>• List and read all properties of Enterprise Directory Service (EDS) application configuration objects.</li> <li>• List and read all properties of EDS display specifier containers.</li> <li>• List and read all properties of control access rights.</li> <li>• List and read all properties of attribute schemas.</li> <li>• List and read all properties of class schemas.</li> <li>• List and read all properties of all containers.</li> <li>• List and read all properties of display specifiers.</li> </ul>
<b>AR Server Security - Client Sessions Container</b>	<p>Grants the following permissions to ensure default security on the <b>Client Sessions</b> container:</p> <ul style="list-style-type: none"> <li>• Write the <b>Client Version</b> attribute of connected users.</li> <li>• Read the object class of connected users.</li> </ul>
<b>AR Server Security - Configuration Objects</b>	<p>Grants the following permissions to ensure default security on configuration objects:</p> <ul style="list-style-type: none"> <li>• List and read all properties of the <b>Managed Domains</b> container.</li> <li>• List and read all properties of the <b>Managed Units</b> container.</li> <li>• Read all properties of ATs.</li> <li>• List and read all properties of policy objects.</li> <li>• List and read all version information.</li> <li>• List and read all properties of the <b>Configuration</b> container.</li> <li>• List and read all properties of the change tracking log configuration.</li> <li>• Read all properties of the Active Roles Administration Service.</li> <li>• Read the edsvaXSLPolicyCheckReport attribute of the EDS policy check configuration.</li> <li>• List and read all properties of the EDS management history replication partner.</li> <li>• List and read all properties of the <b>Management History Databases</b> container.</li> </ul>

Access Template	Description
	<ul style="list-style-type: none"> <li>List and read all properties of the policy configuration.</li> <li>List and read all properties of the <b>Azure Configuration</b> container (that is, the edsAzureConfigurationContainer resource).</li> <li>List and read all properties of Azure containers.</li> <li>List and read all properties of Azure tenants.</li> </ul>
<b>AR Server Security - Export/Import Application</b>	<p>Grants the following permissions to ensure default security on the export/import application:</p> <ul style="list-style-type: none"> <li>Read the edsvaDSMLProcessingInstructionsAsXML attribute of applications.</li> <li>Read the edsvaAttributesExcludedFromImport attribute of applications.</li> <li>Read the object class of applications.</li> </ul>
<b>AR Server Security - Managed Units Container</b>	<p>Grants the following permissions to ensure default security on the <b>Managed Units</b> container:</p> <ul style="list-style-type: none"> <li>List all Managed Units.</li> <li>Read all properties of Managed Units.</li> </ul>
<b>AR Server Security - Web Interface Configuration</b>	<p>Grants the following permissions to ensure default security on the Active Roles Web Interface configuration objects:</p> <ul style="list-style-type: none"> <li>Read all Web Interface configuration data.</li> <li>Read and write the personal settings of Web Interface users.</li> </ul>
<b>AR Server Security - Workflow Container</b>	<p>Grants read permission to the <b>Workflow</b> container and its sub-containers.</p>
<b>Special - Block Permission Inheritance</b>	<p>When assigned to an object, this AT prevents propagating inheritable permissions to the children of the object and other target objects as well.</p> <p>When assigned to the <b>Active Directory</b> node, this AT blocks all inheritable AD permissions.</p>

# Computer Resources

The **Configuration > Access Templates > Computer Resources** container of the Active Roles Console contains Access Templates (ATs) that you can use to delegate computer resource management duties, such as:

- Local users and groups.
- Services.
- Network file shares (for example, shared directories).
- Printers and printing jobs.

This container has an **Advanced** sub-container, containing special ATs for computer resource management with highly granular permissions. For more information, see [Computer Resources – General ATs](#).

## Computer Resources – General ATs

To delegate common computer resource permissions in your organization, use the Access Templates (ATs) in the root of the **Configuration > Access Templates > Computer Resources** container of the Active Roles Console.

**Table 13: Computer Resources – General Access Templates**

Access Template	Description
<b>Computer Management - Full Control</b>	Grants full permission to: <ul style="list-style-type: none"><li>• List and select computer resources.</li><li>• Perform all management tasks on any computer.</li></ul>
<b>Computer Management - Local Account Operator</b>	Grants the following permissions: <ul style="list-style-type: none"><li>• Create, update, or delete local user accounts and groups on a computer.</li><li>• List and select computers.</li></ul>
<b>Computer Management - Network Share Operator</b>	Grants the following permissions: <ul style="list-style-type: none"><li>• Create, update, or delete network shares on a computer.</li><li>• List and select computers.</li></ul>
<b>Computer Management -</b>	Grants the following permissions:

Access Template	Description
<b>Print Operator</b>	<ul style="list-style-type: none"> <li>View or modify the properties of logical printers installed on a computer.</li> <li>List and select computers.</li> </ul>
<b>Computer Management - Read-Only Access</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>View the properties of all computer resources.</li> <li>List and select computers.</li> </ul>
<b>Computer Management - Server Operator</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>Start or stop services.</li> <li>Pause, resume or cancel printing.</li> <li>Create, update or delete network shares on a computer.</li> <li>List and select computers.</li> <li>List local users and groups.</li> <li>View all properties of local user accounts and groups on a computer.</li> </ul>
<b>Computer Management - Service Operator</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>Perform all management tasks on services on a computer.</li> <li>List and select computers.</li> </ul>

## Computer Resources – Advanced ATs

To delegate more granular computer resource management permissions in your environment, use the Access Templates (ATs) in the **Configuration > Access Templates > Computer Resources > Advanced** container of the Active Roles Console.

These ATs contain more granular resource management tasks for local groups, local users, printers, services, and shared resources.

**Table 14: Computer Resources – Advanced Access Templates**

Access Template	Description
<b>Local Groups - Add/Remove Members</b>	Grants permission to add or remove group members on a computer. <b>  NOTE:</b> This AT provides no additional permissions.
<b>Local Groups -</b>	Grants permission to create local groups on a computer.

Access Template	Description
<b>Create</b>	<a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Local Groups - Delete</b>	Grants permission to delete local groups on a computer.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Local Groups - List</b>	Grants permission to list the local groups on a computer.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Local Groups - Read/Write General Information</b>	Grants permission to view or modify the descriptions and membership lists of local groups on a computer.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Local Groups - Rename</b>	Grants permission to rename local groups on a computer.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Local Users - Create</b>	Grants permission to create local users on a computer.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Local Users - Delete</b>	Grants permission to delete local users on a computer.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Local Users - List</b>	Grants permission to list local users on a computer.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Local Users - Read Group Membership</b>	Grants permission to view the list of groups to which a local user belongs.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Local Users - Read/Write Account Options</b>	Grants permission to modify the account settings of local users, such as its password options, or whether the user is enabled, disabled, or locked out.
<b>Local Users - Read/Write General Information</b>	Grants permission to view or modify the full name and description of local users on a computer.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Local Users - Read/Write Profile Properties</b>	Grants permission to view or modify the user profile and home folder settings of local users on a computer.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Local Users - Rename</b>	Grants permission to rename local users on a computer.   <a href="#">NOTE</a> : This AT provides no additional permissions.

Access Template	Description
<b>Local Users - Write Password</b>	Grants permission to change the password of local users on a computer.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Printer Resources - Read/Write Advanced Information</b>	Grants permission to view or modify the following settings of logical printers: <ul style="list-style-type: none"> <li>• <b>Port</b></li> <li>• <b>Advanced</b></li> </ul>
<b>Printer Resources - Read/Write General Information</b>	Grants permission to view or modify the following settings of logical printers: <ul style="list-style-type: none"> <li>• <b>Name</b></li> <li>• <b>Location</b></li> <li>• <b>Comment</b></li> </ul>
<b>Printer Resources - Read/Write Sharing Information</b>	Grants permission to modify the sharing settings of logical printers (that is, enabling or disabling printer sharing).   <b>NOTE:</b> This AT provides no additional permissions.
<b>Services - List</b>	Grants permission to list the services defined on a computer.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Services - Read/Write General Information</b>	Grants permission to view or modify the following service settings: <ul style="list-style-type: none"> <li>• <b>Name</b></li> <li>• <b>Display Name</b></li> <li>• <b>Description</b></li> <li>• <b>Path to Executable</b></li> <li>• <b>Startup Type</b></li> </ul>
<b>Services - Read/Write Log On Information</b>	Grants permission to view or modify the <b>Log On As</b> setting of services.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Services - Read/Write Start type</b>	Grants permission to view or modify the <b>Startup Type</b> setting of services.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Services - Start /Stop/</b>	Grants permission to start, stop, pause, or resume services.   <b>NOTE:</b> This AT provides no additional permissions.

Access Template	Description
<b>Pause/Resume</b>	
<b>Shares - Create</b>	Grants permission to create network shares on a computer.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Shares - List</b>	Grants permission to list the network shares defined on a computer.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Shares - Read/Write General Information</b>	Grants permission to view or modify the following settings of network shares: <ul style="list-style-type: none"> <li>• <b>Share Name</b></li> <li>• <b>Path</b></li> <li>• <b>Comment</b></li> <li>• <b>User Limit</b></li> </ul>
<b>Shares - Read/Write Permissions</b>	Grants permission to view or modify share permissions on network shares.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Shares - Stop Sharing</b>	Grants permission to stop sharing folders on a computer.   <b>NOTE:</b> This AT provides no additional permissions.

# Configuration

The **Configuration > Access Templates > Configuration** container of the Active Roles Console contains Access Templates (ATs) that you can use to delegate Active Roles configuration object management duties, such as:

- Administering Managed Units (MUs), Policy Objects, or ATs.
- Configuring Active Roles replication.
- Adding or removing managed domains.

This container has an **Advanced** sub-container, containing special ATs to delegate configuration object management duties with very granular permissions. For more information, see [Computer Resources – Advanced ATs](#).

## Configuration – General ATs

To delegate common configuration object management permissions in your organization, use the Access Templates (ATs) in the root of the **Configuration > Access Templates > Configuration** container of the Active Roles Console.

**Table 15: Configuration – General Access Templates**

Access Template	Description
<b>Access Rules - Full Control</b>	<p>Grants full permission to create, read, update and delete Access Rule objects.</p> <p>To delegate this AT, apply it on the container(s) that hold Access Rule objects.</p> <p>For more information on applying ATs on resources, see <i>Applying Access Templates on a securable object</i> in the <i>Active Roles Administration Guide</i>.</p>
<b>Access Rules - Modify</b>	<p>Grants permission to view or modify all properties of Access Rule objects.</p> <p>To delegate this AT, apply it on the container(s) that hold Access Rule objects.</p> <p>For more information on applying ATs on resources, see <i>Applying Access Templates on a securable object</i> in the <i>Active Roles Administration Guide</i>.</p>
<b>Access Rules - View</b>	<p>Grants permission to view all properties of Access Rule objects.</p> <p>To delegate this AT, apply it on the container(s) that hold Access Rule</p>

Access Template	Description
<b>Automation Workflow - Full Control</b>	<p>objects.</p> <p>For more information on applying ATs on resources, see <i>Applying Access Templates on a securable object</i> in the <i>Active Roles Administration Guide</i>.</p>
<b>Automation Workflow - View</b>	<p>Grants full permission to:</p> <ul style="list-style-type: none"> <li>• View or modify automation workflow definitions.</li> <li>• Start automation workflows.</li> <li>• View the run history of automation workflows.</li> </ul> <p>To delegate this AT, apply it either to automation workflow definition objects, or to containers holding automation workflow definitions.</p> <p>For more information on applying ATs on resources, see <i>Applying Access Templates on a securable object</i> in the <i>Active Roles Administration Guide</i>.</p>
<b>Automation Workflow - View and Run</b>	<p>Grants permission to view automation workflow definitions and their run history.</p> <p>To delegate this AT, apply it either to automation workflow definition objects, or to containers holding automation workflow definitions.</p> <p>For more information on applying ATs on resources, see <i>Applying Access Templates on a securable object</i> in the <i>Active Roles Administration Guide</i>.</p>
<b>Configuration - Add/Remove Managed Domains</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• Read automation workflow definitions.</li> <li>• Start automation workflows.</li> <li>• View the run history of automation workflows.</li> </ul> <p>To delegate this AT, apply it either to automation workflow definition objects, or to containers holding automation workflow definitions.</p> <p>For more information on applying ATs on resources, see <i>Applying Access Templates on a securable object</i> in the <i>Active Roles Administration Guide</i>.</p>
<b>Configuration - Manage Access Templates</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• Register domains with Active Roles.</li> <li>• View or modify registration information for managed domains.</li> </ul> <p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• Create, read, update or delete ATs and AT containers.</li> </ul>

Access Template	Description
	<ul style="list-style-type: none"> <li>Add or remove permissions to or from ATs.</li> </ul>
<b>Configuration - Manage Configuration</b>	Grants permission to view or change any Active Roles configuration settings, except Active Roles replication settings.
<b>Configuration - Manage Policy Objects</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>Create, read, update or delete Active Roles Policy Objects and Policy Object containers.</li> <li>Configure Active Roles policies.</li> </ul>
<b>Configuration - Manage Script Modules</b>	Grants permission to create, read, update or delete Active Roles Script Modules and Script Module containers.
<b>Configuration - View Configuration</b>	Grants permission to view any Active Roles configuration settings, including replication settings.
<b>Managed Object Statistics - Read Detailed Data</b>	Grants permission to read detailed statistical information about the number of objects managed by Active Roles.
<b>Managed Object Statistics - View Report</b>	Grants permission to read the Active Roles product usage statistics, that is, statistical reports on the number of objects managed with the product.
<b>Workflow - View Workflow Containers</b>	Grants permission to access containers that hold workflow definition objects. To delegate this AT, apply it to the <b>Configuration &gt; Policies &gt; Workflow</b> node of the Active Roles Console. For more information on applying ATs on resources, see <i>Applying Access Templates on a securable object</i> in the <i>Active Roles Administration Guide</i> .

## Configuration – Advanced ATs

To delegate more granular configuration object management permissions in your environment, use the Access Templates (ATs) in the **Configuration > Access Templates > Configuration > Advanced** container of the Active Roles Console.

These ATs contain more granular configuration object management tasks for local groups, local users, printers, services and shared resources.

**Table 16: Configuration – Advanced Access Templates**

<b>Access Template</b>	<b>Description</b>
<b>Access Templates - Copy</b>	Grants permission to copy ATs.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Access Templates - Create</b>	Grants permission to create ATs.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Access Templates - Delete</b>	Grants permission to delete ATs.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Access Templates - List</b>	Grants permission to list ATs.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Access Templates - Read/Write Permissions</b>	Grants permission to view or modify the permission entries of ATs.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Access Templates - Rename</b>	Grants permission to rename ATs.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Policy Objects - Copy</b>	Grants permission to copy Active Roles Policy Objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Policy Objects - Create</b>	Grants permission to create Active Roles Policy Objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Policy Objects - Delete</b>	Grants permission to delete Active Roles Policy Objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Policy Objects - List</b>	Grants permission to list Active Roles Policy Objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Policy Objects - Read/Write Policy Entries</b>	Grants permission to view or modify policy definitions, that is, Policy Object entries in Active Roles Policy Objects.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Policy Objects - Rename</b>	Grants permission to rename Active Roles Policy Objects   <b>NOTE:</b> This AT provides no additional permissions.

Access Template	Description
<b>Script Modules - Copy</b>	Grants permission to copy Active Roles Script Modules.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Script Modules - Create</b>	Grants permission to create Active Roles Script Modules.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Script Modules - Delete</b>	Grants permission to delete Active Roles Script Modules.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Script Modules - List</b>	Grants permission to list Active Roles Script Modules.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Script Modules - Read/Write Script Text</b>	Grants permission to view or modify scripts stored in Active Roles Script Modules.   <a href="#">NOTE</a> : This AT provides no additional permissions.
<b>Script Modules - Rename</b>	Grants permission to rename Active Roles Script Modules.   <a href="#">NOTE</a> : This AT provides no additional permissions.

The **Configuration > Access Templates > Exchange** container of the Active Roles Console contains Access Templates (ATs) that you can use to delegate Microsoft Exchange recipient management duties, such as:

- Managing recipient settings.
- Using the Exchange Tasks Wizard.
- Managing email addresses.
- Configuring general and advanced message settings.

This container has an **Advanced** sub-container, containing special ATs for Microsoft Exchange resource management with very granular permissions. For more information, see [Computer Resources – Advanced ATs](#).

## Exchange – General ATs

To delegate common Microsoft Exchange management permissions in your organization, use the Access Templates (ATs) in the root of the **Configuration > Access Templates > Exchange** container of the Active Roles Console.

**NOTE:** Active Roles 8.0 LTS contains several outdated Exchange ATs. The name of these ATs contain the **(deprecated)** suffix, and are not listed in the following table.

**Table 17: Exchange – General Access Templates**

Access Template	Description
<b>Exchange - Configure Calendar Settings</b>	Grants the following permissions: <ul style="list-style-type: none"><li>• View or modify the <b>Calendar Settings</b> of Exchange recipients.</li><li>• List all Exchange users.</li><li>• View all Exchange properties of users.</li></ul>
<b>Exchange - Configure E-mail Addresses</b>	Grants the following permissions: <ul style="list-style-type: none"><li>• View or modify the <b>E-Mail Addresses</b> settings of Exchange recipients.</li><li>• List all Exchange users, groups and contacts.</li><li>• View all Exchange properties of users, groups and contacts.</li></ul>
<b>Exchange - Configure</b>	Grants the following permissions:

Access Template	Description
<b>Exchange Advanced Settings</b>	<ul style="list-style-type: none"> <li>• View or modify the <b>Advanced</b> Exchange settings of Exchange recipients.</li> <li>• List all Exchange users, groups and contacts.</li> <li>• View all Exchange properties of users, groups and contacts.</li> </ul>
<b>Exchange - Configure Exchange General Settings</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• View or modify the <b>General</b> Exchange settings of Exchange recipients.</li> <li>• List all Exchange users, groups and contacts.</li> <li>• View all Exchange properties of users, groups and contacts.</li> </ul>
<b>Exchange - Configure Mail Flow Settings</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• View or modify the <b>Mail Flow Settings</b> of Exchange recipients.</li> <li>• List all Exchange users, groups and contacts.</li> <li>• View all Exchange properties of users, groups and contacts.</li> </ul>
<b>Exchange - Configure Mailbox Features</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• View or modify the <b>Mailbox Features</b> settings of Exchange recipients.</li> <li>• List all Exchange users.</li> <li>• View all Exchange properties of users.</li> </ul>
<b>Exchange - Configure Mailbox Settings</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• View or modify the <b>Mailbox Settings</b> of Exchange recipients.</li> <li>• List all Exchange users.</li> <li>• View all Exchange properties of users.</li> </ul>
<b>Exchange - Configure Resource General Settings</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• View or modify the <b>Resource &gt; General</b> settings of Exchange recipients.</li> <li>• List all Exchange users.</li> <li>• View all Exchange properties of users.</li> </ul>
<b>Exchange - Configure Resource Information Settings</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• View or modify the <b>Resource &gt; Information</b> settings of Exchange recipients.</li> <li>• List all Exchange users.</li> <li>• View all Exchange properties of users.</li> </ul>

Access Template	Description
<b>Exchange - Configure Resource In-Policy Requests</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• View or modify the <b>Resource &gt; In-Policy Requests</b> settings of Exchange recipients.</li> <li>• List all Exchange users.</li> <li>• View all Exchange properties of users.</li> </ul>
<b>Exchange - Configure Resource Out-of-Policy Requests</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• View or modify the <b>Resource &gt; Out-of-Policy Requests</b> settings of Exchange recipients.</li> <li>• List all Exchange users.</li> <li>• View all Exchange properties of users.</li> </ul>
<b>Exchange - Configure Resource Policy</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• View or modify the <b>Resource &gt; Policy</b> settings of Exchange recipients.</li> <li>• List all Exchange users.</li> <li>• View all Exchange properties of users.</li> </ul>
<b>Exchange - Manage Resource, Linked and Shared Mailboxes</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Create, read, or update room mailboxes, equipment mailboxes, linked mailboxes and shared mailboxes.</li> <li>• List all Exchange users.</li> <li>• View all Exchange properties of users.</li> </ul>
<b>Exchange - Perform Exchange Tasks</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Create any kind of mailbox.</li> <li>• Use the <b>Exchange Task Wizard</b> to manage Exchange recipients.</li> <li>• List all Exchange users, groups and contacts.</li> <li>• View all Exchange properties of users, groups and contacts.</li> </ul>
<b>Exchange - Recipients Full Control</b>	Grants the following permissions: <ul style="list-style-type: none"> <li>• Perform all Exchange recipient management tasks.</li> <li>• View or modify all properties of Exchange recipients.</li> <li>• List all Exchange users, groups and contacts.</li> <li>• View all Exchange properties of users, groups and contacts.</li> </ul>

# Exchange – Advanced ATs

To delegate more granular Microsoft Exchange resource management permissions in your environment, use the Access Templates (ATs) in the **Configuration > Access Templates > Exchange > Advanced** container of the Active Roles Console.

These ATs contain more granular Exchange resource management tasks for various mailbox resources.

**Table 18: Exchange – Advanced Access Templates**

<b>Access Template</b>	<b>Description</b>
<b>Exchange - Convert Linked Mailbox to User Mailbox</b>	Grants permission to convert linked mailboxes to user mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Convert User Mailbox to Linked Mailbox</b>	Grants permission to convert user mailboxes to linked mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Create Equipment Mailboxes</b>	Grants permission to create equipment mailboxes for new or existing equipment resources.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Create Linked Mailboxes</b>	Grants permission to create linked mailboxes for new or existing user accounts.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Create Room Mailboxes</b>	Grants permission to create room mailboxes for new or existing room resources.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Create Shared Mailboxes</b>	Grants permission to create shared mailboxes for new or existing user accounts.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Create User Mailboxes</b>	Grants permission to create user mailboxes for new or existing user accounts.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Delete Recipient's E-</b>	Grants permission to delete email addresses.   <b>NOTE:</b> This AT provides no additional permissions.

Access Template	Description
<b>mail Address</b>	
<b>Exchange - Delete User Mailbox</b>	Grants permission to delete user mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Designate Contact as Mail-Enabled</b>	Grants permission to designate contacts as mail-enabled recipients.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Designate Group as Mail-Enabled</b>	Grants permission to designate groups as mail-enabled recipients.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Designate User as Mail-Enabled</b>	Grants permission to designate users as mail-enabled recipients.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Enable Archive</b>	Grants permission to enable archives for Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Enable Unified Messaging</b>	Grants permission to enable Unified Messaging for Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Move Mailbox</b>	Grants permission to move Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read ERFM Attributes</b>	Grants permission to read the Exchange Resource Forest Management-specific (ERFM-specific) attributes of master accounts.   <b>TIP:</b> Assign this AT to the administrators delegated to manage the ERFM solution and its associated resources.   <b>NOTE:</b> Consider the following when planning to delegate permissions for reading ERFM-specific attributes: <ul style="list-style-type: none"> <li>• This AT will work properly only if Exchange Resource Forest Management (ERFM) is configured in your organization. For more information, see <i>Configuring linked mailboxes with Exchange Resource Forest Management</i> in the <i>Active Roles Administration Guide</i>.</li> <li>• You do not have to apply this AT if your organization already uses any general-purpose ATs for delegating Exchange</li> </ul>

Access Template	Description
	recipient management tasks. This is because those ATs already provide the required permissions for reading the ERFM-related attributes of master accounts too.
<b>Exchange - Read/Write Address Book Policy</b>	Grants permission to change the address book policy settings on the <b>Mailbox Settings</b> page of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Advanced Properties for Mailbox-Enabled Users</b>	Grants permission to view or modify the <b>Advanced</b> Exchange properties for mailbox-enabled users.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Advanced Properties for Mail-Enabled Groups</b>	Grants permission to view or modify the <b>Advanced</b> Exchange properties for mail-enabled groups.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Advanced Properties for Mail-Enabled Users and Contacts</b>	Grants permission to view or modify the <b>Advanced</b> Exchange properties for mail-enabled contacts and users.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Archive</b>	Grants permission to view or modify the <b>Mailbox Features &gt; Archive</b> settings of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Archive Quota</b>	Grants permission to view or modify the archive quota settings on the <b>Mailbox Features</b> page of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Autoreply Settings</b>	Grants permission to view or modify the automatic reply settings of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Custom</b>	Grants permission to view or change custom Exchange attributes.   <b>NOTE:</b> This AT provides no additional permissions.

Access Template	Description
<b>Attributes</b>	
<b>Exchange - Read/Write Deleted Item Retention Period</b>	Grants permission to view or modify the retention period of deleted items in Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Delivery Options</b>	Grants permission to change the delivery options of <b>Mail Flow Settings</b> for Exchange recipients.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Exchange ActiveSync</b>	Grants permission to view or modify the <b>Mailbox Features &gt; Exchange ActiveSync</b> settings of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange-Read/Write Forwarding Address</b>	Grants permission to view or modify the <b>Forwarding Address</b> setting of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write ILS Settings</b>	Grants permission to view or modify the <b>ILS Settings</b> of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write IMAP4</b>	Grants permission to view or modify the <b>Mailbox Features &gt; IMAP4</b> settings of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Mailbox Rights</b>	Grants permission to view or modify the security settings of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Mailbox Storage Limits</b>	Grants permission to view or modify the storage limit of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write MAPI</b>	Grants permission to view or modify the <b>Mailbox Features &gt; MAPI</b> settings of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write</b>	Grants permission to view or modify the <b>Maximum Size of Incoming Messages</b> setting of Exchange mailboxes.

Access Template	Description
<b>Maximum Size of Incoming Messages</b>	<b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Maximum Size of Outgoing Messages</b>	Grants permission to view or modify the <b>Maximum Size of Outgoing Messages</b> setting of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Message Delivery Restrictions</b>	Grants permission to view or modify the message delivery restrictions of the <b>Mail Flow Settings</b> for Exchange recipients.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Message Moderation</b>	Grants permission to view or modify the message moderation options of the <b>Mail Flow Settings</b> for Exchange recipients.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Message Restrictions</b>	Grants permission to view or modify the <b>Message Restrictions</b> for Exchange recipients.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Message Size Restrictions</b>	Grants permission to view or modify the <b>Message Size Restrictions</b> for Exchange recipients.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Messaging Records Management</b>	Grants permission to view or modify the <b>Mailbox Settings &gt; Messaging Records Management</b> (MRM) settings for Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Outlook Mobile Access</b>	Grants permission to view or modify the <b>Mailbox Features &gt; Outlook Mobile Access</b> settings for Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Outlook Web App</b>	Grants permission to view or modify the <b>Mailbox Features &gt; Outlook Web App</b> settings for Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange -</b>	Grants permission to view or modify the <b>Mailbox Features &gt; POP3</b>

Access Template	Description
<b>Read/Write POP3</b>	settings for Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Protocol Settings</b>	Grants permission to view or modify the protocol settings for Exchange recipients.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Recipient Limits</b>	Grants permission to view or modify the recipient limit settings for Exchange recipients.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Role Assignment Policy</b>	Grants permission to view or modify the <b>Mailbox Settings &gt; Role Assignment Policy</b> settings for Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Send on Behalf Permission</b>	Grants permission to view or modify the <b>Send on Behalf</b> permissions of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Sharing</b>	Grants permission to view or modify the <b>Mailbox Settings &gt; Sharing</b> settings of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Storage Quotas</b>	Grants permission to view or modify the <b>Mailbox Settings &gt; Storage Quotas</b> settings of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Unified Messaging</b>	Grants permission to enable or disable Unified Messaging for Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.
<b>Exchange - Read/Write Up-to-date Notifications</b>	Grants permission to view or modify the <b>Mailbox Features &gt; Up-to-date Notifications</b> settings of Exchange mailboxes.   <b>NOTE:</b> This AT provides no additional permissions.

# Skype for Business Server

The **Configuration > Access Templates > Skype for Business Server** container of the Active Roles Console contains Access Templates (ATs) that you can use to delegate Microsoft Skype for Business user and contact management duties.

**NOTE:** The ATs of this container will work only if the Active Roles Skype for Business Server Solution is already configured in your organization. For more information, see *Skype for Business Server Solution* in the *Active Roles Solutions Guide*.

## Skype for Business Server – General ATs

If the Skype for Business Server Solution is configured in your organization, you can delegate Microsoft Skype for Business user and contact management duties with the ATs of the **Configuration > Access Templates > Skype for Business Server** container of the Active Roles Console.

**Table 19: Skype for Business Server – General Access Templates**

Access Template	Description
<b>Skype for Business Server - User Disable/Re-enable</b>	Grants the following permissions: <ul style="list-style-type: none"><li>• Temporarily disable or re-enable the users of the Skype for Business server.</li><li>• View Skype for Business server users.</li><li>• View the Session Initiation Protocol (SIP) address.</li><li>• View telephony-related settings.</li><li>• View the user policy assignments of the Skype for Business server.</li></ul>
<b>Skype for Business Server - User Full Control</b>	Grants full permission to: <ul style="list-style-type: none"><li>• Add, enable or remove Skype for Business users.</li><li>• View Skype for Business server users.</li><li>• View or modify the SIP address.</li><li>• View or modify telephony-related settings.</li><li>• View or modify the user policy assignments of the Skype for Business server.</li></ul>

Access Template	Description
<b>Skype for Business Server - User Policies</b>	<ul style="list-style-type: none"> <li>• Temporarily disable or re-enable the users of the Skype for Business server.</li> <li>• Move users to another Skype for Business server or pool.</li> </ul> <p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• View Skype for Business server users.</li> <li>• View the SIP address.</li> <li>• View telephony-related settings.</li> <li>• View or modify the user policy assignments of the Skype for Business server.</li> </ul>
<b>Skype for Business Server - User Telephony</b>	<p>Grants the following permissions:</p> <ul style="list-style-type: none"> <li>• View Skype for Business server users.</li> <li>• View the SIP address.</li> <li>• View or modify telephony-related settings.</li> <li>• View the user policy assignments of the Skype for Business server.</li> </ul>

The **Configuration > Access Templates > Starling** container of the Active Roles Console contains Access Templates (ATs) to delegate One Identity Starling operational duties.

## Starling – General ATs

To delegate common One Identity Starling operational permissions in your organization, use the Access Templates (ATs) in the root of the **Configuration > Access Templates > Starling** container of the Active Roles Console.

**Table 20: Starling – General Access Templates**

Access Template	Description
<b>Starling -Two Factor Authentication User</b>	Grants the minimal read permission required to enable Starling Two-Factor Authentication (Starling 2FA) for a user. <b>NOTE:</b> Starting from Active Roles 7.6, Starling 2FA is no longer supported. Therefore, this AT is deprecated and no longer functional.

# User Interfaces

The **Configuration > Access Templates > User Interfaces** container contains Access Templates (ATs) to delegate access permissions to the Active Roles Console (also called the Active Roles MMC Interface).

## User Interfaces – General ATs

To delegate Active Roles Console access permissions to administrators in your organization, use the Access Templates (ATs) in the root of the **Configuration > Access Templates > User Interfaces** container of the Active Roles Console.

**Table 21: User Interfaces– General Access Templates**

<b>Access Template</b>	<b>Description</b>
<b>User Interface Management-MMC Full control</b>	Grants permission to login to the Active Roles Console.

# User Self-management

The **Configuration > Access Templates > User Self-management** container contains Access Templates (ATs) to delegate self-management tasks to users (for example, allowing users to view or modify specific properties of their accounts on the Active Roles Web Interface).

## User Self-management – General ATs

To delegate self-management permissions for users in your organization, use the Access Templates (ATs) in the root of the **Configuration > Access Templates > User Self-management** container of the Active Roles Console.

**Table 22: User Self-management – General Access Templates**

Access Template	Description
<b>Self - Account Management</b>	<p>Grants permission to users to view or modify their profile information on the Active Roles Web Interface.</p> <p><b>TIP:</b> When configuring this AT, specify the <b>Self</b> built-in account as the trustee.</p> <p>For more information on applying ATs on resources, see <i>Applying Access Templates on a securable object</i> in the <i>Active Roles Administration Guide</i>.</p>
<b>Self - Group Management</b>	<p>Grants permission to users to view or modify the groups they manage.</p> <p><b>TIP:</b> When configuring this AT, specify one of these built-in accounts as the trustee:</p> <ul style="list-style-type: none"><li>• <b>Primary Owner (Managed By)</b></li><li>• <b>Secondary Owners</b></li></ul> <p>For more information on applying ATs on resources, see <i>Applying Access Templates on a securable object</i> in the <i>Active Roles Administration Guide</i>.</p> <p><b>NOTE:</b> Applying only this AT to group owners does not grant them permission to view the list of group members. To do so, group owners must also have read access to the group member objects as well.</p> <p>To grant that permission, apply the <b>Active Directory &gt; All Objects - Read All Properties</b> AT to a scope containing the group member objects, then set the <b>Authenticated Users</b> built-in account as the</p>

Access Template	Description
<b>Self - Group Membership Approval Setting</b>	<p>trustee.</p> <p>Grants permission to users to modify group membership approval settings, that is, whether group membership changes, such as joining or leaving a group, requires approval from the group owner.</p>
<b>Self - Group Membership Management</b>	<p>Grants permission to users to add or remove their own user account to or from groups.</p> <p><b>TIP:</b> When configuring this AT, consider the following recommendations:</p> <ul style="list-style-type: none"> <li>• Apply this AT to a scope containing the groups, with the appropriate user accounts set as trustees. One Identity recommends adding the affected user accounts to a specific group, then selecting that group as the trustee for the AT.</li> <li>• To allow users to view the groups they are members of, assign them the <b>Self - Account Management</b> AT as well. Apply this AT to a scope containing the user accounts for which you want to grant the permission, and specify the built-in <b>Self</b> account as the trustee.</li> </ul> <p>For more information on applying ATs on resources, see <i>Applying Access Templates on a securable object</i> in the <i>Active Roles Administration Guide</i>.</p>

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](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product