Active Roles 8.0 LTS

Built-in Access Templates Reference Guide

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.

ARSBuilt-in Access Templates Reference Guide
Updated - 06 October 2022, 15:42

For the most recent documents and product information, see the Active Roles online documentation.

Contents

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.

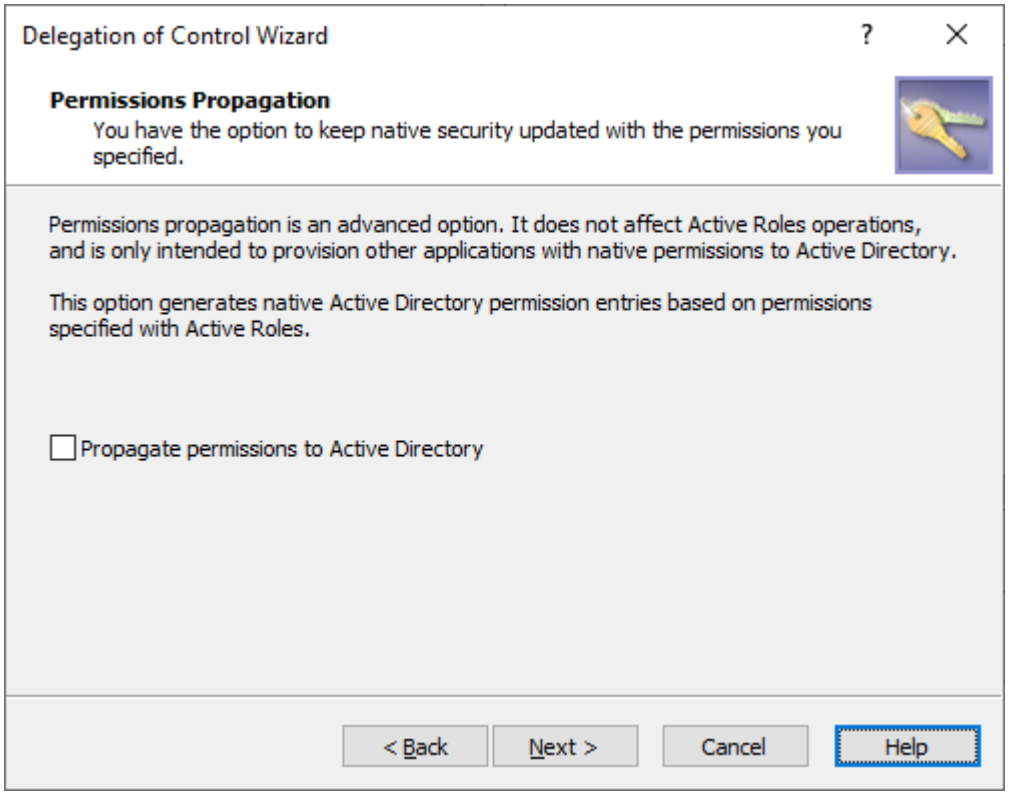
This container has two sub-containers:

- **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
All Objects - Full Control	Grants full permission to perform any administrative operation on any object in AD.

Access Template	Description
	TIP: 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.
All Objects - Read All Properties	Grants the following permissions: • List directory objects. • View all properties of any object in AD.
All Objects - View or Restore Deleted Objects	Grants the permission to view or restore AD objects deleted from a container. TIP: Apply this AT to the container whose deleted objects the data administrators should be able to view or restore. 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*.
Claim Types - Full Control	Grants full permission to: • Create new claim types. • Perform all administrative operations on existing claim types. 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.
Claim Types - Modify All Properties	Grants permission to view or change all claim type properties.
Claim Types - Read All Properties	Grants permission to list claim types and view all claim type properties.
Computers - Create Computer Accounts	Grants the following permissions: • Create new computer accounts. • View all properties of computer accounts.
Computers - Full Control	Grants full permission to: • Create new computer accounts. • Perform all administrative tasks on existing computer accounts.
Computers - Modify All Properties	Grants permission to view or change all properties of computer accounts.

Access Template	Description
Computers - Move Computer Accounts	Grants the following permissions: • Move computer accounts. • View all properties of computer accounts.
Computers - Read All Properties	Grants the following permissions: • List computer accounts. • View all properties of computer accounts.
Computer - Reset Computer Accounts	Grants the following permissions: • Reset computer accounts. • View all properties of computer accounts.
Contacts - Create Contacts	Grants the following permissions: • Create new contacts. • View all contact properties.
Contacts - Full Control	Grants full permission to: • Create new contacts. • Perform all administrative operations on existing contacts.
Contacts - Modify All Properties	Grants permission to view or modify all contact properties.
Contacts - Modify Picture	Grants the following permissions: • View or change the image, that is, the `thumbnailPhoto` attribute. • View all contact properties.
Contacts - Read All Properties	Grants the following permissions: • List contacts. • View all contact properties.
Domains - Read All Properties	Grants the following permissions: • List domain objects. • View all properties of domain objects.
gMSA - Full Control	Grants full permission to: • Create new group Managed Service Accounts (gMSAs). • Perform all administrative operations on existing gMSAs.

Access Template	Description
gMSA - Modify All Properties	Grants permission to view or change all gMSA properties.
gMSA - Modify Membership Policy	Grants permission to view or change the list of computers and computer groups allowed to use a specific gMSA.
gMSA - Read All Properties	Grants the following permissions: • List gMSAs. • View all gMSA properties.
Groups - Add/Remove Members	Grants permission to view or modify the members of groups.
Groups - Create Groups	Grants the following permissions: • Create new groups. • View all group properties.
Groups - Full Control	Grants full permission to: • Create new groups. • Perform all administrative operations on existing groups.
Groups - Manage Dynamic Groups	Grants the following permissions: • Configure rule-based membership rules for dynamic groups. • View all group properties. • List groups in AD containers. • List AD containers.
Groups - Modify All Properties	Grants permission to view or modify all group properties.
Groups - Modify Picture	Grants the following permissions: • View or change the image, that is, the `thumbnailPhoto` attribute. • View all group properties.
Groups - Perform Deprovision Tasks	Grants the following permissions: • Deprovision groups. • View all group properties. TIP: Use this AT to delegate group deprovisioning permissions to

Access Template	Description
	data administrators without also delegating group create and group delete permissions.
Groups - Perform Undo Deprovision Tasks	Grants the following permissions: • Restore groups. • View all group properties. TIP: Use this AT to delegate the permission of performing the **Undo Deprovisioning** command on groups only.
Groups - Read all Properties	Grants the following permissions: • List groups. • View all group properties.
OUs - Create OUs	Grants the following permissions: • Create new Organizational Units (OUs). • View all OU properties.
OUs - Full Control	Grants full permission to: • Create new OUs. • Perform all administrative operations on OUs.
OUs - Modify All Properties	Grants permission to view or modify all OU properties.
OUs - Read All Properties	Grants the following permissions: • List OUs. • View all OU properties.
Printers - Full Control	Grants full permission to: • Create new printer queue objects. • Perform all administrative operations on existing printer queues.
Printers - Modify All Properties	Grants permission to view or modify all printer queue properties.
Printers - Read All Properties	Grants the following permissions: • List printer queue objects. • View all printer queue properties.
Shared	Grants full permission to:

Access Template	Description
Folders - Full Control	• Create new shared folder objects. • Perform all administrative operations on existing shared folders.
Shared Folders - Modify All Attributes	Grants permissions to view or modify all shared folder properties.
Shared Folders - Read All Properties	Grants the following permissions: • List shared folders. • View all shared folder properties.
Users - Create User Accounts	Grants the following permissions: • Create new user accounts. • View all user account properties.
Users - Delete User Accounts	Grants the following permissions: • Delete user accounts. • View all user account properties.
Users - Full Control	Grants full permission to: • Create new user accounts. • Perform all administrative operations on existing user accounts.
Users - Help Desk	Grants the following permissions: • Reset user passwords. • Unlock user accounts. • Assign or remove digital (X.509) certificates from user accounts. • View all user account properties. TIP: One Identity recommends using this AT to delegate permissions required for the day-to-day operations of your helpdesk service.
Users - Modify All Properties	Grants permission to view or modify all user account properties.
Users - Modify Personal Data	Grants permission to manage the basic HR-related properties of user accounts.
Users - Modify	Grants the following permissions:

Access Template	Description
Picture	• View or change the image, that is, the `thumbnailPhoto` attribute. • View all user account properties.
Users - Move User Accounts	Grants the following permissions: • Move user accounts. • View all user account properties.
Users - Pager & Cell Phone Numbers	Grants the following permissions: • View and modify the mobile phone and pager number information of the user accounts. • View all user account properties.
Users - Perform Deprovision Tasks	Grants the following permissions: • Deprovision user accounts and other user-related resources. • View all user account properties. TIP: Use this AT to delegate user deprovisioning permissions to data administrators without also delegating user create and user delete permissions.
Users - Perform Undo Deprovision Tasks	Grants the following permissions: • Restore user accounts. • View all user account properties. TIP: Use this AT to delegate the permission of performing the **Undo Deprovisioning** command on user accounts only.
Users - Phone Number & Address	Grants the following permissions: • Modify the address and telephone number properties of user accounts. • View all user account properties.
Users - Read All Properties	Grants the following permissions: • List user accounts. • View all user account properties.
Users and Groups - Basic Management	Grants the following permissions: • List groups and user accounts. • Add or remove users and groups to or from groups. • Reset user passwords. • View or modify the login-related properties of user accounts.

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
Computer Objects – Create	Grants permission to create computer objects. NOTE: This AT provides no additional permissions.
Computer Objects – Delete	Grants permission to delete computer objects. NOTE: This AT provides no additional permissions.
Computer Objects – List	Grants permission to list computer objects. NOTE: This AT provides no additional permissions.
Computer Objects – Read/Write Account Restrictions	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 User-Account-Restrictions property set in the *Microsoft Active Directory Schema documentation*.
Computer Objects – Read/Write General Information	Grants permission to view or modify the following general information properties of computer objects: • Computer name (pre-Windows 2000) • DNS name • Role • Description • Flags controlling password, lockout, and computer disable/enable behavior (that is, the **User Account Control** attribute)
Computer Objects – Read/Write Manager	Grants permission to view or modify the person assigned to the management of the computer resource (that is, the **Managed By** attribute of the computer). NOTE: This AT provides no additional permissions.

Access Template	Description
Computer Objects – Read/Write Personal Information	Grants permission to view or modify the personal information properties of computer objects (that is, the `Personal-Information` property set of computer objects). For more information on the affected properties, see Personal-Information property set in the *Microsoft Active Directory Schema documentation*.
Computer Objects – Read/Write Public Information	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 Public-Information property set in the *Microsoft Active Directory Schema documentation*.
Computer Objects - Reset Computer Accounts	Grants permission to reset computer accounts. NOTE: This AT provides no additional permissions.
Computer Objects - View BitLocker Recovery Keys	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). TIP: Use this AT to delegate the task of retrieving BitLocker recovery keys stored in AD.
Contacts – Create	Grants permission to create contact objects. NOTE: This AT provides no additional permissions.
Contacts – Delete	Grants permission to delete contact objects. NOTE: This AT provides no additional permissions.
Contacts – Read Group Membership	Grants permission to view the list of groups to which the contact object belongs. NOTE: This AT provides no additional permissions.
Contacts – Read/Write Organizational Information	Grants permission to view or modify the following organizational properties of the contact: • Job title • Department • Company • Employee ID • Manager

Access Template	Description
	• Office location
Contacts – Read/Write Personal Information	Grants permission to view or modify the personal information properties of contacts (that is, the `Personal-Information` property set of contacts). For more information on the affected properties, see Personal-Information property set in the *Microsoft Active Directory Schema documentation*.
Contacts – Read/Write Web Information	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 Web-Information property set in the *Microsoft Active Directory Schema documentation*.
Contacts – Rename	Grants permission to rename contact objects. NOTE: This AT provides no additional permissions.
Domains – Change PDC	Grants permission to change the role owner of the Primary Domain Controller (PDC) Emulator. NOTE: This AT provides no additional permissions.
Domains – Delegate Control and Enforce Active Roles Server Policy	Grants permission to apply Active Roles ATs and Policy Objects to domain objects. NOTE: This AT provides no additional permissions.
Domains – Generate Resultant Set of Policy (Logging)	Grants permission to generate Group Policy Result data for the users and/or computers in a specific domain.
Domains – Generate Resultant Set of Policy (Planning)	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.
Domains – List	Grants permission to list domain objects. NOTE: This AT provides no additional permissions.
Domains –	Grants permission to view or modify the following general

Access Template	Description
Read/Write General Information	information properties of domain objects: • Domain name (pre-Windows 2000) • Description
Domains – Read/Write Manager	Grants permission to view or modify the person assigned to the management of a domain (that is, the **Managed By** attribute of the domain). NOTE: This AT provides no additional permissions.
Domains – Read/Write Other Domain Parameters	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). For more information on the affected properties, see Domain-Other-Parameters property set in the *Microsoft Active Directory Schema documentation*.
Domains – Read/Write Password & Lockout Policies	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). For more information on the affected properties, see Domain-Password property set in the *Microsoft Active Directory Schema documentation*.
Group Policy Container – Apply Group Policy	Grants the extended right used by the Group Policy engine (that is, the *Apply-Group-Policy* extended right) to determine if a Group Policy Object (GPO) applies to a user and/or computer.
Groups – Add/Remove Self As Member	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).
Groups – Copy	Grants permission to copy groups. NOTE: This AT provides no additional permissions.
Groups – Create	Grants permission to create groups. NOTE: This AT provides no additional permissions.
Groups – Delete	Grants permission to delete groups. NOTE: This AT provides no additional permissions.
Groups - Deprovision	Grants permission to deprovision groups. NOTE: This AT provides no additional permissions.
Groups – List	Grants permission to list groups.

Access Template	Description
	NOTE: This AT provides no additional permissions.
Groups – Manage Membership Rules	Grants permission to view or modify the criteria of rule-based group membership assignments within Active Roles. NOTE: This AT provides no additional permissions.
Groups – Read Group Membership	Grants permission to view the list of groups to which a specific group belongs. NOTE: This AT provides no additional permissions.
Groups – Read/Write E-mail Address	Grants permission to view or modify the list of email addresses for a group.
Groups – Read/Write General Information	Grants permission to view or modify the following general information properties of groups: • Group name (pre-Windows 2000) • Description • E-mail • Group scope • Group type • Notes
Groups – Read/Write Group Members	Grants permission to add or remove members to or from a group.
Groups – Read/Write Group Type and Scope	Grants permission to view or modify the type and scope settings of a group. NOTE: This AT provides no additional permissions.
Groups – Read/Write Manager	Grants permission to view or modify the person assigned to manage a specific group (that is, the **Managed By** attribute of the group).
Groups – Read/Write Phone and Mail Options	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 Email-Information property set in the *Microsoft Active Directory Schema documentation*.

Access Template	Description
Groups – Rename	Grants permission to rename groups. NOTE: This AT provides no additional permissions.
Groups - Undo Deprovision	Grants permission to restore (that is, perform the **Undo Deprovision** action) on groups. NOTE: This AT provides no additional permissions.
Groups - Undo Deprovision - Deny	Grants permission to deny the restoration of group objects (that is, performing the **Undo Deprovision** action on them).
Objects - Deny Deletion	Grants permission to deny the deletion and sub-tree deletion of a specific object. NOTE: This AT provides no additional permissions.
Objects - Deny Deletion of Child Objects	Grants permission to deny deleting all child objects from a specific AD container. NOTE: This AT provides no additional permissions.
OUs – Create	Grants permission to create Organizational Units (OUs). NOTE: This AT provides no additional permissions.
OUs – Delegate Control and Enforce Active Roles Server Policy	Grants permission to apply Active Roles ATs and Policy Objects to an OU. NOTE: This AT provides no additional permissions.
OUs – Delete	Grants permission to delete OUs. NOTE: This AT provides no additional permissions.
OUs – Generate Resultant Set of Policy (Logging)	Grants permission to generate Group Policy Results data for the users and computers within the specific OU.
OUs – Generate Resultant Set of Policy (Planning)	Grants permission to generate Group Policy Modeling data for the users and computers within the specific OU.
OUs – List	Grants permission to list OUs. NOTE: This AT provides no additional permissions.
OUs – Read/Write	Grants permission to view or modify the following general information properties of OUs:

Access Template	Description
General Information	• Description • Street • City • State/province • Zip/Postal Code • Country/region
OUs – Read/Write Manager	Grants permission to view or modify the person assigned to manage a specific OU (that is, the **Managed By** attribute of the OU).
OUs – Rename	Grants permission to rename OUs. NOTE: This AT provides no additional permissions.
Printer Objects – Create	Grants permission to create printer queue objects. NOTE: This AT provides no additional permissions.
Printer Objects – Delete	Grants permission to delete printer queue objects. NOTE: This AT provides no additional permissions.
Printer Objects – List	Grants permission to list printer queue objects. NOTE: This AT provides no additional permissions.
Printer Objects – Read/Write General Information	Grants permission to view or modify the following general information properties of printer queue objects: • Location • Model • Description • Color • Staple • Double-sided • Printing speed • Maximum resolution
Printer Objects – Read/Write Manager	Grants permission to view or modify the person assigned to manage a specific printer (that is, the **Managed By** attribute of the printer).
Printer Objects – Rename	Grants permission to rename printer queue objects. NOTE: This AT provides no additional permissions.

Access Template	Description
Shared Folders – Create	Grants permission to create shared folder objects. NOTE: This AT provides no additional permissions.
Shared Folders – Delete	Grants permission to delete shared folder objects. NOTE: This AT provides no additional permissions.
Shared Folders – List	Grants permission to list shared folder objects. NOTE: This AT provides no additional permissions.
Shared Folders – Read/Write General Information	Grants permission to view or modify the following general information properties of shared folders: • Description • UNC name
Shared Folders – Read/Write Manager	Grants permission to view or modify the person assigned to manage a specific shared folder (that is, the **Managed By** attribute of the shared folder).
Shared Folders – Rename	Grants permission to rename shared folder objects. NOTE: This AT provides no additional permissions.
Users - Assign/Remove Digital Certificates	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).
Users - Change Password (Extended Right)	Grants permission to change the password of users (that is, grants the `User-Change-Password` extended right).
Users - Copy	Grants the permission to copy user objects. NOTE: This AT provides no additional permissions.
Users - Create	Grants permission to create user objects. NOTE: This AT provides no additional permissions.
Users - Delete	Grants permission to delete user objects. NOTE: This AT provides no additional permissions.
Users - Deprovision	Grants permission to deprovision user objects. NOTE: This AT provides no additional permissions.
Users - Enable/Disable	Grants permission to enable or disable user objects. NOTE: This AT provides no additional permissions.

Access Template	Description
Account	
Users - List	Grants permission to list user objects. NOTE: This AT provides no additional permissions.
Users - Read Group Membership	Grants permission to view the list of groups the selected user is a member of. NOTE: This AT provides no additional permissions.
Users - Read/Write Account Information	Grants permission to view or modify the following account information properties of user objects: • User logon name • User logon name (pre-Windows 2000) • Logon Hours • Last Logon • Account is locked out • Account options • Account expires
Users - Read/Write Account Restrictions	Grants permission to view or modify the account restriction properties of user objects (that is, the `User-Account-Restrictions` property set of user objects). For more information on the affected properties, see User-Account-Restrictions property set in the *Microsoft Active Directory Schema documentation*.
Users - Read/Write Dial-In Properties	Grants permission to view or modify the following dial-in specific properties of user objects: • Remote Access Permission (Dial-in or VPN) • Verify Caller-ID • Callback Options • Assign a Static IP Address • Apply Static Routes Settings
Users - Read/Write General Information	Grants permission to view or modify the general information properties of user objects (that is, the `General-Information` property set of user objects). For more information on the affected properties, see General-Information property set in the *Microsoft Active Directory Schema documentation*.

Access Template	Description
Users - Read/Write Logon Information	Grants permission to view or modify the logon information properties of user objects (that is, the `User-Logon` property set of user objects). For more information on the affected properties, see User-Logon property set in the *Microsoft Active Directory Schema documentation*.
Users - Read/Write Organizational Information	Grants permission to view or modify the following organization-related properties of user objects: • Title • Department • Company • Manager • Direct reports • Office (General tab)
Users - Read/Write Personal Information	Grants permission to view or modify the personal information properties of user objects (that is, the `Personal-Information` property set of user objects). For more information on the affected properties, see Personal-Information property set in the *Microsoft Active Directory Schema documentation*.
Users - Read/Write Phone and Mail Options	Grants permission to view or modify the email-related information properties of user objects (that is, the `Email-Information` property set of user objects). For more information on the affected properties, see Email-Information property set in the *Microsoft Active Directory Schema documentation*.
Users - Read/Write Profile Properties	Grants permission to view or modify the following profile-related properties of user objects: • User profile • Home folder
Users - Read/Write Public Information	Grants permission to view or modify the public information properties of user objects (that is, the `Public-Information` property set of user objects). For more information on the affected properties, see Public-Information property set in the *Microsoft Active Directory Schema documentation*.
Users - Read/Write	Grants permission to view or modify the web-related information properties of user objects (that is, the `Web-Information` property set of

Access Template	Description
Web Information	user objects). For more information on the affected properties, see Web-Information property set in the *Microsoft Active Directory Schema documentation*.
Users - Read/Write WTS Properties	Grants permission to view or modify the following user object properties describing Terminal Services-related information: • Terminal Services user profile • Terminal Services home folder • Allow login to the terminal server • Starting program • Client devices • Terminal Service timeout and reconnection settings
Users - Rename	Grants permission to rename user objects. NOTE: This AT provides no additional permissions.
Users - Reset Password (Extended Right)	Grants permission to reset the password of user objects (that is, grants the `User-Reset-Password` extended right). NOTE: This AT provides no additional permissions.
Users - Run Check Policy (Extended Right)	Grants permission to use the **Check Policy** action on user objects. NOTE: This AT provides no additional permissions.
Users - Undo Deprovision	Grants permission to restore user objects (that is, performing the **Undo Deprovision** action on them).
Users - Undo Deprovision - Deny	Grants permission to deny the restoration of user objects (that is, performing the **Undo Deprovision** action on them).
Users - Unlock Account	Grants permission to unlock user objects that get locked due to reaching the limit of failed login attempts set in your organization.
Users - View Change History (Extended Right)	Grants permission to use the **Change History** and **User Activity** actions on user objects.
Users - View Delegated Rights	Grants permission to use the **Delegated Rights** action on user objects.

Access Template	Description
(Extended Right)	
Users - View Digital Certificates	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).
Users - View Entitlement Profile (Extended Right)	Grants permission to use the **Entitlement Profile** action on user objects to view the resources to which the selected user object is entitled.
Users - Write Password	Grants permission to set the password of user objects. NOTE: 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.

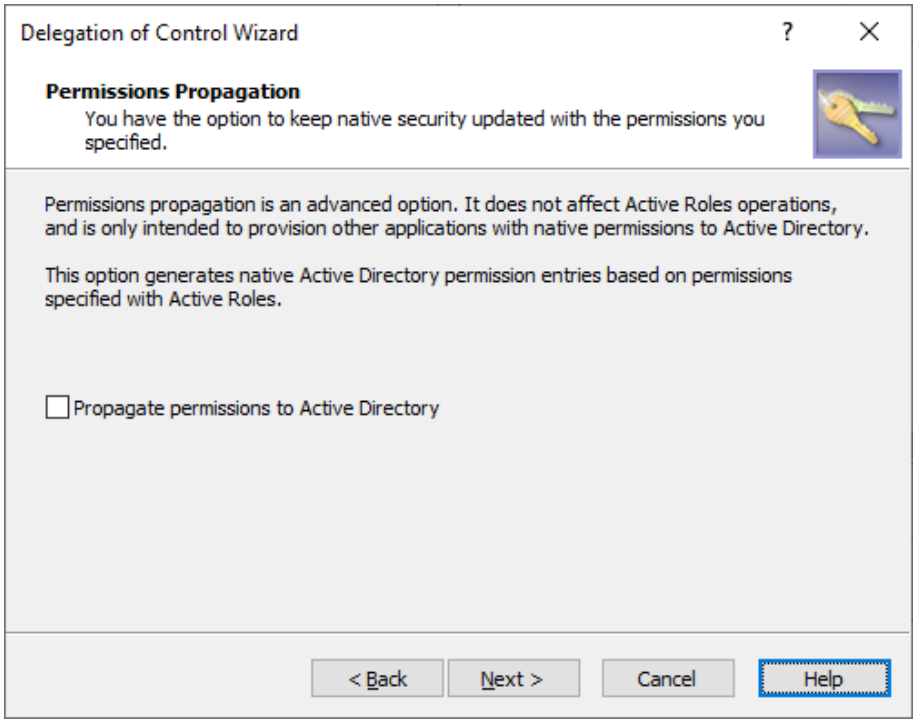
The ATs that are available in this container are grouped into additional sub-containers, in accordance with the operator, administrator or manager roles that they are recommended to be used with.

- 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
DNS Admins - Microsoft DNS Management	Grants permission to perform management tasks on the Microsoft DNS servers within your organization. To delegate this AT, apply it on the following resources of your Active Directory tree in the Active Roles Console: 1. **<forest-root-domain>** > **ForestDnsZones** > **MicrosoftDNS** 2. **<domain>** > **System** > **MicrosoftDNS** 3. **<domain>** > **DomainDnsZones** > **MicrosoftDNS** IMPORTANT: When configuring this AT, always select the **Propagate permissions to Active Directory** option in the **Permissions Propagation** step of the **Delegation of Control Wizard**. **Figure 2: 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 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

Access Template	Description
Domain Configuration Operators - Domain Controllers OU Management	Grants full permission to domain configuration, applied to all classes. To delegate this AT, select the trustee(s), then apply it to the **Domain Controllers** container of your AD environment: **<domain>** > **Domain Controllers**
Domain Configuration Operators - Domain Management	Grants the following permissions, applied to all classes: • Add or remove replicas in the domain. • Modify the infrastructure master. • Modify the PDC. • Write the `fSMORoleOwner` attribute. • Write the `msDS-Behavior-Version` attribute.

Access Template	Description
	To delegate this AT, select the trustee(s), then apply it on the root domain of your AD environment.
Domain Configuration Operators - Full Control for "Creator Owner"	Grants full permission in a Creator Owner role, applied to all classes. 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: **<forest-root-domain>** > **Configuration** > **Sites**
Domain Configuration Operators - Full Control on Computer Object	Grants full permission to perform domain configuration tasks on all computer objects. To delegate this AT, select the trustee(s), then apply the AT on the computer object that will be promoted to Domain Controller (DC).
Domain Configuration Operators - Infrastructure Master Management	Grants the following permissions, applied to all classes: • Write the `fSMORoleOwner` attribute. • Modify the infrastructure master. To delegate this AT, select the trustee(s), then apply the AT to the AD infrastructure container: **<domain>** > **Infrastructure**
Domain Configuration Operators - Replication Management	Grants the following domain-level configuration permissions: • Manage the replication topology, applied to all classes. • Replicate directory changes, applied to all classes • Monitor AD replication, applied to the Directory Management Domain (DMD). • Replicate all directory changes, applied to the DMD. To delegate this AT, select the trustee(s), then apply the AT to the following AD containers: • **<domain>** • **<forest-root-domain>** > **Configuration** NOTE: You must apply the permissions that are specified by this AT to the AD configuration schemas too. These are located in the following container: **<forest-root-domain>** > **Configuration** > **Schema** To apply the permissions to the **Schema** container, use native AD management tools, such as ADSI Edit.

Access Template	Description
Domain Configuration Operators - RID Master Management	Grants the following permissions, applied to all classes: • Modify the RID master. • Write the `fSMORoleOwner` attribute. To delegate this AT, select the trustee(s), then apply the AT to the AD RID manager container: **<domain>** > **System** > **RID Managers**
Domain Configuration Operators - Server Object Creation	Grants permission to create all server child objects in the domain, applied to all classes. To delegate this AT, select the trustee(s), then apply the AT to the AD server configuration container: **<forest-root-domain>** > **Configuration** > **Sites** > **<site>** > **Servers**
Domain Configuration Operators - Site Objects - Read All Properties	Grants permission to read all site objects in the domain, applied to all classes. To delegate this AT, select the trustee(s), then apply the AT to the AD site configuration container: **<forest-root-domain>** > **Configuration** > **Sites**
Domain Configuration Operators - System Container Management	Grants full permission to manage the AD **System** 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: **<domain>** > **System**

Active Directory – Forest Configuration Operators Role ATs

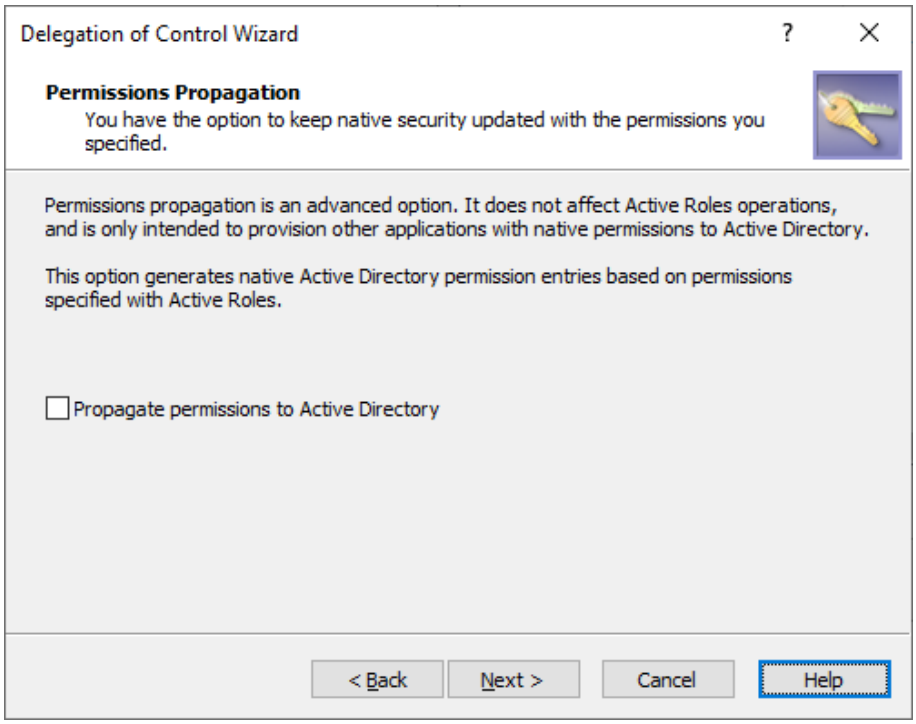
To delegate forest configuration duties to operators within your organization, use the Access Templates (ATs) available under the **Configuration** > **Access Templates** > **Active Directory** > **Best Practices for Delegating Active Directory Administration** > **Forest Configuration Operators Role** 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
Forest Configuration Operators - Change Domain Master Management	Grants the following permissions, applied to all classes: • Modify the domain master. • Write the `fSMORoleOwner` attribute. To delegate this AT, select the trustee(s), then apply it to the domain partitions container of your AD environment: **<forest-root-domain> > Configuration > Partitions**
Forest Configuration Operators - Change Schema Master Management	Grants permission to modify the schema master. To delegate this AT, select the trustee(s), then apply it to the domain schema container of your AD environment: **<forest-root-domain> > Configuration > Schema** IMPORTANT: When configuring this AT, always select the **Propagate permissions to Active Directory** option in the **Permissions Propagation** step of the **Delegation of Control Wizard**. **Figure 3: Delegation of Control Wizard – Permissions**

Access Template	Description
	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*.
Forest Configuration Operators - Computer Object Creation	Grants permission to create computer objects in the forest, applied to all classes. To delegate this AT, select the trustee(s), then apply it to the **Domain Controllers** container of your AD environment: **<domain> > Domain Controllers** This will apply the AT to every domain in your forest.
Forest Configuration Operators - Full Control for "Creator Owner"	Grants full permission to the Creator Owner role in your forest environment, applied to all classes. 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: **<forest-root-domain> > Configuration > Sites**
Forest Configuration Operators - Full Control	Grants full permission to perform domain configuration tasks on all computer objects. To delegate this AT, select the trustee(s), then apply the AT on the

Access Template	Description
on Computer Object	computer object that will be promoted to Domain Controller (DC).
Forest Configuration Operators - NTDS Domain Controller Settings Management	Grants permission to write the `queryPolicyObject` attribute, applied to the NT Directory Services (NTDS) of the DC settings. To delegate this AT, select the trustee(s), then apply it to the DC NTDS settings container of your AD environment: **<forest-root-domain>** > **Configuration** > **Sites** > **<site>** > **Servers** > **<domain-controller>** > **NTDS Settings**
Forest Configuration Operators - NTDS Site Settings Management	Grants permission to write the `queryPolicyObject` attribute, applied to the NTDS site settings. To delegate this AT, select the trustee(s), then apply it to the site NTDS settings container of your AD environment: **<forest-root-domain>** > **Configuration** > **Sites** > **<site>** > **NTDS Site Settings**
Forest Configuration Operators - Query Policies Management	Grants the following permissions: • Create or delete Query Policy Objects, applied to all classes. • Write all properties of Query Policies. To delegate this AT, select the trustee(s), then apply it to the site NTDS query policies container of your AD environment: **<forest-root-domain>** > **Configuration** > **Services** > **Windows NT** > **Directory Service** > **Query-Policies**
Forest Configuration Operators - Replication Management	Grants the following forest-level configuration permissions: • Manage the replication topology, applied to all classes. • Replicate directory changes, applied to all classes • Monitor AD replication, applied to the Directory Management Domain (DMD). • Replicate all directory changes, applied to the DMD. To delegate this AT, select the trustee(s), then apply the AT to the following AD container: **<forest-root-domain>** > **Configuration** NOTE: You must apply the permissions that are specified by this AT to the AD configuration schemas too. These are located in the following container: **<forest-root-domain>** > **Configuration** > **Schema**

Access Template	Description
	To apply the permissions to the **Schema** container, use native AD management tools, such as ADSI Edit.
Forest Configuration Operators - Server Object Creation	Grants permission to create all server child objects in the forest, applied to all classes. To delegate this AT, select the trustee(s), then apply the AT to the AD server configuration container: **<forest-root-domain>** > **Configuration** > **Sites** > **<site>** > **Servers**
Forest Configuration Operators - Site Objects - Read All Properties	Grants permission to read all site objects in the forest, applied to all classes. To delegate this AT, select the trustee(s), then apply the AT to the AD site configuration container: **<forest-root-domain>** > **Configuration** > **Sites**
Forest Configuration Operators - Trust Relationship Management	Grants the following permissions: • Create or delete Trusted Domain objects, applied to all classes. • Write all properties of Trusted Domains. To delegate this AT, select the trustee(s), then apply it to the domain 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
Replication Management Admins - Inter-Site Transports Management	Grants the following permissions: • Create or delete Site Link objects, applied to all classes. • Write all properties of Site Links. To delegate this AT, select the trustee(s), then apply it to the inter-site transport container of the forest root domain: **<forest-root-domain> > Configuration > Sites > Inter-Site Transports**

Access Template	Description
Replication Management Admins - Replication Topology Management	Grants permission to manage replication topology, applied to all classes. To delegate this AT, select the trustee(s), then apply it to the following AD containers: • **<forest-root-domain>** > **Configuration** • Every domain in the forest, including the forest root domain. NOTE: You must apply the permissions that are specified by this AT to the AD configuration schemas too. These are located in the following container: **<forest-root-domain>** > **Configuration** > **Schema** To apply the permissions to the **Schema** container, use native AD management tools, such as ADSI Edit.
Replication Management Admins - Site Management	Grants the following permissions, applied to all classes: • Write all site properties. • Create or delete connection objects. • Create or delete site objects. To delegate this AT, select the trustee(s), then apply it to the site configuration container of the forest root domain: **<forest-root-domain>** > **Configuration** > **Sites**
Replication Management Admins - Subnet Management	Grants the following permissions: • Create or delete subnet objects, applied to all classes. • Write all subnet object properties. To delegate this AT, select the trustee(s), then apply it to the subnet configuration container of the forest root domain: **<forest-root-domain>** > **Configuration** > **Sites** > **Subnets**

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
Replication Monitoring Operators - Windows 2000	Grants permission to manage replication topology, applied to all classes. NOTE: 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: • **<forest-root-domain>** > **Configuration** • Every domain in the forest, including the forest root domain. NOTE: You must apply the permissions that are specified by this AT to the AD configuration schemas too. These are located in the following container: **<forest-root-domain>** > **Configuration** > **Schema** To apply the permissions to the **Schema** container, use native AD management tools, such as ADSI Edit.
Replication Monitoring Operators - Windows Server 2003	Grants permission to monitor AD replication, applied to the Directory Management Domain (DMD). NOTE: Use this AT to configure replication monitoring in Windows Server 2003 Active Directory environments. To delegate this AT, select the trustee(s), then apply it to the following AD containers: • **<forest-root-domain>** > **Configuration** • Every domain in the forest, including the forest root domain. NOTE: You must apply the permissions that are specified by this AT to the AD configuration schemas too. These are located in the following container: **<forest-root-domain>** > **Configuration** > **Schema** To apply the permissions to the **Schema** container, use native AD management tools, such as ADSI Edit.

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

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

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
AD LDS Containers - Full Control	Grants full permission to: • Create new AD LDS containers. • Perform all administrative operations on existing AD LDS containers.
AD LDS Containers - Modify All Properties	Grants the following permissions: • List all AD LDS containers. • View or modify the properties of any AD LDS container.
AD LDS Containers - Read All Properties	Grants the following permissions: • List all AD LDS containers. • View the properties of any AD LDS container.
AD LDS Groups - Add/Remove Members	Grants the following permissions: • List all AD LDS groups. • View or modify the members of AD LDS groups.
AD LDS Groups - Full Control	Grants full permission to: • Create new AD LDS groups. • Perform all management tasks on existing AD LDS groups.

Access Template	Description
AD LDS Groups - Modify All Properties	Grants the following permissions: • List AD LDS groups. • View or modify all properties of AD LDS groups.
AD LDS Groups - Read All Properties	Grants the following permissions: • List AD LDS groups. • View all properties of AD LDS groups.
AD LDS OUs - Full Control	Grants full permission to: • Create new AD LDS Organizational Units (OUs). • Perform all management tasks on existing AD LDS OUs.
AD LDS OUs - Modify All Properties	Grants the following permissions: • List AD LDS OUs. • View or modify all properties of AD LDS OUs.
AD LDS OUs - Read All Properties	Grants the following permissions: • List AD LDS OUs. • View all properties of AD LDS OUs.
AD LDS Users - Full Control	Grants full permission to: • Create new AD LDS user accounts. • Perform all management tasks on existing AD LDS user accounts.
AD LDS Users - Modify All Properties	Grants the following permissions: • List AD LDS user accounts. • View or modify all properties of AD LDS user accounts.
AD LDS Users - Read All Properties	Grants the following permissions: • List AD LDS user accounts. • View all properties of AD LDS user accounts.
All AD LDS Objects - Full Control	Grants full permission to perform any management task on any AD LDS object.
All AD LDS Objects - Read All Properties	Grants the following permissions: • List all AD LDS objects. • View all properties of any AD LDS object.

Azure

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
Azure - Configuration Administrator	Grants the following permissions: • Read and write Azure tenants. • Read and write Azure applications. • Read Azure health check reports. • Read Azure license reports. • Read Azure roles reports.
Azure - Contact Full Control	Grants the following permissions: • Add and enable new Azure contacts. • View existing Azure contacts. • Update the properties of existing Azure contacts.

Access Template	Description
Azure - Full Control	Grants full permission to: • Read and write Azure configuration objects. • Read and write Azure user attributes. • Read and write Azure group attributes. • Read and write Azure M365 group objects.
Azure - Group Full Control	Grants the following permissions: • Add and enable new Azure groups. • View existing Azure groups. • Update the properties of existing Azure groups.
Azure - Health Check, O365 Roles Report and License Report	Grants permission to access the Azure health check, M365 roles and license reports. NOTE: This Access Template must be applied on a **Configuration** container.
Azure - O365 Groups Full Control	Grants the following permissions: • Add and enable new Azure M365 groups. • View existing Azure M365 groups. • Update the properties of existing Azure M365 groups.
Azure - Read All Attributes	Grants permission to read all Azure attributes. NOTE: This AT provides no additional permissions.
Azure - Read All Contact Attributes	Grants permission to read all Azure contact attributes. NOTE: This AT provides no additional permissions.
Azure - Read All Group Attributes	Grants the following permissions: • List all Azure groups. • View all Azure group properties.
Azure - Read All O365 Group Attributes	Grants the following permissions: • List all Azure M365 groups. • View all Azure M365 group properties.
Azure - Read All User Attributes	Grants permission to read all Azure user and guest user attributes. NOTE: This AT provides no additional permissions.

Access Template	Description
Azure - User Full Control	Grants the following permissions: • Create new Azure user and guest user accounts. • Perform all administrative operations on existing Azure user and guest user accounts.
Azure Cloud Contact- Create Objects	Grants permission to create cloud-only Azure contact accounts. NOTE: This AT provides no additional permissions.
Azure Cloud Contact - Delete Objects	Grants permission to delete cloud-only Azure contact accounts. NOTE: This AT provides no additional permissions.
Azure Cloud Contact - Full Control	Grants the following permissions: • Create new cloud-only Azure contact accounts. • Perform all administrative operations on existing cloud-only Azure contact accounts.
Azure Cloud Contact - Modify Objects	Grants permission to modify cloud-only Azure contact accounts. NOTE: This AT provides no additional permissions.
Azure Cloud Contact - Read All Attributes	Grants permission to read all cloud-only Azure contact attributes. NOTE: This AT provides no additional permissions.
Azure Cloud User - Create Objects	Grants permission to create cloud-only Azure user accounts. NOTE: This AT provides no additional permissions.
Azure Cloud User - Delete Objects	Grants permission to delete cloud-only Azure user accounts. NOTE: This AT provides no additional permissions.
Azure Cloud User - Full Control	Grants the following permissions: • Create new cloud-only Azure user accounts. • Perform all administrative operations on existing cloud-only Azure user accounts.
Azure Cloud User - Modify	Grants permission to modify cloud-only Azure user accounts. NOTE: This AT provides no additional permissions.

Access Template	Description
Objects	
Azure Cloud User - Read All Attributes	Grants permission to read all cloud-only Azure user attributes. NOTE: This AT provides no additional permissions.
Azure Create O365 Groups	Grants permission to create M365 groups. NOTE: This AT provides no additional permissions.
Azure Distribution Groups - Create Objects	Grants permission to create Azure distribution groups. NOTE: This AT provides no additional permissions.
Azure Distribution Groups - Delete Objects	Grants permission to delete Azure distribution groups. NOTE: This AT provides no additional permissions.
Azure Distribution Groups - Full Control	Grants the following permissions: • Add and enable new Azure distribution groups. • View existing Azure distribution groups. • Update the properties of existing Azure distribution groups.
Azure Distribution Groups - Modify Members	Grants permission to modify the members of Azure distribution groups. NOTE: This AT provides no additional permissions.
Azure Distribution Groups - Modify Objects	Grants the following permissions: • List all Azure distribution groups. • Update all Azure distribution group properties.
Azure Distribution Groups - Read All Attributes	Grants the following permissions: • List all Azure distribution groups. • Read all Azure distribution group properties.
Azure Guest User - Create Objects	Grants permission to create Azure guest user accounts. NOTE: This AT provides no additional permissions.
Azure Guest User - Delete Objects	Grants permission to delete Azure guest user accounts. NOTE: This AT provides no additional permissions.

Access Template	Description
Azure Guest User - Full Control	Grants the following permissions: • Create new Azure guest user accounts. • Perform all administrative operations on existing Azure guest user accounts.
Azure Guest User - Modify Objects	Grants the following permissions: • List all Azure guest user accounts. • Update all Azure guest user properties.
Azure Guest User - Read All Attributes	Grants the following permissions: • List all Azure guest user accounts. • Read all Azure guest user properties.
Azure Health Check Report	Grants permission to access Azure health check reports. NOTE: This Access Template must be applied on a **Configuration** container.
Azure License Report	Grants permission to access Azure license reports. NOTE: This Access Template must be applied on a **Configuration** container.
Azure Modify O365 Group Members	Grants permission to modify the membership list of M365 groups.
Azure O365 Roles Report	Grants permission to access M365 roles reports. NOTE: This Access Template must be applied on a **Configuration** container.
Azure Resource Mailboxes - Create Objects	Grants permission to create Azure resource mailboxes. NOTE: This AT provides no additional permissions.
Azure Resource Mailboxes - Delete Objects	Grants permission to delete Azure resource mailboxes. NOTE: This AT provides no additional permissions.
Azure Resource Mailboxes -	Grants the following permissions: • Add and enable new Azure resource mailboxes.

Access Template	Description
Full Control	• View existing Azure resource mailboxes. • Update the properties of existing Azure resource mailboxes.
Azure Resource Mailboxes - Modify Objects	Grants the following permissions: • List all Azure resource mailboxes. • Update the properties of Azure resource mailboxes.
Azure Resource Mailboxes - Read All Attributes	Grants the following permissions: • List all Azure resource mailboxes. • Read the properties of Azure resource mailboxes.
Azure Security Group - Create Objects	Grants permission to create Azure security groups. NOTE: This AT provides no additional permissions.
Azure Security Group - Delete Objects	Grants permission to delete Azure security groups. NOTE: This AT provides no additional permissions.
Azure Security Group - Full Control	Grants the following permissions: • Add and enable new Azure security groups. • View existing Azure security groups. • Update the properties of existing Azure security groups.
Azure Security Group - Modify Members	Grants permission to modify the members of Azure security groups.
Azure Security Group - Modify Objects	Grants the following permissions: • List all Azure security groups. • Update all Azure security group properties.
Azure Security	Grants the following permissions: • List all Azure security groups.

Access Template	Description
Group - Read All Attributes	• Read all Azure security group properties.
Azure Shared Mailboxes- Create Objects	Grants permission to create Azure shared mailboxes. NOTE: This AT provides no additional permissions.
Azure Shared Mailboxes - Delete Objects	Grants permission to delete Azure shared mailboxes. NOTE: This AT provides no additional permissions.
Azure Shared Mailboxes - Full Control	Grants the following permissions: • Add and enable new Azure shared mailboxes. • View existing Azure shared mailboxes. • Update the properties of existing Azure shared mailboxes.
Azure Shared Mailboxes - Modify Members	Grants the following permissions: • List all Azure shared mailboxes. • Update all Azure shared mailbox properties.
Azure Shared Mailboxes - Read All Attributes	Grants the following permissions: • List all Azure shared mailboxes. • Read all Azure shared mailbox properties.

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
Azure Health Check Allow for Search	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. NOTE: 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.

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
AR Server Security - Active Directory Container	Grants the following permissions to ensure default security on the **Active Directory** container: • Read all domain properties. • Write the LDAP server properties of the domain. • List all Active Directory (AD) resources. • Read all properties of AD resources.
AR Server Security - Active Directory Container - Self	Grants the following permissions to ensure default security on the **Active Directory** container for the security principal self: • Read the membership status of users (that is, their **Member Of** attribute). • Read the object class of users (that is, their **objectClass** attribute).
AR Server Security - AD LDS (ADAM) Container	Grants the following permissions to ensure default security on the **AD LDS (ADAM)** container: • List all Active Directory Lightweight Directory Services (AD LDS) resources. • Read all properties of AD LDS resources.

Access Template	Description
	• Read all properties of **crossRefContainers**.
AR Server Security - Application Configuration Objects	Grants the following permissions to ensure default security on application configuration objects: • List and read all properties of **Schema Cache** containers. • List and read all properties of Enterprise Directory Service (EDS) application configuration objects. • List and read all properties of EDS display specifier containers. • List and read all properties of control access rights. • List and read all properties of attribute schemas. • List and read all properties of class schemas. • List and read all properties of all containers. • List and read all properties of display specifiers.
AR Server Security - Client Sessions Container	Grants the following permissions to ensure default security on the **Client Sessions** container: • Write the **Client Version** attribute of connected users. • Read the object class of connected users.
AR Server Security - Configuration Objects	Grants the following permissions to ensure default security on configuration objects: • List and read all properties of the **Managed Domains** container. • List and read all properties of the **Managed Units** container. • Read all properties of ATs. • List and read all properties of policy objects. • List and read all version information. • List and read all properties of the **Configuration** container. • List and read all properties of the change tracking log configuration. • Read all properties of the Active Roles Administration Service. • Read the `edsvaXSLPolicyCheckReport` attribute of the EDS policy check configuration. • List and read all properties of the EDS management history replication partner. • List and read all properties of the **Management History Databases** container.

Access Template	Description
	• List and read all properties of the policy configuration. • List and read all properties of the **Azure Configuration** container (that is, the `edsAzureConfigurationContainer` resource). • List and read all properties of Azure containers. • List and read all properties of Azure tenants.
AR Server Security - Export/Import Application	Grants the following permissions to ensure default security on the export/import application: • Read the `edsvaDSMLProcessingInstructionsAsXML` attribute of applications. • Read the `edsvaAttributesExcludedFromImport` attribute of applications. • Read the object class of applications.
AR Server Security - Managed Units Container	Grants the following permissions to ensure default security on the **Managed Units** container: • List all Managed Units. • Read all properties of Managed Units.
AR Server Security - Web Interface Configuration	Grants the following permissions to ensure default security on the Active Roles Web Interface configuration objects: • Read all Web Interface configuration data. • Read and write the personal settings of Web Interface users.
AR Server Security - Workflow Container	Grants read permission to the **Workflow** container and its sub-containers.
Special - Block Permission Inheritance	When assigned to an object, this AT prevents propagating inheritable permissions to the children of the object and other target objects as well. When assigned to the **Active Directory** node, this AT blocks all inheritable AD permissions.

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
Computer Management - Full Control	Grants full permission to: • List and select computer resources. • Perform all management tasks on any computer.
Computer Management - Local Account Operator	Grants the following permissions: • Create, update, or delete local user accounts and groups on a computer. • List and select computers.
Computer Management - Network Share Operator	Grants the following permissions: • Create, update, or delete network shares on a computer. • List and select computers.
Computer Management -	Grants the following permissions:

Access Template	Description
Print Operator	• View or modify the properties of logical printers installed on a computer. • List and select computers.
Computer Management - Read-Only Access	Grants the following permissions: • View the properties of all computer resources. • List and select computers.
Computer Management - Server Operator	Grants the following permissions: • Start or stop services. • Pause, resume or cancel printing. • Create, update or delete network shares on a computer. • List and select computers. • List local users and groups. • View all properties of local user accounts and groups on a computer.
Computer Management - Service Operator	Grants the following permissions: • Perform all management tasks on services on a computer. • List and select computers.

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

Access Template	Description
Create	NOTE: This AT provides no additional permissions.
Local Groups - Delete	Grants permission to delete local groups on a computer. NOTE: This AT provides no additional permissions.
Local Groups - List	Grants permission to list the local groups on a computer. NOTE: This AT provides no additional permissions.
Local Groups - Read/Write General Information	Grants permission to view or modify the descriptions and membership lists of local groups on a computer. NOTE: This AT provides no additional permissions.
Local Groups - Rename	Grants permission to rename local groups on a computer. NOTE: This AT provides no additional permissions.
Local Users - Create	Grants permission to create local users on a computer. NOTE: This AT provides no additional permissions.
Local Users - Delete	Grants permission to delete local users on a computer. NOTE: This AT provides no additional permissions.
Local Users - List	Grants permission to list local users on a computer. NOTE: This AT provides no additional permissions.
Local Users - Read Group Membership	Grants permission to view the list of groups to which a local user belongs. NOTE: This AT provides no additional permissions.
Local Users - Read/Write Account Options	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.
Local Users - Read/Write General Information	Grants permission to view or modify the full name and description of local users on a computer. NOTE: This AT provides no additional permissions.
Local Users - Read/Write Profile Properties	Grants permission to view or modify the user profile and home folder settings of local users on a computer. NOTE: This AT provides no additional permissions.
Local Users - Rename	Grants permission to rename local users on a computer. NOTE: This AT provides no additional permissions.

Access Template	Description
Local Users - Write Password	Grants permission to change the password of local users on a computer. NOTE: This AT provides no additional permissions.
Printer Resources - Read/Write Advanced Information	Grants permission to view or modify the following settings of logical printers: • **Port** • **Advanced**
Printer Resources - Read/Write General Information	Grants permission to view or modify the following settings of logical printers: • **Name** • **Location** • **Comment**
Printer Resources - Read/Write Sharing Information	Grants permission to modify the sharing settings of logical printers (that is, enabling or disabling printer sharing). NOTE: This AT provides no additional permissions.
Services - List	Grants permission to list the services defined on a computer. NOTE: This AT provides no additional permissions.
Services - Read/Write General Information	Grants permission to view or modify the following service settings: • **Name** • **Display Name** • **Description** • **Path to Executable** • **Startup Type**
Services - Read/Write Log On Information	Grants permission to view or modify the **Log On As** setting of services. NOTE: This AT provides no additional permissions.
Services - Read/Write Start type	Grants permission to view or modify the **Startup Type** setting of services. NOTE: This AT provides no additional permissions.
Services - Start /Stop/	Grants permission to start, stop, pause, or resume services. NOTE: This AT provides no additional permissions.

Access Template	Description
Pause/ Resume	
Shares - Create	Grants permission to create network shares on a computer. NOTE: This AT provides no additional permissions.
Shares - List	Grants permission to list the network shares defined on a computer. NOTE: This AT provides no additional permissions.
Shares - Read/Write General Information	Grants permission to view or modify the following settings of network shares: • **Share Name** • **Path** • **Comment** • **User Limit**
Shares - Read/Write Permissions	Grants permission to view or modify share permissions on network shares. NOTE: This AT provides no additional permissions.
Shares - Stop Sharing	Grants permission to stop sharing folders on a computer. NOTE: 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
Access Rules - Full Control	Grants full permission to create, read, update and delete Access Rule objects. To delegate this AT, apply it on the container(s) that hold Access Rule objects. For more information on applying ATs on resources, see *Applying Access Templates on a securable object* in the *Active Roles Administration Guide*.
Access Rules - Modify	Grants permission to view or modify all properties of Access Rule objects. To delegate this AT, apply it on the container(s) that hold Access Rule objects. For more information on applying ATs on resources, see *Applying Access Templates on a securable object* in the *Active Roles Administration Guide*.
Access Rules - View	Grants permission to view all properties of Access Rule objects. To delegate this AT, apply it on the container(s) that hold Access Rule

Access Template	Description
	objects. For more information on applying ATs on resources, see *Applying Access Templates on a securable object* in the *Active Roles Administration Guide*.
Automation Workflow - Full Control	Grants full permission to: • View or modify automation workflow definitions. • Start automation workflows. • View the run history of automation workflows. To delegate this AT, apply it either to automation workflow definition objects, or to containers holding automation workflow definitions. For more information on applying ATs on resources, see *Applying Access Templates on a securable object* in the *Active Roles Administration Guide*.
Automation Workflow - View	Grants permission to view automation workflow definitions and their run history. To delegate this AT, apply it either to automation workflow definition objects, or to containers holding automation workflow definitions. For more information on applying ATs on resources, see *Applying Access Templates on a securable object* in the *Active Roles Administration Guide*.
Automation Workflow - View and Run	Grants the following permissions: • Read automation workflow definitions. • Start automation workflows. • View the run history of automation workflows. To delegate this AT, apply it either to automation workflow definition objects, or to containers holding automation workflow definitions. For more information on applying ATs on resources, see *Applying Access Templates on a securable object* in the *Active Roles Administration Guide*.
Configuration - Add/Remove Managed Domains	Grants the following permissions: • Register domains with Active Roles. • View or modify registration information for managed domains.
Configuration - Manage Access	Grants the following permissions: • Create, read, update or delete ATs and AT containers.

Access Template	Description
Templates	• Add or remove permissions to or from ATs.
Configuration - Manage Configuration	Grants permission to view or change any Active Roles configuration settings, except Active Roles replication settings.
Configuration - Manage Policy Objects	Grants the following permissions: • Create, read, update or delete Active Roles Policy Objects and Policy Object containers. • Configure Active Roles policies.
Configuration - Manage Script Modules	Grants permission to create, read, update or delete Active Roles Script Modules and Script Module containers.
Configuration - View Configuration	Grants permission to view any Active Roles configuration settings, including replication settings.
Managed Object Statistics - Read Detailed Data	Grants permission to read detailed statistical information about the number of objects managed by Active Roles.
Managed Object Statistics - View Report	Grants permission to read the Active Roles product usage statistics, that is, statistical reports on the number of objects managed with the product.
Workflow - View Workflow Containers	Grants permission to access containers that hold workflow definition objects. To delegate this AT, apply it to the **Configuration** > **Policies** > **Workflow** node of the Active Roles Console. For more information on applying ATs on resources, see *Applying Access Templates on a securable object* in the *Active Roles Administration Guide*.

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

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

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

Exchange

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
Exchange - Configure Calendar Settings	Grants the following permissions: • View or modify the **Calendar Settings** of Exchange recipients. • List all Exchange users. • View all Exchange properties of users.
Exchange - Configure E-mail Addresses	Grants the following permissions: • View or modify the **E-Mail Addresses** settings of Exchange recipients. • List all Exchange users, groups and contacts. • View all Exchange properties of users, groups and contacts.
Exchange - Configure	Grants the following permissions:

Access Template	Description
Exchange Advanced Settings	• View or modify the **Advanced** Exchangesettings of Exchange recipients. • List all Exchange users, groups and contacts. • View all Exchange properties of users, groups and contacts.
Exchange - Configure Exchange General Settings	Grants the following permissions: • View or modify the **General** Exchangesettings of Exchange recipients. • List all Exchange users, groups and contacts. • View all Exchange properties of users, groups and contacts.
Exchange - Configure Mail Flow Settings	Grants the following permissions: • View or modify the **Mail Flow Settings** of Exchange recipients. • List all Exchange users, groups and contacts. • View all Exchange properties of users, groups and contacts.
Exchange - Configure Mailbox Features	Grants the following permissions: • View or modify the **Mailbox Features** settings of Exchange recipients. • List all Exchange users. • View all Exchange properties of users.
Exchange - Configure Mailbox Settings	Grants the following permissions: • View or modify the **Mailbox Settings** of Exchange recipients. • List all Exchange users. • View all Exchange properties of users.
Exchange - Configure Resource General Settings	Grants the following permissions: • View or modify the **Resource** > **General** settings of Exchange recipients. • List all Exchange users. • View all Exchange properties of users.
Exchange - Configure Resource Information Settings	Grants the following permissions: • View or modify the **Resource** > **Information** settings of Exchange recipients. • List all Exchange users. • View all Exchange properties of users.

Access Template	Description
Exchange - Configure Resource In-Policy Requests	Grants the following permissions: • View or modify the **Resource** > **In-Policy Requests** settings of Exchange recipients. • List all Exchange users. • View all Exchange properties of users.
Exchange - Configure Resource Out-of-Policy Requests	Grants the following permissions: • View or modify the **Resource** > **Out-of-Policy Requests** settings of Exchange recipients. • List all Exchange users. • View all Exchange properties of users.
Exchange - Configure Resource Policy	Grants the following permissions: • View or modify the **Resource** > **Policy** settings of Exchange recipients. • List all Exchange users. • View all Exchange properties of users.
Exchange - Manage Resource, Linked and Shared Mailboxes	Grants the following permissions: • Create, read, or update room mailboxes, equipment mailboxes, linked mailboxes and shared mailboxes. • List all Exchange users. • View all Exchange properties of users.
Exchange - Perform Exchange Tasks	Grants the following permissions: • Create any kind of mailbox. • Use the **Exchange Task Wizard** to manage Exchange recipients. • List all Exchange users, groups and contacts. • View all Exchange properties of users, groups and contacts.
Exchange - Recipients Full Control	Grants the following permissions: • Perform all Exchange recipient management tasks. • View or modify all properties of Exchange recipients. • List all Exchange users, groups and contacts. • View all Exchange properties of users, groups and contacts.

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

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

Access Template	Description
mail Address	
Exchange - Delete User Mailbox	Grants permission to delete user mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Designate Contact as Mail-Enabled	Grants permission to designate contacts as mail-enabled recipients. NOTE: This AT provides no additional permissions.
Exchange - Designate Group as Mail-Enabled	Grants permission to designate groups as mail-enabled recipients. NOTE: This AT provides no additional permissions.
Exchange - Designate User as Mail-Enabled	Grants permission to designate users as mail-enabled recipients. NOTE: This AT provides no additional permissions.
Exchange - Enable Archive	Grants permission to enable archives for Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Enable Unified Messaging	Grants permission to enable Unified Messaging for Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Move Mailbox	Grants permission to move Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Read ERFM Attributes	Grants permission to read the Exchange Resource Forest Management-specific (ERFM-specific) attributes of master accounts. TIP: Assign this AT to the administrators delegated to manage the ERFM solution and its associated resources. NOTE: Consider the following when planning to delegate permissions for reading ERFM-specific attributes: • This AT will work properly only if Exchange Resource Forest Management (ERFM) is configured in your organization. For more information, see *Configuring linked mailboxes with Exchange Resource Forest Management* in the *Active Roles Administration Guide*. • You do not have to apply this AT if your organization already uses any general-purpose ATs for delegating Exchange

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.
Exchange - Read/Write Address Book Policy	Grants permission to change the address book policy settings on the **Mailbox Settings** page of Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Advanced Properties for Mailbox-Enabled Users	Grants permission to view or modify the **Advanced** Exchange properties for mailbox-enabled users. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Advanced Properties for Mail-Enabled Groups	Grants permission to view or modify the **Advanced** Exchange properties for mail-enabled groups. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Advanced Properties for Mail-Enabled Users and Contacts	Grants permission to view or modify the **Advanced** Exchange properties for mail-enabled contacts and users. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Archive	Grants permission to view or modify the **Mailbox Features** > **Archive** settings of Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Archive Quota	Grants permission to view or modify the archive quota settings on the **Mailbox Features** page of Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Autoreply Settings	Grants permission to view or modify the automatic reply settings of Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Custom	Grants permission to view or change custom Exchange attributes. NOTE: This AT provides no additional permissions.

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

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

Access Template	Description
Read/Write POP3	settings for Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Protocol Settings	Grants permission to view or modify the protocol settings for Exchange recipients. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Recipient Limits	Grants permission to view or modify the recipient limit settings for Exchange recipients. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Role Assignment Policy	Grants permission to view or modify the **Mailbox Settings** > **Role Assignment Policy** settings for Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Send on Behalf Permission	Grants permission to view or modify the **Send on Behalf** permissions of Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Sharing	Grants permission to view or modify the **Mailbox Settings** > **Sharing** settings of Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Storage Quotas	Grants permission to view or modify the **Mailbox Settings** > **Storage Quotas** settings of Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Unified Messaging	Grants permission to enable or disable Unified Messaging for Exchange mailboxes. NOTE: This AT provides no additional permissions.
Exchange - Read/Write Up-to-date Notifications	Grants permission to view or modify the **Mailbox Features** > **Up-to-date Notifications** settings of Exchange mailboxes. NOTE: 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
Skype for Business Server - User Disable/Re-enable	Grants the following permissions: • Temporarily disable or re-enable the users of the Skype for Business server. • View Skype for Business server users. • View the Session Initiation Protocol (SIP) address. • View telephony-related settings. • View the user policy assignments of the Skype for Business server.
Skype for Business Server - User Full Control	Grants full permission to: • Add, enable or remove Skype for Business users. • View Skype for Business server users. • View or modify the SIP address. • View or modify telephony-related settings. • View or modify the user policy assignments of the Skype for Business server.

Access Template	Description
	• Temporarily disable or re-enable the users of the Skype for Business server. • Move users to another Skype for Business server or pool.
Skype for Business Server - User Policies	Grants the following permissions: • View Skype for Business server users. • View the SIP address. • View telephony-related settings. • View or modify the user policy assignments of the Skype for Business server.
Skype for Business Server - User Telephony	Grants the following permissions: • View Skype for Business server users. • View the SIP address. • View or modify telephony-related settings. • View the user policy assignments of the Skype for Business server.

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
Starling -Two Factor Authentication User	Grants the minimal read permission required to enable Starling Two-Factor Authentication (Starling 2FA) for a user. NOTE: 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

Access Template	Description
User Interface Management-MMC Full control	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
Self - Account Management	Grants permission to users to view or modify their profile information on the Active Roles Web Interface. TIP: When configuring this AT, specify the **Self** built-in account as the trustee. For more information on applying ATs on resources, see *Applying Access Templates on a securable object* in the *Active Roles Administration Guide*.
Self - Group Management	Grants permission to users to view or modify the groups they manage. TIP: When configuring this AT, specify one of these built-in accounts as the trustee: • **Primary Owner (Managed By)** • **Secondary Owners** For more information on applying ATs on resources, see *Applying Access Templates on a securable object* in the *Active Roles Administration Guide*. NOTE: 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. To grant that permission, apply the **Active Directory** > **All Objects - Read All Properties** AT to a scope containing the group member objects, then set the **Authenticated Users** built-in account as the

Access Template	Description
	trustee.
Self - Group Membership Approval Setting	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.
Self - Group Membership Management	Grants permission to users to add or remove their own user account to or from groups. TIP: When configuring this AT, consider the following recommendations: • 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. • To allow users to view the groups they are members of, assign them the **Self - Account Management** 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 **Self** account as the trustee. For more information on applying ATs on resources, see *Applying Access Templates on a securable object* in the *Active Roles Administration Guide*.

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

Contacting us

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

Technical support resources

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

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

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