One Identity Active Roles

Access Templates Available out of the Box

Legend

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

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

Active Roles Access Templates Available out of the Box
Updated - March 2022
Version - 7.5.2

Contents

1

Introduction

Active Roles (formerly known as ActiveRoles®) comes with an extensive suite of predefined Access Templates that facilitate the delegation of various administrative tasks. The key goal for Access Templates is to simplify the management of administration related permissions. Active Roles does this by abstracting the low-level permissions on directory objects and managing them as a single unit—Access Template—based on the task that an administrator wants to delegate.

The predefined Access Templates are installed with Active Roles out of the box. These templates allow the Active Roles administrator to delegate the correct level of administrative authority quickly and consistently.

This document provides a comprehensive list of Access Templates that install with Active Roles out of the box.

2

Access Templates

The predefined Access Templates are grouped by category into the following containers:

- **Active Directory** Templates to delegate Active Directory service management and Active Directory data management tasks.
- **Azure** Templates to delegate the configuration and management of Azure objects.
- **AD LDS (ADAM)** Templates to delegate data management tasks for Microsoft Active Directory Lightweight Directory Services (AD LDS) - an independent mode of Active Directory formerly known as Active Directory Application Mode (ADAM).
- **Computer Resources** Templates to delegate the management of computer resources, such as printers or network shares.
- **Configuration** Templates to delegate the management of Active Roles configuration objects, such as Policy Objects or Access Templates.
- **Exchange** Templates to delegate the management of Exchange recipients, such as mailbox-enabled users or mail-enabled groups.
- **Skype for Business Server** Templates to delegate the management of Skype for Business Server users or contacts. Require the Skype for Business Server user management policies to be applied, as described in the *Skype for Business Server User Management Administration Guide* for *Active Roles*.
- **Starling** Templates to delegate required permission to perform Starling operations.
- **User Interfaces** Templates to delegate permission to access MMC interface.
- **User Self-management** Templates to delegate self-management tasks to end-users (for instance, allowing end-users to view or change certain properties of their own accounts in the Web Interface).

These containers are located in the **Configuration/Access Templates** container. Some of these containers include the **Advanced** sub-container to hold Access Templates with very granular permission specifications.

The tables below group Access Template by category, and include the following information on each Access Template:

- **Access Template** Access Template name.
- **Description** Tasks that can be delegated with the Access Template.

Active Directory Service Management

You can use Access Templates in this category to delegate management tasks on the directory service. Access Templates are grouped by role for delegating service management as follows:

- Forest Configuration Operators
- Domain Configuration Operators
- Service Admin Managers
- Replication Management Admins
- Replication Monitoring Operators

Engineered by Microsoft, these role recommendations take into account well-defined sets of logically related administrative tasks and the security sensitivity and impact of these tasks (see Best Practices for Delegating Active Directory Administration at http://technet.microsoft.com/en-us/library/cc773318.aspx).

The service management-related Access Templates are located in subfolders of the folder **Configuration/Access Templates/Active Directory/Best Practices for Delegating Active Directory Administration**, with each subfolder containing the Access Templates specific to a certain role.

To implement a given role, you must apply each of the role-specific Access Templates as specified in the description of the Template. For example, to implement the Forest Configuration Operators role for a certain group, you must select the group as a Trustee and then apply the Access Templates held in the **Forest Configuration Operators** subfolder.

IMPORTANT:

- When applying service management-related Access Templates, you must select the **Propagate permissions to Active Directory** check box on the **Permissions Propagation** page in the Delegation of Control Wizard. This ensures the appropriate permission entries are added to Active Directory.
- As Active Roles does not provide the ability to apply Access Templates to the Schema container, you should use native tools, such as ADSI Edit, to apply permissions to that container as appropriate. For details, see descriptions of the Access Templates later this section.

Forest Configuration Operators

The following is the set of administrative tasks assigned to this role:

- Create a child domain in an existing domain tree
- Demote the last domain controller in a child domain
- Demote the last domain controller in a tree-root domain

- Raise forest functional level
- Create all types of trusts for all domains
- Delete all types of trusts for all domains
- Change the direction of a trust
- Enable/disable name suffix routing (for a given suffix) in a forest
- Reset the trust passwords shared by a trust-pair
- Force the removal of a trust
- Enable/disable SID History on an outbound forest trust
- Enable/disable SID filtering
- Enable selective authentication on an outbound forest/external trust
- Enable/disable placing of name suffix (top level names) information on a realm trust
- Add/remove top-level names from a realm trust
- Add/remove top-level name exclusions from a realm trust
- Modify the transitivity of a realm-trust
- Transfer the domain naming master role
- Seize the domain naming master role
- Manage all LDAP query policy related administrative tasks

To implement the Forest Configuration Operators role, Active Roles offers the following Access Templates, located in the **Forest Configuration Operators Role** subfolder of the **Access Templates/Active Directory/Best Practices for Delegating Active Directory Administration** folder.

Table 1: Forest Configuration Operators

Access Template	Description
Forest Configuration Operators - Change Domain Master Management	Permissions: • Change Domain Master, applied to All Classes • Write fSMORoleOwner, applied to All Classes Apply this Access Template on: • <Forest-Root-Domain>/Configuration/Partitions
Forest Configuration Operators - Computer Object Creation	Permissions: • Create Computer Objects, applied to All Classes Apply this Access Template on: • <Domain>/Domain Controllers (for every domain in the forest)
Forest Configuration	Permissions:

Access Template	Description
Operators - Full Control for "Creator Owner"	• Full Control, applied to All Classes Select Creator Owner as Trustee, and apply this Access Template on: • <Forest-Root-Domain>/Configuration/Sites
Forest Configuration Operators - Full Control on Computer Object	Permissions: • Full Control, applied to Computer Apply this Access Template on: • Computer object representing the server that is to be promoted to domain controller
Forest Configuration Operators - NTDS Domain Controller Settings Management	Permissions: • Write queryPolicyObject, applied to Domain Controller Settings Apply this Access Template on: • <Forest-Root-Domain>/ Configuration/Sites/<Site>/Servers/<Domain Controller>/NTDS Settings
Forest Configuration Operators - NTDS Site Settings Management	Permissions: • Write queryPolicyObject, applied to Site Settings Apply this Access Template on: • <Forest-Root-Domain>/Configuration/Sites/<Site>/NTDS Site Settings
Forest Configuration Operators - Query Policies Management	Permissions: • Create/Delete Query Policy Objects, applied to All Classes Write All Properties, applied to Query Policy • Apply this Access Template on: <Forest-Root-Domain>/ Configuration/Services/Windows NT/Directory Service/Query-Policies
Forest Configuration Operators - Replication Management	Permissions: • Manage Replication Topology, applied to All Classes • Replicating Directory Changes, applied to All Classes • Monitor Active Directory Replication, applied to DMD

Access Template	Description
	• Replicating Directory Changes All, applied to DMD Apply this Access Template on: • <Forest-Root-Domain>/Configuration The permissions specified by this Access Template must also be applied on: • <Forest-Root-Domain>/Configuration/Schema You can do this using native AD management tools, such as the ADSI Edit tool.
Forest Configuration Operators - Server Object Creation	Permissions: • Create All Child Objects, applied to All Classes Apply this Access Template on: • <Forest-Root-Domain>/ Configuration/Sites/<Site>/Servers
Forest Configuration Operators - Site Objects - Read All Properties	Permissions: • Read All Properties, applied to All Classes Apply this Access Template on: • <Forest-Root-Domain>/Configuration/Sites
Forest Configuration Operators - Trust Relationship Management	Permissions: • Create/Delete Trusted Domain Objects, applied to All Classes Write All Properties, applied to Trusted Domain • Apply this Access Template on: <Domain>/System (for every domain in the forest)

Domain Configuration Operators

The following is the set of administrative tasks assigned to this role:

- Create a replica (additional domain controller)
- Remove a replica
- Designate a domain controller as a global catalog
- Un-designate a domain controller as a global catalog
- Rename a domain controller

- Raise domain functional level
- Create a replica (additional domain controller)
- Remove a replica
- Transfer the RID master role
- Transfer the PDC emulator master role
- Transfer the infrastructure master role
- Seize the RID master role
- Seize the PDC emulator master role
- Seize the infrastructure master role
- Protect and manage the default domain controllers OU
- Protect and manage the content stored in the System container
- Restore Active Directory from backup

To implement the Domain Configuration Operators role, Active Roles offers the following Access Templates, located in the **Domain Configuration Operators Role** subfolder of the **Access Templates/Active Directory/Best Practices for Delegating Active Directory Administration** folder.

Table 2: Domain Configuration Operators

Access Template	Description
Domain Configuration Operators - Domain Controllers OU Management	Permissions: • Full Control, applied to All Classes Apply this Access Template on: • <Domain>/Domain Controllers
Domain Configuration Operators - Domain Management	Permissions: • Add/Remove Replica In Domain, applied to All Classes • Change Infrastructure Master, applied to All Classes • Change PDC, applied to All Classes • Write fSMORoleOwner, applied to All Classes • Write msDS-Behavior-Version, applied to All Classes Apply this Access Template on: • <Domain>
Domain Configuration Operators - Full Control for "Creator Owner"	Permissions: • Full Control, applied to All Classes Select Creator Owner as Trustee, and apply this Access

Access Template	Description
	Template on: • <Forest-Root-Domain>/Configuration/Sites
Domain Configuration Operators - Full Control on Computer Object	Permissions: • Full Control, applied to Computer Apply this Access Template on: • Computer object representing the server that is to be promoted to domain controller
Domain Configuration Operators - Infrastructure Master Management	Permissions: • Write fSMORoleOwner, applied to All Classes • Change Infrastructure Master, applied to All Classes Apply this Access Template on: • <Domain>/Infrastructure
Domain Configuration Operators - Replication Management	Permissions: • Manage Replication Topology, applied to All Classes • Replicating Directory Changes, applied to All Classes • Monitor Active Directory Replication, applied to DMD • Replicating Directory Changes All, applied to DMD Apply this Access Template on: • <Domain> • <Forest-Root-Domain>/Configuration The permissions specified by this Access Template must also be applied on: • <Forest-Root-Domain>/Configuration/Schema You can do this using native AD management tools, such as the ADSI Edit tool.
Domain Configuration Operators - RID Master Management	Permissions: • Change Rid Master, applied to All Classes • Write fSMORoleOwner, applied to All Classes Apply this Access Template on: • <Domain>/System/RID Manager$
Domain Configuration	Permissions:

Access Template	Description
Operators - Server Object Creation	• Create All Child Objects, applied to All Classes Apply this Access Template on: • <Forest-Root-Domain>/ Configuration/Sites/<Site>/Servers
Domain Configuration Operators - Site Objects - Read All Properties	Permissions: • Read All Properties, applied to All Classes Apply this Access Template on: • <Forest-Root-Domain>/Configuration/Sites
Domain Configuration Operators - System Container Management	Permissions: • Full Control, applied to All Classes Apply this Access Template on: • <Domain>/System

Service Admin Managers

The following is the set of administrative tasks assigned to this role:

- Manage and protect all service administrator security groups in the forest
- Manage and protect all service administrator accounts in the forest

To implement the Service Admin Managers role, Active Roles offers the following Access Templates, located in the **Service Admin Managers Role** subfolder of the **Access Templates/Active Directory/Best Practices for Delegating Active Directory Administration** folder.

Table 3: Service Admin Managers

Access Template	Description
Service Admin Managers - Admin SD Holder Management	Permissions: • Full Control, applied to All Classes Apply this Access Template on: • <Domain>/System/AdminSDHolder (for every domain in the forest)

Replication Management Admins

The following is the set of administrative tasks assigned to this role:

- Create a site and add a site
- Rename a site
- Specify the location of a site
- Delete a site
- Create a subnet and add a subnet
- Specify the location of a subnet
- Associate a subnet with a site
- Delete a subnet
- Create a site link
- Add or remove sites to and from a site link
- Modify the cost associated with a site link
- Modify the replication period associated with a site link
- Modify the replication schedule for a site link
- Delete a site link
- Create a site link bridge (object)
- Add or remove sites to and 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
- Delete a site link bridge (object)
- Create a connection (only if needed)
- Delete a connection (only if needed)
- Take ownership of a KCC-generated connection object
- Manually set a schedule for connection objects
- Enable and disable data compression for inter-site replication
- Change the default setting for the intra-site replication schedule within a site
- Designate or remove a preferred bridgehead server
- Replace a failed preferred bridgehead server
- Force replication between two servers
- Force a synchronization between two servers
- Disable automatic topology generation for a site
- Disable automatic topology cleanup for a site
- Disable minimum hops topology for a site

- Disable automatic stale server detection for a site
- Disable automatic inter-site topology generation for a site
- Disable inbound replication on a domain controller
- Disable outbound replication on a domain controller
- Enable reciprocal replication between sites (only for IP transport links)
- Enable change notification between sites (only for IP transport links)
- Force replication topology generation

To implement the Replication Management Admins role, Active Roles offers the following Access Templates, located in the **Replication Management Admins Role** subfolder of the **Access Templates/Active Directory/Best Practices for Delegating Active Directory Administration** folder.

Table 4: Replication Management Admins

Access Template	Description
Replication Management Admins - Inter-Site Transports Management	Permissions: • Create/Delete Site Links Objects, applied to All Classes • Write All Properties, applied to Site Link Apply this Access Template on: • <Forest-Root-Domain>/Configuration/Sites/Inter-Site Transports
Replication Management Admins - Replication Topology Management	Permissions: • Manage Replication Topology, applied to All Classes Apply this Access Template on: • <Forest-Root-Domain>/Configuration • <Domain> (for every domain in the forest, including the forest root domain) NOTE: The permissions specified by this Access Template must also be applied on: • <Forest-Root-Domain>/Configuration/Schema You can do this using native AD management tools, such as the ADSI Edit tool.
Replication Management Admins - Site Management	Permissions: • Write All Properties, applied to All Classes • Create/Delete Connection Objects, applied to All Classes

Access Template	Description
	• Create/Delete Site Objects, applied to All Classes Apply this Access Template on: • <Forest-Root-Domain>/Configuration/Sites
Replication Management Admins - Subnet Management	Permissions: • Create/Delete Subnet Objects, applied to All Classes • Write All Properties, applied to Subnet Apply this Access Template on: • <Forest-Root-Domain>/Configuration/Sites/Subnets

Replication Monitoring Operators

The following is the set of administrative tasks assigned to this role:

- Get replication latency information
- Get pending operations on a domain controller
- Get replication summary information
- Check replication status

To implement the Replication Monitoring Operators role, Active Roles offers the following Access Templates, located in the **Replication Monitoring Operators Role** subfolder of the **Access Templates/Active Directory/Best Practices for Delegating Active Directory Administration** folder.

Table 5: Replication Monitoring Operators

Access Template	Description
Replication Monitoring Operators - Windows 2000	This Access Template is to be used in Windows 2000 Active Directory environments. Permissions: • Manage Replication Topology, applied to All Classes Apply this Access Template on: • <Forest-Root-Domain>/Configuration • <Domain> (for every domain in the forest, including the forest root domain) NOTE: The permissions specified by this Access Template must

Access Template	Description
	also be applied on: • <Forest-Root-Domain>/Configuration/Schema You can do this using native AD management tools, such as the ADSI Edit tool.
Replication Monitoring Operators - Windows Server 2003	This Access Template is to be used in Windows Server 2003 Active Directory environments. Permissions: • Monitor Active Directory Replication, applied to DMD Apply this Access Template on: • <Forest-Root-Domain>/Configuration • <Domain> (for every domain in the forest, including the forest root domain) NOTE: The permissions specified by this Access Template must also be applied on: • <Forest-Root-Domain>/Configuration/Schema You can do this using native AD management tools, such as the ADSI Edit tool.

Active Directory Data Management

You can use Access Templates in this category to delegate management tasks on the content that is stored in Active Directory. The data management tasks include, but are not limited to, managing user objects (users), computer objects (computers), and groups.

Table 6: Active Directory Data Management

Access Template	Description
All Objects - Full Control	Perform any administrative operation on any object in Active Directory. This Access Template allows data owners to delegate control of Active Directory objects to data administrators who are responsible for carrying out all tasks required to manage the Active Directory contents.
All Objects - Read All Properties	List directory objects and view all properties of any object in Active Directory.

Access Template	Description
All Objects - View or Restore Deleted Objects	Apply this template to a container to allow viewing and restoring Active Directory objects that were deleted from that container.
Claim Types - Full Control	Create new claim types; perform all administrative operations on existing claim types. Claim types determine the claims to be issued for an Active Directory security principal upon its authentication. Claim types are used to define permissions when authoring claim-based access rules.
Claim Types - Modify All Properties	View or change all claim type properties.
Claim Types - Read All Properties	List claim types; view all claim type properties.
Computers - Create Computer Accounts	Create new computer accounts; view all properties of computer accounts.
Computers - Full Control	Create new computer accounts; perform all administrative tasks on existing computer accounts.
Computers - Modify All Properties	View or change all properties of computer accounts.
Computers - Move Computer Accounts	Move computer accounts; view all properties of computer accounts.
Computers - Read All Properties	List computer accounts. View all properties of computer accounts.
Computer - Reset Computer Accounts	Reset computer accounts; view all properties of computer accounts.
Contacts - Create Contacts	Create new contacts, view all properties of contacts.
Contacts - Full Control	Create new contacts; perform all administrative operations on existing contacts.
Contacts - Modify All Properties	View and modify all properties of contacts.
Contacts - Modify Picture	View or change the image of the contact (the thumbnailPhoto attribute of the contact object). View all properties of the contact object in the directory.
Contacts - Read All Properties	List contacts, view all properties of contacts.
Domains - Read All Properties	List domain objects; view all properties of domain objects.

Access Template	Description
gMSA - Full Control	Create new group Managed Service Accounts; perform all administrative operations on existing group Managed Service Accounts.
gMSA - Modify All Properties	View or change all properties of group Managed Service Accounts.
gMSA - Modify Membership Policy	View or change the list of computers and computer groups allowed to use a given group Managed Service Account.
gMSA - Read All Properties	List group Managed Service Accounts; view all properties of group Managed Service Accounts.
Groups - Add/Remove Members	View and modify lists of group members.
Groups - Create Groups	Create new groups, view all properties of groups.
Groups - Full Control	Create new groups; perform all administrative operations on existing groups.
Groups - Manage Dynamic Groups	Configure rules-based management of group membership lists; view all properties of groups; list groups in containers; list containers.
Groups - Modify All Properties	View and modify all properties of groups.
Groups - Modify Picture	View or change the image of the group (the thumbnailPhoto attribute of the group object). View all properties of the group object in the directory.
Groups - Perform Deprovision Tasks	Deprovision groups; view all properties of groups. This template is intended to delegate the use of the Deprovision command on groups without requiring the delegation of the create/delete operation.
Groups - Perform Undo Deprovision Tasks	Restore (un-deprovision) groups; view all properties of groups. This template is intended to delegate the use of the Undo Deprovisioning command on groups.
Groups - Read all Properties	List groups, view all properties of groups.
OUs - Create OUs	Create new Organizational Units; view all properties of Organizational Units.
OUs - Full Control	Create new Organizational Units; perform all administrative operations on existing Organizational Units.
OUs - Modify All Properties	View and modify all properties of Organizational Units.

Access Template	Description
OUs - Read All Properties	List Organizational Units; view all properties of Organizational Units.
Printers - Full Control	Create new printer queue objects; perform all administrative operations on existing printer queue objects.
Printers - Modify All Properties	View and modify all properties of printer queue objects.
Printers - Read All Properties	List printer queue objects; view all properties of printer queue objects.
Shared Folders - Full Control	Create new shared folder objects; perform all administrative operations on existing shared folder objects.
Shared Folders - Modify All Attributes	View and modify all properties of shared folder objects.
Shared Folders - Read All Properties	List shared folder objects; view all properties of shared folder objects.
Users - Create User Accounts	Create new user accounts; view all properties of user accounts.
Users - Delete User Accounts	Delete user accounts; view all properties of user accounts.
Users - Perform Deprovision Tasks	Deprovision user accounts and other user-related resources; view all properties of user accounts. This template is intended to delegate the use of the Deprovision command on user accounts without requiring the delegation of the create/delete operation.
Users - Perform Undo Deprovision Tasks	Restore (un-deprovision) user accounts; view all properties of user accounts. This template is intended to delegate the use of the Undo Deprovisioning command on user accounts.
Users - Full Control	Create new user accounts; perform all administrative operations on existing user accounts.
Users - Help Desk	Reset user passwords, unlock user accounts, assign or remove digital (X.509) certificates from user accounts, and view all properties of user accounts. Recommended for implementing Help Desk. Data owners can use this Access Template to delegate day-to-day operations to the Help Desk service.

Access Template	Description
Users - Modify All Properties	View and modify all properties of user accounts.
Users - Modify Personal Data	Manage a basic set of HR-related properties in user accounts.
Users - Modify Picture	View or change the image of the user (the thumbnailPhoto attribute of the user account). View all properties of the user account in the directory.
Users - Move User Accounts	Move user accounts; view all properties of user accounts.
Users - Pager & Cell Phone Numbers	View and modify mobile phone and pager numbers in user accounts, view all properties of user accounts.
Users - Phone Number & Address	Modify the address settings and telephone numbers in user accounts; view all properties of user accounts.
Users - Read All Properties	List user accounts; view all properties of user accounts.
Users and Groups - Basic Management	List groups and user accounts, add/remove them into/from groups, reset user passwords, view and modify logon-related properties of user accounts.

Active Directory/Advanced: Computer Objects

Table 7: Active Directory/Advanced: Computer Objects

Access Template	Description
Computer Objects – Create	Create computer objects; no other permissions are included.
Computer Objects – Delete	Delete computer objects; no other permissions are included.
Computer Objects – List	List computer objects; no other permissions are included.
Computer Objects – Read/Write Account Restrictions	View and modify properties that describe account restrictions for computer objects (User-Account-Restrictions property set); no other permissions are included. Property set members: See "User-Account-Restrictions Property Set" at http://msdn.microsoft.com/en-us/library/ms684412.aspx
Computer Objects – Read/Write General	View and modify properties that constitute general information for computer objects:

Access Template	Description
Information	• Computer name (pre-Windows 2000) • DNS name • Role • Description • The flags that control password, lockout, and disable/enable behavior (User-Account-Control attribute) No other permissions are included.
Computer Objects – Read/Write Manager	View and modify what person is assigned to manage a computer (Managed-By attribute); no other permissions are included.
Computer Objects – Read/Write Personal Information	View and modify properties that describe personal information for computer objects (Personal-Information property set); no other permissions are included. Property set members: See "Personal-Information Property Set" at http://msdn.microsoft.com/en-us/library/ms684394.aspx
Computer Objects – Read/Write Public Information	View and modify properties that describe public information for computer objects (Public-Information property set); no other permissions are included. Property set members: See "Public-Information Property Set" at http://msdn.microsoft.com/en-us/library/ms684396.aspx
Computer Objects - Reset Computer Account	Reset computer accounts; no other permissions are included.
Computer Objects - View BitLocker Recovery Keys	Search for, and view all properties of, computer child objects each of which contains a Full Volume Encryption recovery password with its associated GUID. Use this template to delegate the task of retrieving BitLocker recovery keys that are stored in Active Directory.

Active Directory/Advanced: Contacts

Table 8: Active Directory/Advanced: Contacts

Access Template	Description
Contacts – Create	Create contact objects; no other permissions are included.

Access Template	Description
Contacts – Delete	Delete contact objects; no other permissions are included.
Contacts – Read Group Membership	View a list of groups to which a contact object belongs; no other permissions are included.
Contacts – Read/Write Organizational Information	View and modify properties that describe organizational information for contact objects: • Job title • Department • Company • Employee ID • Manager • Office location No other permissions are included.
Contacts – Read/Write Personal Information	View and modify properties that describe personal information for contact objects (Personal-Information property set); no other permissions are included. Property set members: See "Personal-Information Property Set" at http://msdn.microsoft.com/en-us/library/ms684394.aspx
Contacts – Read/Write Web Information	View and modify properties that describe Web-related information for contact objects (Web-Information property set); no other permissions are included. Property set members: See "Web-Information Property Set" at http://msdn.microsoft.com/en-us/library/ms684418.aspx
Contacts – Rename	Rename contact objects; no other permissions are included.

Active Directory/Advanced: Domains

Table 9: Active Directory/Advanced: Domains

Access Template	Description
Domains – Change PDC	Change the PDC emulator role owner; no other permissions are included.
Domains – Delegate Control and Enforce Active Roles	Apply Active Roles Access Templates and Policy Objects to a domain object; no other permissions are included.

Access Template	Description
Policy	
Domains – Generate Resultant Set of Policy (Logging)	Generate Group Policy Results data for the users/computers within a given domain; no other permissions are included.
Domains – Generate Resultant Set of Policy (Planning)	Generate Group Policy Modeling data for the users/computers within a given domain; no other permissions are included.
Domains – List	List domain objects; no other permissions are included.
Domains – Read/Write General Information	View and modify properties that constitute general information for domain objects: • Domain name (pre-Windows 2000) • Description No other permissions are included.
Domains – Read/Write Manager	View and modify what person is assigned to manage a domain (Managed-By attribute); no other permissions are included.
Domains – Read/Write Other Domain Parameters	View and modify properties that permit control to a list of domain attributes (Domain-Other-Parameters property set); no other permissions are included. Property set members: See "Domain-Other-Parameters Property Set" at http://msdn.microsoft.com/en-us/library/ms684338.aspx
Domains – Read/Write Password & Lockout Policies	View and modify lockout and password age related properties on the domain user accounts (Domain-Password property set); no other permissions are included. Property set members: See "Domain-Password Property Set" at http://msdn.microsoft.com/en-us/library/ms684341.aspx

Active Directory/Advanced: Group Policy Container

Table 10: Active Directory/Advanced: Group Policy Container

Access Template	Description
Group Policy Container –	Extended right used by the Group Policy engine to

Access Template	Description
Apply Group Policy	determine if a GPO applies to a user/computer or not (Apply-Group-Policy extended right); no other permissions are included.

Active Directory/Advanced: Groups

Table 11: Active Directory/Advanced: Groups

Access Template	Description
Groups – Add/Remove Self As Member	Permission to enable updating membership of a group in terms of adding/removing one's own account (Self-Membership validated write); no other permissions are included.
Groups – Copy	Create copies of existing groups; no other permissions are included.
Groups – Create	Create groups; no other permissions are included.
Groups – Delete	Delete groups; no other permissions are included.
Groups - Deprovision	Perform the deprovisioning operation on 'groups' objects; no other permissions are included.
Groups – List	List groups; no other permissions are included.
Groups – Manage Membership Rules	View and modify criteria used by Active Roles for rules-based control of group membership lists; no other permissions are included.
Groups – Read Group Membership	View a list of groups to which a given group belongs; no other permissions are included.
Groups – Read/Write E-mail Address	View and modify the list of email addresses for a group; no other permissions are included.
Groups – Read/Write General Information	View and modify properties that constitute general information for groups: • Group name (pre-Windows 2000) • Description • E-mail • Group scope • Group type • Notes No other permissions are included.

Access Template	Description
Groups – Read/Write Group Members	Add or remove members from a group; no other permissions are included.
Groups – Read/Write Group Type and Scope	View and modify the type and scope settings for a group; no other permissions are included.
Groups – Read/Write Manager	View and modify what person is assigned to manage a given group (Managed-By attribute); no other permissions are included.
Groups – Read/Write Phone and Mail Options	View and modify properties that describe email related information for groups (Email-Information property set); no other permissions are included. Property set members: See "Email-Information Property Set" at http://msdn.microsoft.com/en-us/library/ms684362.aspx
Groups – Rename	Rename groups; no other permissions are included.
Groups - Undo Deprovision	Perform the undo deprovisioning operation on 'group' objects; no other permissions are included.
Groups - Undo Deprovision - Deny	Prohibit the undo deprovisioning operation on 'group' objects; no other permissions are included.

Active Directory/Advanced: Objects

Table 12: Active Directory/Advanced: Objects

Access Template	Description
Objects - Deny Deletion	Deny deletion and sub-tree deletion of a given object; no other permissions are included.
Objects - Deny Deletion of Child Objects	Deny deletion of all child objects from a given container; no other permissions are included.

Active Directory/Advanced: OUs

Table 13: Active Directory/Advanced: OUs

Access Template	Description
OUs – Create	Create Organizational Units; no other permissions are included.

Access Template	Description
OUs – Delegate Control and Enforce Active Roles Policy	Apply Active Roles Access Templates and Policy Objects to an Organizational Unit; no other permissions are included.
OUs – Delete	Delete Organizational Units; no other permissions are included.
OUs – Generate Resultant Set of Policy (Logging)	Generate Group Policy Results data for the users/computers within a given Organizational Unit; no other permissions are included.
OUs – Generate Resultant Set of Policy (Planning)	Generate Group Policy Modeling data for the users/computers within a given Organizational Unit; no other permissions are included.
OUs – List	List Organizational Units; no other permissions are included.
OUs – Read/Write General Information	View and modify properties that constitute general information for Organizational Units: • Description • Street • City • State/province • Zip/Postal Code • Country/region No other permissions are included.
OUs – Read/Write Manager	View and modify what person is assigned to manage a given Organizational Unit (Managed-By attribute); no other permissions are included.
OUs – Rename	Rename Organizational Units; no other permissions are included.

Active Directory/Advanced: Printer Objects

Table 14: Active Directory/Advanced: Printer Objects

Access Template	Description
Printer Objects – Create	Create printer queue objects; no other permissions are included.
Printer Objects – Delete	Delete printer queue objects; no other permissions are included.

Access Template	Description
Printer Objects – List	List printer queue objects; no other permissions are included.
Printer Objects – Read/Write General Information	View and modify properties that constitute general information for printer queue objects: • Location • Model • Description • Color • Staple • Double-sided • Printing speed • Maximum resolution
Printer Objects – Read/Write Manager	View or modify what person is assigned to manage a given printer (Managed-By attribute); no other permissions are included.
Printer Objects – Rename	Rename printer queue objects; no other permissions are included.

Active Directory/Advanced: Shared Folders

Table 15: Active Directory/Advanced: Shared Folders

Access Template	Description
Shared Folders – Create	Create shared folder objects; no other permissions are included.
Shared Folders – Delete	Delete shared folder objects; no other permissions are included.
Shared Folders – List	List shared folder objects; no other permissions are included.
Shared Folders – Read/Write General Information	View and modify properties that constitute general information for shared folder objects: • Description • UNC name No other permissions are included.
Shared Folders – Read/Write	View and modify what person is assigned to manage a

Access Template	Description
Manager	given shared resource (Managed-By attribute); no other permissions are included.
Shared Folders – Rename	Rename shared folder objects; no other permissions are included.

Active Directory/Advanced: Users

Table 16: Active Directory/Advanced: Users

Access Template	Description
Users - Assign/Remove Digital Certificates	Assign or remove digital (X.509) certificates from the user in Active Directory (read/write the userCertificate attribute of user objects); no other permissions are included.
Users - Change Password (Extended Right)	Change password on user object (User-Change-Password extended right); no other permissions are included.
Users - Copy	Create copies of existing user objects; no other permissions are included.
Users - Create	Create user objects; no other permissions are included.
Users - Delete	Delete user objects; no other permissions are included.
Users - Deprovision	Perform the deprovisioning operation on user objects; no other permissions are included.
Users - Undo Deprovision	Perform the undo deprovisioning operation on user objects; no other permissions are included.
Users - Undo Deprovision - Deny	Prohibit the undo deprovisioning operation on user objects; no other permissions are included.
Users - Enable/Disable Account	Enable or disable user objects; no other permissions are included.
Users - List	List user objects; no other permissions are included.
Users - Read Group Membership	View a list of groups to which a given user belongs; no other permissions are included.
Users - Read/Write Logon Information	View and modify properties that describe logon information for user objects (User-Logon property set); no other permissions are included. Property set members: See "User-Logon Property Set" at http://msdn.microsoft.com/en-us/library/ms684415.aspx

Access Template	Description
Users - Read/Write Account Information	View or modify properties that describe account information for user objects (no other permissions are included): • 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	View and modify properties that describe account restrictions for user objects (User-Account-Restrictions property set); no other permissions are included. Property set members: See "User-Account-Restrictions Property Set" at http://msdn.microsoft.com/en-us/library/ms684412.aspx
Users - Read/Write Dial-In Properties	View and modify properties that describe dial-in related information for user objects (no other permissions are included): • 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	View and modify properties that constitute general information for user objects (General-Information property set); no other permissions are included. Property set members: See "General-Information Property Set" at http://msdn.microsoft.com/en-us/library/ms684366.aspx
Users - Read/Write Personal Information	View and modify properties that describe personal information for user objects (Personal-Information property set); no other permissions are included. Property set members: See "Personal-Information Property Set" at http://msdn.microsoft.com/en-us/library/ms684394.aspx

Access Template	Description
Users - Read/Write Organizational Information	View and modify properties that describe organization related information for user objects (no other permissions are included): • Title • Department • Company • Manager • Direct reports • Office (General tab)
Users - Read/Write Phone and Mail Options	View and modify properties that describe email related information for user objects (Email-Information property set); no other permissions are included. Property set members: See "Email-Information Property Set" at http://msdn.microsoft.com/en-us/library/ms684362.aspx
Users - Read/Write Profile Properties	View and modify properties that describe profile related information for user objects (no other permissions are included): • User profile • Home folder
Users - Read/Write Public Information	View and modify properties that describe public information for user objects (Public-Information property set); no other permissions are included. Property set members: See "Public-Information Property Set" at http://msdn.microsoft.com/en-us/library/ms684396.aspx
Users - Read/Write Web Information	View and modify properties that describe Web-related information for user objects (Web-Information property set); no other permissions are included. Property set members: See "Web-Information Property Set" at http://msdn.microsoft.com/en-us/library/ms684418.aspx
Users - Read/Write WTS Properties	View and modify properties that describe Terminal Services related information for user objects (no other permissions are included): • Terminal Services User Profile • Terminal Services Home Folder

Access Template	Description
	• Allow logon to terminal server • Starting program • Client devices • Terminal Service timeout and reconnection settings
Users - Rename	Rename user objects; no other permissions are included.
Users - Reset Password (Extended Right)	Reset password on user object (User-Reset-Password extended right); no other permissions are included.
Users - Run Check Policy (Extended Right)	Use the 'Check Policy' command; no other permissions are included.
Users - Unlock Account	Unlock user objects that get locked due to a number of failed logon attempts; no other permissions are included.
Users - Write Password	Set password on user object; no other permissions are included.
Users - View Change History (Extended Right)	Use the 'Change History' and 'User Activity' commands; no other permissions are included.
Users - View Delegated Rights (Extended Right)	Use the 'Delegated Rights' command; no other permissions are included.
Users - View Digital Certificates	View digital (X.509) certificates assigned to the user in Active Directory (read the userCertificate attribute of user objects); no other permissions are included.
Users - View Entitlement Profile (Extended Right)	Use the 'Entitlement Profile' command, to view resources to which a given user is entitled. No other permissions are included.

Azure

Use the Access Templates of this category to delegate management tasks for searching, reading, creating, updating or deleting Azure AD resources, such as Azure tenants, users, guest users, groups, and so on.

Table 17: Azure Access Templates

Access Template	Description
Azure - Configuration Administrator	Gives permission to perform the following tasks: • Read and write Azure tenants. • Read and write Azure applications.

Access Template	Description
	• Read Azure health check reports. • Read Azure license reports. • Read Azure roles reports.
Azure - Contact Full Control	Gives permission to perform the following tasks: • Add and enable new Azure contacts. • View existing Azure contacts. • Update the properties of existing Azure contacts.
Azure - Full Control	Gives permission to perform the following tasks: • Read and write Azure configuration objects. • Read and write Azure user attributes. • Read and write Azure group attributes. • Read and write Azure O365 group objects.
Azure - Group Full Control	Gives permission to perform the following tasks: • 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	Gives access to the Azure health check, O365 roles and license reports. NOTE: This Access Template must be applied on a **Configuration** container.
Azure - O365 Groups Full Control	Gives permission to perform the following tasks: • Add and enable new Azure O365 groups. • View existing Azure O365 groups. • Update the properties of existing Azure O365 groups.
Azure - Read All Attributes	Gives permission to read all Azure attributes.
Azure - Read All Contact Attributes	Gives permission to read all Azure contact attributes.
Azure - Read All Group Attributes	Gives permission to list all Azure groups and view all Azure group properties.
Azure - Read All O365 Group Attributes	Gives permission to list all Azure O365 groups and view all Azure O365 group properties.

Access Template	Description
Azure - Read All User Attributes	Gives permission to read all Azure user and guest user attributes.
Azure - User Full Control	Gives permission to perform the following tasks: • 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	Gives permission to create Azure cloud contact accounts.
Azure Cloud Contact - Delete Objects	Gives permission to delete Azure cloud contact accounts.
Azure Cloud Contact - Full Control	Gives permission to create new Azure cloud contact accounts, and perform all administrative operations on existing Azure cloud contact accounts.
Azure Cloud Contact - Modify Objects	Gives permission to modify Azure cloud contact accounts.
Azure Cloud Contact - Read All Attributes	Gives permission to read all Azure cloud contact attributes.
Azure Cloud User - Create Objects	Gives permission to create Azure cloud user accounts.
Azure Cloud User - Delete Objects	Gives permission to delete Azure cloud user accounts.
Azure Cloud User - Full Control	Gives permission to create new Azure cloud user accounts, and perform all administrative operations on existing Azure cloud user accounts.
Azure Cloud User - Modify Objects	Gives permission to modify Azure cloud user accounts.
Azure Cloud User - Read All Attributes	Gives permission to read all Azure cloud user attributes.
Azure Create O365 Groups	Gives permission to create O365 groups.
Azure Guest User - Create Objects	Gives permission to create Azure guest user accounts.
Azure Guest User - Delete Objects	Gives permission to delete Azure guest user accounts.
Azure Guest User - Full Control	Gives permission to create new Azure guest user accounts, and perform all administrative operations on existing Azure guest user accounts.

Access Template	Description
Azure Guest User - Modify Objects	Gives permission to modify Azure guest user accounts.
Azure Guest User - Read All Attributes	Gives permission to read all Azure guest user attributes.
Azure Health Check Report	Gives permission to access Azure health check reports. NOTE: This Access Template must be applied on a **Configuration** container.
Azure License Report	Gives permission to access Azure license reports. NOTE: This Access Template must be applied on a **Configuration** container.
Azure Modify O365 Group Members	Gives permission to modify O365 groups.
Azure O365 Roles Report	Gives permission to access O365 roles reports. NOTE: This Access Template must be applied on a **Configuration** container.
Azure Resource Mailboxes - Create Objects	Gives permission to create Azure resource mailboxes.
Azure Resource Mailboxes - Delete Objects	Gives permission to delete Azure resource mailboxes.
Azure Resource Mailboxes - Full Control	Gives permission to perform the following tasks: • Add and enable new Azure resource mailboxes. • View existing Azure resource mailboxes. • Update the properties of existing Azure resource mailboxes.
Azure Resource Mailboxes - Modify Objects	Gives permission to list all Azure resource mailboxes and modify their properties.
Azure Resource Mailboxes - Read All Attributes	Gives permission to list all Azure resource mailboxes and view their properties.
Azure Security Group - Create Objects	Gives permission to create Azure security groups.
Azure Security Group - Delete Objects	Gives permission to delete Azure security groups.
Azure Security Group - Full Control	Gives permission to perform the following tasks: • Add and enable new Azure security groups.

Access Template	Description
	• View existing Azure security groups. • Update the properties of existing Azure security groups.
Azure Security Group - Modify Members	Gives permission to modify the members of Azure security groups.
Azure Security Group - Modify Objects	Gives permission to list all Azure security groups and modify their properties.
Azure Security Group - Read All Attributes	Gives permission to list all Azure security groups and read their properties.

The **Azure** > **Miscellaneous** sub-node contains one additional Azure Access Template.

Table 18: Azure > Miscellaneous Access Templates

Access Template	Description
Azure Health Check Access	Gives read permission to the Azure Health Check service to 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.

AD LDS (ADAM) Data Management

You can use Access Templates in this category to delegate management tasks on the content that is stored in Microsoft Active Directory Lightweight Directory Services (AD LDS) - an independent mode of Active Directory formerly known as Active Directory Application Mode (ADAM). The data management tasks include managing user accounts (users), groups, and container objects.

Table 19: AD LDS (ADAM) Data Management

Access Template	Description
All AD LDS Objects - Full Control	Perform any management task on any object in Active Directory Lightweight Directory Services.
All AD LDS Objects - Read All Properties	List all directory objects and view all properties of any object in Active Directory Lightweight Directory Services.
AD LDS Users - Full Control	Create new AD LDS user accounts; perform all

Access Template	Description
	management tasks on existing AD LDS user accounts.
AD LDS Users - Modify All Properties	List AD LDS user accounts; view and modify all properties of AD LDS user accounts.
AD LDS Users - Read All Properties	List AD LDS user accounts; view all properties of AD LDS user accounts.
AD LDS Groups - Add/Remove Members	List AD LDS groups; view and modify membership lists of AD LDS groups.
AD LDS Groups - Full Control	Create new AD LDS groups; perform all management tasks on existing AD LDS groups.
AD LDS Groups - Modify All Properties	List AD LDS groups; view and modify all properties of AD LDS groups.
AD LDS Groups - Read All Properties	List AD LDS groups; view all properties of AD LDS groups.
AD LDS Containers - Full Control	Create new AD LDS container objects; perform all administrative operations on existing AD LDS container objects.
AD LDS Containers - Modify All Properties	List AD LDS container objects; view and modify all properties of AD LDS container objects.
AD LDS Containers - Read All Properties	List AD LDS container objects; view all properties of AD LDS container objects.
AD LDS OUs - Full Control	Create new AD LDS organizational units; perform all management tasks on existing AD LDS organizational units.
AD LDS OUs - Modify All Properties	List AD LDS organizational units; view and modify all properties of AD LDS organizational units.
AD LDS OUs - Read All Properties	List AD LDS organizational units; view all properties of AD LDS organizational units.

Computer Resources

Table 20: Computer Resources

Access Template	Description
Computer Management - Full Control	Perform all management tasks on any computer resource; list and select computers.
Computer Management -	Create, modify, and delete local user accounts and groups

Access Template	Description
Local Account Operator	on a computer; list and select computers.
Computer Management - Network Share Operator	Create, modify, and delete network shares on a computer; list and select computers.
Computer Management - Print Operator	View and modify properties of logical printers installed on a computer; list and select computers.
Computer Management - Read-Only Access	View properties of all computer resources; list and select computers.
Computer Management - Server Operator	Start/stop services, pause/resume/cancel printing, and create, modify and 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	Perform all management tasks on services on a computer; list and select computers.

Computer Resources/Advanced

Table 21: Computer Resources/Advanced

Access Template	Description
Local Groups - Add/Remove Members	Add or remove members from groups on a computer; no other permissions are included.
Local Groups - Create	Create groups on a computer; no other permissions are included.
Local Groups - Delete	Delete groups on a computer; no other permissions are included.
Local Groups - List	List groups stored locally on a computer; no other permissions are included.
Local Groups - Read/Write General Information	View and modify descriptions and membership lists of the groups stored locally on a computer; no other permissions are included.
Local Groups - Rename	Rename groups stored locally on a computer; no other permissions are included.
Local Users - Create	Create user accounts on a computer; no other permissions are included.
Local Users - Delete	Delete user accounts on a computer; no other permissions are included.

Access Template	Description
Local Users - List	List user accounts stored locally on a computer; no other permissions are included.
Local Users - Read Group Membership	View a list of groups to which the user account belongs; no other permissions are included.
Local Users - Read/Write Account Options	View and modify user account options such as the password options, 'Account is disabled' and 'Account is locked out'; no other permissions are included.
Local Users - Read/Write General Information	View and modify full names and descriptions of the user accounts stored locally on a computer; no other permissions are included.
Local Users - Read/Write Profile Properties	View and modify user profile and home folder settings for the user accounts stored locally on a computer; no other permissions are included.
Local Users - Rename	Rename user accounts stored locally on a computer; no other permissions are included.
Local Users - Write Password	Change passwords for the user accounts stored locally on a computer; no other permissions are included.
Printer Resources - Read/Write Advanced Information	View and modify information on the Ports and Advanced tabs in the Properties dialog box for logical printers; no other permissions are included.
Printer Resources - Read/Write General Information	View and modify Name, Location, and Comment for logical printers; no other permissions are included.
Printer Resources - Read/Write Sharing Information	View and modify the Not Shared and Shared As options for logical printers; no other permissions are included.
Services - List	List services defined on a computer; no other permissions are included.
Services - Read/Write General Information	View and modify Name, Display Name, Description, Path to Executable, and Startup Type for services; no other permissions are included.
Services - Read/Write Log On Information	View and modify the Log On As options for services; no other permissions are included.
Services - Read/Write Start type	View and modify Startup Type for services; no other permissions are included.
Services - Start /Stop/ Pause/ Resume	Start, stop, pause, and resume services; no other permissions are included.

Access Template	Description
Shares - Create	Create network shares on a computer; no other permissions are included.
Shares - List	List network shares defined on a computer; no other permissions are included.
Shares - Read/Write General Information	View and modify Share Name, Path, Comment, and User Limit for network shares; no other permissions are included.
Shares - Read/Write Permissions	View and modify share permissions on network shares; no other permissions are included.
Shares - Stop Sharing	Stop sharing folders on a computer; no other permissions are included.

Configuration

Table 22: Configuration

Access Template	Description
Access Rules - Full Control	Use this Access Template to enable delegated administrators to create, view, modify and delete Access Rule objects. Apply this Access Template to containers that hold Access Rule objects.
Access Rules - Modify	Use this Access Template to enable delegated administrators to view and modify all properties of existing Access Rule objects. Apply this Access Template to individual Access Rule objects or containers that hold Access Rule objects.
Access Rules - View	Use this Access Template to enable delegated administrators to view all properties of existing Access Rule objects. Apply this Access Template to individual Access Rule objects or containers that hold Access Rule objects.
Automation Workflow - Full Control	Use this Access Template to give delegated administrators full control of automation workflow definitions, including the ability to view and modify workflow definitions, start automation workflow, and view run history. Apply this Access Template to automation workflow definition objects or containers that hold automation workflow definition objects.
Automation Workflow - View	Use this Access Template to enable delegated

Access Template	Description
	administrators to view automation workflow definitions and run history. Apply this Access Template to automation workflow definition objects or containers that hold automation workflow definition objects.
Automation Workflow - View and Run	Use this Access Template to enable delegated administrators to view automation workflow definitions, start automation workflow, and view run history. Apply this Access Template to automation workflow definition objects or containers that hold automation workflow definition objects.
Configuration - Add/Remove Managed Domains	Register domains with Active Roles; view/modify registration information for managed domains.
Configuration - Manage Access Templates	Create, modify, and delete Access Templates and Access Template containers; add/remove permissions from Access Templates; list Access Templates and Access Template containers.
Configuration - Manage Configuration	View or change any configuration settings of Active Roles, except for the settings specific to Active Roles replication.
Configuration - Manage Policy Objects	Create, modify, and delete Active Roles Policy Objects and Policy Object containers; configure Active Roles policies; list Policy Objects and Policy Object containers.
Configuration - Manage Script Modules	Create, modify, and delete Active Roles Script Modules and Script Module containers; list Script Modules and Script Module containers.
Configuration - View Configuration	View any configuration settings of Active Roles, including the settings specific to Active Roles replication.
Managed Object Statistics - View Report	Use this Access Template to allow read access to statistical reports of the number of objects managed by the product (product usage statistics).
Managed Object Statistics - Read Detailed Data	Use this Access Template to allow read access to detailed statistical information about the number of objects managed by the product.
Workflow - View Workflow Containers	Use this Access Template to enable delegated administrators to view containers that hold workflow definition objects. Apply this Access Template to the Policies/Workflow node in the console tree.

Configuration/Advanced

Table 23: Configuration/Advanced

Access Template	Description
Access Templates - Copy	Create copies of Access Templates; no other permissions are included.
Access Templates - Create	Create Access Templates; no other permissions are included.
Access Templates - Delete	Delete Access Templates; no other permissions are included.
Access Templates - List	List Access Templates; no other permissions are included.
Access Templates - Read/Write Permissions	View and modify permission entries in Access Templates; no other permissions are included.
Access Templates - Rename	Rename Access Templates; no other permissions are included.
Policy Objects - Copy	Create copies of Active Roles Policy Objects; no other permissions are included.
Policy Objects - Create	Create Active Roles Policy Objects; no other permissions are included.
Policy Objects - Delete	Delete Active Roles Policy Objects; no other permissions are included.
Policy Objects - List	List Active Roles Policy Objects; no other permissions are included.
Policy Objects - Read/Write Policy Entries	View and modify policy definitions in Active Roles Policy Objects (Policy Object entries); no other permissions are included.
Policy Objects - Rename	Rename Active Roles Policy Objects; no other permissions are included.
Script Modules - Copy	Create copies of Active Roles Script Modules; no other permissions are included.
Script Modules - Create	Create Active Roles Script Modules; no other permissions are included.
Script Modules - Delete	Delete Active Roles Script Modules; no other permissions are included.
Script Modules - List	List Active Roles Script Modules; no other permissions are included.
Script Modules - Read/Write	View and modify scripts stored in Active Roles Script

Access Template	Description
Script Text	Modules; no other permissions are included.
Script Modules - Rename	Rename Active Roles Script Modules; no other permissions are included.

Exchange

Table 24: Exchange

Access Template	Description
Exchange - Recipients Full Control	Perform all Exchange recipient management tasks; view or change all properties of Exchange recipients. View all properties of users, groups and contacts; list contents of container; list containers.
Exchange - Perform Exchange Tasks	Create mailboxes of any type; use Exchange Task Wizard to manage Exchange recipients. View all properties of users, groups and contacts; list contents of container; list containers.
Exchange - Manage Resource, Linked and Shared Mailboxes	Create and administer room, equipment, linked and shared mailboxes. View all properties of users; list contents of container; list containers.
Exchange - Configure Exchange General Settings	View or change the Exchange recipient settings from the Exchange General page. View all properties of users, groups and contacts; list contents of container; list containers.
Exchange - Configure E-mail Addresses	View or change the Exchange recipient settings from the E-mail Addresses page. View all properties of users, groups and contacts; list contents of container; list containers.
Exchange - Configure Mail Flow Settings	View or change the Exchange recipient settings from the Mail Flow Settings page. View all properties of users, groups and contacts; list contents of container; list containers.
Exchange - Configure Mailbox Settings	View or change the Exchange recipient settings from the Mailbox Settings page. View all properties of users; list contents of container; list containers.
Exchange - Configure Mailbox Features	View or change the Exchange recipient settings from the Mailbox Features page. View all properties of users; list contents of container; list containers.

Access Template	Description
Exchange - Configure Calendar Settings	View or change the Exchange recipient settings form the Calendar Settings page. View all properties of users; list contents of container; list containers.
Exchange - Configure Resource General Settings	View or change the Exchange recipient settings from the Resource General page. View all properties of users; list contents of container; list containers.
Exchange - Configure Resource Information Settings	View or change the Exchange recipient settings from the Resource Information page. View all properties of users; list contents of container; list containers.
Exchange - Configure Resource Policy	View or change the Exchange recipient settings from the Resource Policy page. View all properties of users; list contents of container; list containers.
Exchange - Configure Resource In-Policy Requests	View or change the Exchange recipient settings from the Resource In-Policy Requests page. View all properties of users; list contents of container; list containers.
Exchange - Configure Resource Out-of-Policy Requests	View or change the Exchange recipient settings from the Resource Out-of-Policy Requests page. View all properties of users; list contents of container; list containers.
Exchange - Configure Exchange Advanced Settings	View or change the Exchange recipient settings from the Exchange Advanced page. View all properties of users, groups and contacts; list contents of container; list containers.

Exchange/Advanced

Table 25: Exchange/Advanced

Access Template	Description
Exchange - Read/Write Delivery Options	View or change delivery options for Exchange recipients, on the Mail Flow Settings page.
Exchange - Read/Write Message Size Restrictions	View or change message size restrictions for Exchange recipients, on the Mail Flow Settings page.
Exchange - Read/Write Message Delivery Restrictions	View or change message delivery restrictions for Exchange recipients, on the Mail Flow Settings page.
Exchange - Read/Write Message Moderation	View or change the message moderation settings for Exchange distribution groups, on the Mail Flow Settings page.

Access Template	Description
Exchange - Read/Write Messaging Records Management	View or change the messaging records management settings for Exchange mailboxes, on the Mailbox Settings page.
Exchange - Read/Write Storage Quotas	View or change storage quotas for Exchange mailboxes, on the Mailbox Settings page.
Exchange - Read/Write Archive Quota	View or change archive quota for Exchange mailboxes, on the Mailbox Settings page.
Exchange - Read/Write Sharing	View or change the sharing settings for Exchange mailboxes, on the Mailbox Settings page.
Exchange - Read/Write Role Assignment Policy	View or change role assignment policy for Exchange mailboxes, on the Mailbox Settings page.
Exchange - Read/Write Address Book Policy	View or change address book policy for Exchange mailboxes, on the Mailbox Settings page.
Exchange - Read/Write Outlook Mobile Access	View or change the Outlook Mobile Access feature settings for Exchange mailboxes, on the Mailbox Features page.
Exchange - Read/Write Exchange ActiveSync	View or change the Exchange ActiveSync feature settings for Exchange mailboxes, on the Mailbox Features page.
Exchange - Read/Write Unified Messaging	View or change the Unified Messaging feature settings for Exchange mailboxes, on the Mailbox Features page.
Exchange - Read/Write Up-to-date Notifications	View or change the Up-to-date Notifications feature settings for Exchange mailboxes, on the Mailbox Features page.
Exchange - Read/Write IMAP4	View or change the IMAP4 feature settings for Exchange mailboxes, on the Mailbox Features page.
Exchange - Read/Write POP3	View or change the POP3 feature settings for Exchange mailboxes, on the Mailbox Features page.
Exchange - Read/Write Outlook Web App	View or change the Outlook Web App feature settings for Exchange mailboxes, on the Mailbox Features page.
Exchange - Read/Write MAPI	View or change the MAPI feature settings for Exchange mailboxes, on the Mailbox Features page.
Exchange - Read/Write Archive	View or change the Archive feature settings for Exchange mailboxes, on the Mailbox Features page.
Exchange - Enable Archive	Enable archive for Exchange mailboxes.
Exchange - Enable Unified Messaging	Enable Exchange mailboxes for Unified Messaging.
Exchange - Create	Create equipment mailboxes associated with new or

Access Template	Description
Equipment Mailboxes	existing user accounts.
Exchange - Create Linked Mailboxes	Create linked mailboxes associated with new or existing user accounts.
Exchange - Create Room Mailboxes	Create room mailboxes associated with new or existing user accounts.
Exchange - Create Shared Mailboxes	Create shared mailboxes associated with new or existing user accounts.
Exchange - Create User Mailboxes	Create user mailboxes associated with new or existing user accounts.
Exchange - Delete Recipient's E-mail Address	Delete email addresses.
Exchange - Delete User Mailbox	Delete user mailboxes.
Exchange - Designate Contact as Mail-Enabled	Designate contacts as mail-enabled recipients.
Exchange - Designate Group as Mail-Enabled	Designate group as mail-enabled recipients.
Exchange - Designate User as Mail-Enabled	Designate users as mail-enabled recipients.
Exchange - Move Mailbox	Move Exchange mailboxes.
Exchange - Read/Write Advanced Properties for Mailbox-Enabled Users	View or change advanced Exchange properties for mailbox-enabled users.
Exchange - Read/Write Advanced Properties for Mail-Enabled Groups	View or change advanced Exchange properties on mail-enabled groups.
Exchange - Read/Write Advanced Properties for Mail-Enabled Users and Contacts	View or change advanced Exchange properties for mail-enabled users and contacts.
Exchange - Read/Write Autoreply Settings	View or change Automatic Replies settings for the mailbox.
Exchange - Read/Write Custom Attributes	View or change custom Exchange attributes.
Exchange - Read/Write Deleted Item Retention	View or change the Deleted Item Retention Period setting.

Access Template	Description
Period	
Exchange - Read/Write Forwarding Address	View or change the Forwarding Address setting.
Exchange - Read/Write ILS Settings	View or change ILS settings.
Exchange - Read/Write Mailbox Rights	View or change mailbox security settings.
Exchange - Read/Write Mailbox Storage Limits	View or change mailbox storage limits.
Exchange - Read/Write Maximum Size of Incoming Messages	View or change Maximum Size of Incoming Messages settings.
Exchange - Read/Write Maximum Size of Outgoing Messages	View or change Maximum Size of Outgoing Messages settings.
Exchange - Read/Write Message Restrictions	View or change Message Restrictions settings.
Exchange - Read/Write Protocol Settings	View or change Protocol Settings options.
Exchange - Read/Write Recipient Limits	View or change Recipient Limits settings.
Exchange - Read/Write Send on Behalf Permission	View or change Send on Behalf Permission settings.
Exchange - Read ERFM Attributes	Read the ERFM-related attributes of master accounts, required for the delegated administrator to use the Exchange Resource Forest Management (ERFM) solution. NOTE: You don't need to apply this Access Template in conjunction with the general-purpose Access Templates for delegating Exchange recipient management tasks, as those Access Templates already provide all the required permissions to read the ERFM-related attributes of master accounts.
Exchange - Convert User Mailbox to Linked Mailbox	Perform mailbox conversion from user mailbox type to linked mailbox type.
Exchange - Convert Linked Mailbox to User Mailbox	Perform mailbox conversion from linked mailbox type to user mailbox type.

Skype for Business Server

These Access Templates require Skype for Business Server user management policies to be applied, as described in the Skype for Business Server User Management Administration Guide for Active Roles 7.5.2.

Table 26: Skype for Business Server

Access Template	Description
Skype for Business Server - User Full Control	Gives permission to perform the following tasks by using Active Roles: • Add and enable new Skype for Business Server users • View existing Skype for Business Server users • View or change the SIP address • View or change the telephony option and related settings • View or change the user policy assignments in Skype for Business Server • Temporarily disable or re-enable users for Skype for Business Server • Move users to another server or pool in Skype for Business Server • Remove users from Skype for Business Server
Skype for Business Server - User Telephony	Gives permission to perform the following tasks by using Active Roles: • View existing Skype for Business Server users • View the SIP address • View or change the telephony option and related settings • View the user policy assignments in Skype for Business Server
Skype for Business Server - User Disable/Re-enable	Gives permission to perform the following tasks by using Active Roles: • View existing Skype for Business Server users • View the SIP address • View the telephony option and related settings • View the user policy assignments in Skype for Business Server

Access Template	Description
	Temporarily disable or re-enable users for Skype for Business Server
Skype for Business Server - User Policies	Gives permission to perform the following tasks by using Active Roles: • View existing Skype for Business Server users • View the SIP address • View the telephony option and related settings • View or change the user policy assignments in Skype for Business Server

Starling

Table 27: Starling

Access Template	Description
Starling -Two Factor Authentication User	Gives minimal read permission required to enable Two-Factor Authentication for a user.

User Interfaces

Table 28: User Interfaces

Access Template	Description
User Interface Management-MMC Full control	Gives permission for the user to log in to the MMC interface.

User Self-management

Table 29: User Self-management

Access Template	Description
Self - Account Management	Authorize users to view or change their own profile information by using the Web Interface. When applying this template, select the **Self** built-in account as the

Access Template	Description
	trustee.
Self - Group Management	Authorize users to view or change the groups they are responsible for. When applying this template, select the **Primary Owner (Managed By)** or **Secondary Owners** built-in account as the trustee. Note that applying only this template does not give group owners the right to view the lists of group members. The group owners should also be given Read access to the group member objects. This could be accomplished by applying the **All Objects - Read All Properties** template to a scope containing those objects, with the **Authenticated Users** built-in account selected as the trustee.
Self - Group Membership Management	Authorize users to add or remove their own accounts from groups. Apply this template to a scope containing the groups, with the rights assigned to the appropriate user accounts. It is advisable to add the user accounts to a certain group, and then select that group as the trustee when applying the template. In addition to this template, the **Self - Account Management** template should be applied in order to allow the users to view the groups in which they have memberships (the **Member Of** list). The **Self - Account Management** template should be applied to a scope containing the user accounts, with the rights assigned to the **Self** built-in account (select **Self** as the trustee when applying the template).
Self - Group Membership Approval Setting	Authorize users to view or change the properties of the group that determine whether changes to the group members list require approval from the owner of the group.

About us

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

Contacting us

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

Technical support resources

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

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

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