One Identity Active Roles 7.2

What's New Guide

Legend

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

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

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

Active Roles What's New Guide
Updated - October 2017
Version - 7.2

Contents

Summary

Active Roles simplifies and streamlines creation and ongoing management of user accounts, groups, and contacts in Windows Active Directory (AD) and Azure Active Directory environments.

Active roles automates:

- Creating user, groups, and contacts in Active Directory and Azure AD
- Creating mailboxes on Exchange Server and assigning licenses in Office 365
- Managing on-premise Exchange and Exchange Online properties

It provides strictly enforced security, rich capabilities for automating directory management tasks, change approval and easy-to-use Web interfaces, to achieve practical user and group account management for the Windows enterprise.

Active Roles also facilitates administration and provisioning for Active Directory, Exchange, and Azure Active Directory (Azure AD) in a hybrid environment.

1

Key new features

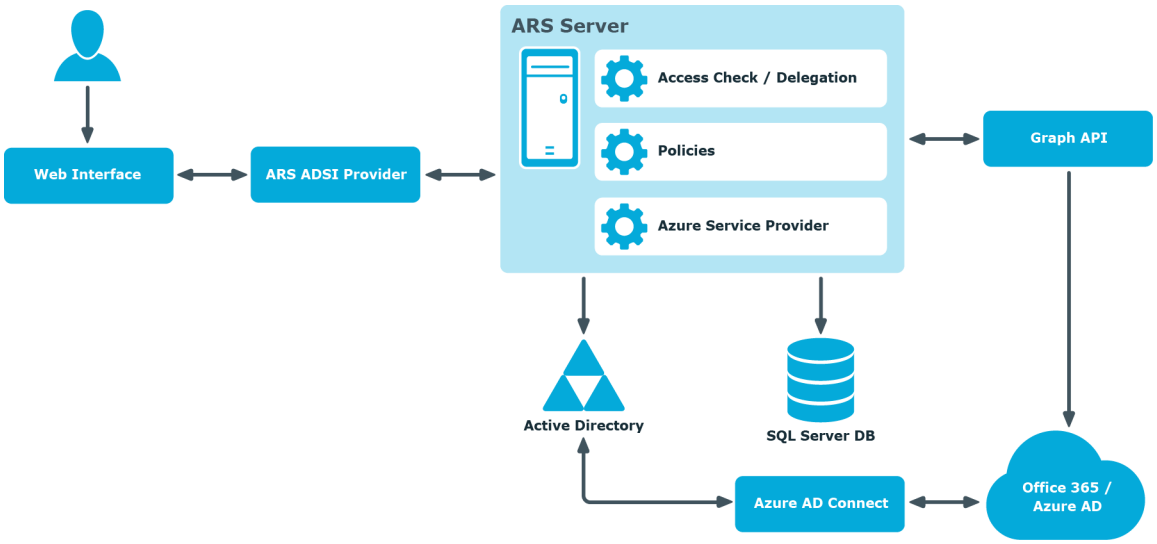
The new release of Active Roles extends and enhances the capabilities of the product to support management of Microsoft Azure Active Directory in a Hybrid mode. This feature now enables Active Roles to synchronize the on-premises Active Directory objects to the Azure Active Directory (Azure AD).

Active Roles 7.2 includes the following features:

- Re-branding Active Roles product and documentation to One Identity brand.
- Enhancements for Active Roles Configuration for Hybrid Environment
- Azure AD /Office 365 Object Management in Hybrid Environment
- Office 365 License Management for hybrid users
- Support for managing Skype for business through Active Roles.
- Active Roles in-place upgrade enhancements.
- Management of Azure AD Contacts.
- Management of Azure AD Distribution groups.
- Enhancements to Azure Active Directory and Office 365 functionality:
    - Azure License Reporting
    - Visual indicator for Azure configuration status
    - Granular license customization
    - Support for synchronized identity environments
    - Azure Application permissions enhancements
    - Support for creating users, groups, and contacts in Azure/Office 365 through SPML

This What's New document elaborates on the features listed above. For detailed information about these features, see the Active Roles Active Roles Azure Administrator's Guide.

The following illustration shows the work-flow for management of hybrid environment using Active Roles.



Active Roles Configuration for Hybrid Environment

When a user signs up for a Microsoft cloud service such as Azure Active Directory, details about the user's organization and the organization's Internet domain name registration are provided to Microsoft. This information is then used to create a new Azure AD instance for the organization. The same directory is used to authenticate sign in attempts when you subscribe to multiple Microsoft cloud services.

The Azure AD instance of the organization, also called the Azure AD tenant, stores the users, groups, applications, and other information pertaining to an organization and its security. To access the Azure AD tenant, we need an application that is registered with the tenant. Active Roles uses this application, also called the Azure AD application, to communicate with the Azure AD tenant after providing the required consent.

The Active Roles 7.2 Web Interface and Management Shell can be used to perform the Azure AD configuration tasks. The new feature in Active Roles enables you to add or modify existing tenants and applications to the management scope through the web interface and Management Shell.

Note: For more information on the Azure Active Directory Management and configuration tasks, see the *Active Roles 7.2 Azure Active Directory and Office 365 Administrator Guide*.

Azure AD /Office 365 Object Management in Hybrid Environment

Active Roles 7.2 supports the following Azure AD/Office 365 management tasks on an on-premises Active Directory container which are synchronized with the Azure Active Directory in Hybrid environment:

Office 365 License Management for hybrid users

Active Roles 7.2 provides the facility to assign or modify the Microsoft Office 365 licenses assigned to on-premises users synchronized to Office 365. You can perform the following Office 365 license management tasks for hybrid users:

- Assign Office 365 licenses to new hybrid users
- Assign Office 365 licenses to existing hybrid users
- Modify or remove Office 365 licenses assigned to hybrid users

NOTE: When a user is de-provisioned or deleted, all the licenses that were assigned to the user are removed and can be assigned to other hybrid users.

On performing an undo-deprovision operation on a hybrid user, the license assignment gets restored to the user on successful completion of the operation.

NOTE: For more information on the Office 365 license management see the *Active Roles 7.2 Azure Active Directory and Office 365 Administrator Guide*.

Support for Microsoft Windows Server 2016

Active Roles 7.2 supports the following:

- Installation on Microsoft Windows Server 2016
- Management of Microsoft Windows Server 2016 servers
- Management of domain controllers hosted on Microsoft Windows Server 2016 servers

Support for Microsoft SQL Server 2016

Active Roles 7.2 supports hosting the database on Microsoft SQL Server 2016. Active Roles 7.2 Administrator Service can be configured by hosting the Active Roles Database in SQL 2016 Database.

Support for Contacts and Distribution Groups

The Active Roles web interface enables you to:

- Management of Office 365 contacts including CRUD, Add or Remove members to groups, and view change history.
- Support for Distribution group including CRUD and Add or Remove Members to groups
- Management of Distribution groups – Assign/Remove Owner

Support for Exchange Online

Active Roles 7.2 supports identity management for Exchange Online:

- Setting Exchange Online properties
- Delegation of Mailbox (Send as)
- Enable/Disable Mailbox Features (For example, POP3, IMAP, Archiving)
- Mailbox Settings (Message size restriction)
- Manage permissions for recipients "Send As" and "Send on Behalf"
- Support for "Email Addresses" all the email addresses (proxy addresses) for the recipient, including the primary SMTP address.
- Message Size Restrictions
- Delivery Options
- Enable or disable POP3, IMAP, MAPI, Outlook Web App or Exchange ActiveSync for a mailbox in Office 365

Support for Skype for Business

Active Roles 7.2 supports identity management for Skype for Business for all the operations that were performed using earlier versions of Lync Server.

Active Roles In-place upgrade improvements

Active Roles 7.2 offers the following in-place upgrade enhancements:

- The in-place upgrade of Active Roles 7.2 upgrades the Active Roles 7.2 Administration service and Web interface components.

Enhancements to Azure AD and Office 365 functionality

Active Roles 7.2 provides the following enhancements for Enhancements to Azure Active Directory and Office 365 functionality:

- Azure License Reporting - Azure Licenses Report displays the Office 365 licenses that are available and assigned to a user.
- Visual indicator for Azure configuration status - Azure Health Check page informs you about the Active Roles to Azure AD connectivity status, and the Active Roles Azure AD tenant and application heath status.
- Granular license customization - License management can be performed through provisioning policy. For Example I want to assign Exchange Online license to all the newly created users automatically so that when a new user is created a mailbox should be provisioned for him Also users will be able to set particular licenses to particular users based of user's attributes For Example: If the designation is Manager then assign a particular license
- Support for synchronized identity environments - In an environment where Azure AD Connect is used to sync the on-premise AD objects with Azure AD domain without federating the on-premise domain in Azure, Active Roles enables the synchronization of all the on-premise objects to Azure through Azure AD Connect and no modification to the objects is allowed in Azure directly.
- Azure Application permissions enhancements - When an Azure AD application is registered, the administrator defines the permission scope for the application. By default, minimal permissions are assigned to every application.

- Support for creating users, groups, and contacts in Azure/Office 365 through SPML
- New Access Template for Azure Configuration Administrator and Azure Health Status Check:
    - Azure Config Admin access template allows the user to perform only Azure Configuration from WI
    - Health Check Access Template will allows a user to check Azure Configuration status and License Reports

Extensibility

To access external data systems, Synchronization Service employs so-called *connectors*. A connector enables Synchronization Service to read and synchronize the identity data contained in a particular data system. Out of the box, Synchronization Service includes connectors that allow you to connect to the following data systems:

- Microsoft Active Directory Domain Services
- Microsoft Active Directory Lightweight Directory Services
- Microsoft Exchange Server
- Microsoft Skype for Business Server
- Microsoft Windows Azure Active Directory
- Microsoft Office 365
- Microsoft SQL Server
- Microsoft SharePoint
- Active Roles version 7.2, 7.1, 7.0, 6.9, 6.8, or 6.7
- One Identity Manager version 6.1 or 6.0
- One Identity Manager 7.0
- Data sources accessible through an OLE DB provider
- Delimited text files

2

Upgrade issues

Impact on Active Roles replication

The upgrade process of the Administration Service does not preserve the replication settings. An upgrade can only be performed if the Administration Service is not configured for replication. Before upgrading the Administration Service, you should ensure that its database server is not configured as a Subscriber or Publisher. Replication for the new Administration Service needs to be configured after the upgrade.

Impact on custom solutions

An upgrade of Active Roles components may affect custom solutions that build upon the functions of Active Roles. Custom solutions (such as scripts or other modifications) that work fine with the earlier version of Active Roles may cease to work after the upgrade. Prior to attempting an upgrade, you should test the existing solutions with the new version of Active Roles in a lab environment to verify that the solutions continue to work. Should any compatibility issues arise during the test process, you can contact One Identity Software Professional Services for paid assistance with those solutions.

Impact on unmanaged domains

Upgrade of the Administration Service converts unmanaged domains to regular managed domains. If you have any domains registered as unmanaged domains with Active Roles version 6.8 or earlier, then, after the upgrade, you will need to make them unmanaged by applying the build-in Policy Object **Exclude from Managed Scope**. For further information and instructions, see "Configuring an unmanaged domain" in the Active Roles Administrator Guide.

Impact on add-ons

After an upgrade of Active Roles components to the latest version, the add-ons which were supported in the earlier versions of Active Roles, cease to work. Hence, it is recommended to uninstall the add-ons prior to the upgrade of Active Roles.

NOTE: Office 365 add-on is not supported on the Active Roles 7.2.

Glossary

A

Access Control

A security mechanism that determines which operations a user, group, service, or computer is authorized to perform on a computer or on a particular object, such as a file, printer, registry key, or directory service object.

Access Control Entry (ACE)

An entry in an object's discretionary access control list (DACL) that grants permissions to a user or group. An ACE is also an entry in an object's system access control list (SACL) that specifies the security events to be audited for a user or group.

Access Control List (ACL)

A list of security protections that apply to an entire object, a set of the object’s properties, or an individual property of an object. There are two types of access control lists: discretionary and system

Access Mask

In an access control entry (ACE) of the access control list (ACL) associated with an object, a 32-bit value specifying the operations allowed, denied, or audited when the SID-holder accesses the object.

Access Template

Each access template represents a stand-alone collection of access masks. When an access template is applied to a network object in relation to a given trustee, the entire collection of access masks is translated into a set of access control entries in the object's access control list, with each entry containing the trustee's security identifier and one of the access masks extracted from the access template. When an access template is modified, all the access control entries created by applying that access template are modified accordingly.

Active Directory

The Windows-based directory service. Active Directory stores information about objects on a network and makes this information available to users and network administrators. Active Directory gives network users access to permitted resources anywhere on the network using a single logon process. It provides network administrators with an intuitive, hierarchical view of the network and a single point of administration for all network objects.

Active Directory Schema

The Active Directory schema defines the set of all object classes and attributes that can be stored in the directory. For each object class, the schema defines what attributes an instance of the class must or may have and specifies the legal parents of the class. The Active Directory schema is stored in the directory as specific schema objects that are protected with access control. Schema objects can be accessed and updated dynamically.

Administration Service

A core component of Active Roles, the Administration Service manages requests to network data sources. It validates requests, performs administrative tasks, and enforces administrative policies.

Administrator

In the Windows Server family, a person who is responsible for setting up and managing local computers, stand-alone servers, member servers, or domain controllers. An administrator sets up user and group accounts, assigns passwords and permissions, and helps users with networking problems. Administrators can be members of the Administrators group on local computers or servers. A person who is a member of the Administrators group on a local computer or server has full access to that computer or server and can assign access control rights to users as necessary. Administrators can also be members of the Domain Admins group on domain controllers and have full control over user and computer accounts residing in that domain.

C

Cache

For Administration Service, a special pool in memory in which directory object data are held for quicker access. Administration Service updates the data in the cache immediately after a modification in Active Directory occurs, thereby ensuring that the cached data is always current and correct. For better performance, Administration Service only refreshes the data that is actually changed in Active Directory, achieving the real-time update of the cached data.

Collection

A set of network objects defined by membership rules. For example, a Managed Unit is a collection. The same object can be a member of more than one collection.

Computer Name

Computer names define computers to a network. Each computer name cannot be the same as any other computer or domain name in the network. A valid computer name contains letters (a-z, A-Z), numbers (0-9), and hyphens (-), but no spaces or periods (.). In addition, it may not consist solely of numbers.

Computer Resource

A computer system itself, or a network component that resides on a computer system, such as a service, share, printer, print job, connected user, or open file.

See also *Network Object* and *Directory Object*.

Configuration

See *Directory Partition*.

Console Tree

The left pane in Microsoft Management Console (MMC) that displays the items contained in the console. The items in the console tree and their hierarchical organization determine the capabilities of a console.

See also *Microsoft Management Console (MMC)* and *Details Pane*.

Container

An object that can logically contain other objects. The objects created or placed in a container object are referred to as the container's child objects, and the container object is referred to as their parent object. For example, an Organizational Unit is a container object. An object can have only one parent container.

D

Delegate Administrative Control

To assign responsibility for management and administration of a collection of network objects to an individual user or a group of users.

Delegated Administrator

See *Trustee*.

Details Pane

The right pane in Microsoft Management Console (MMC) that displays details for the selected item in the console tree. The details can be a list of items or they can be administrative properties, services, and events that are acted on by a snap-in.

See also *Console Tree*, *Microsoft Management Console (MMC)*, and *Snap-in*.

Directory Database

The physical storage for each replica of Active Directory. Also called the *store*.

See also *Active Directory*.

Directory Object

Any object stored in Active Directory or other directory service. A directory object is described by a distinct, named set of attributes. For example, the attributes of an Active Directory user object might include the user's first name, last name, and e-mail address.

See also *Network Object*.

Directory Partition

Active Directory is made up of one or more partitions (naming contexts). Each partition represents a contiguous sub-tree that is replicated as a unit to other domain controllers in the forest. In Active Directory, a single server holds at least three directory partitions: schema (class and attribute definitions for the directory), configuration (replication topology and related metadata), and domain (sub-tree that contains the per-domain objects for one domain).

Domain

In Active Directory, a collection of computer, user, and group objects defined by the administrator. These objects share a common directory database, security policies, and security relationships with other domains.

Domain Controller

In an Active Directory forest, a server that contains a writable copy of the Active Directory database, participates in Active Directory replication, and controls access to network resources. Administrators can manage user accounts, network access, shared resources, site topology, and other directory objects from any domain controller in the forest.

Domain Local Group

A security or distribution group that can contain universal groups, global groups, other domain local groups from its own domain, and accounts from any domain in the forest. Domain local security groups can be granted rights and permissions on resources that reside only in the same domain where the domain local group is located.

See also *Group*.

Domain Tree

In Active Directory, a hierarchical structure of one or more domains, connected by transitive, bidirectional trusts, that forms a contiguous namespace. Multiple domain trees can belong to the same forest.

See also *Forest*.

E

Explicit Permissions

Explicit permissions are those that are defined directly on an object. Explicit permissions are defined either automatically when the object is created, or by user action. For example, when a user account is created, the permissions on it are explicit permissions.

See also *Permissions* and *Inherited Permissions*.

F

Fault Tolerance

The ability of a software product to ensure data integrity when hardware failures occur. Active Roles provides fault tolerance through multi-muster replication of the data individually stored by each of a number of Administration Services.

Forest

One or more Active Directory domains that share the same class and attribute definitions (schema), site and replication information (configuration), and forest-wide search capabilities (global catalog). Domains in the same forest are linked with two-way, transitive trust relationships.

G

Global Catalog

A server that holds a partial replica of every user-naming context in Active Directory. The Global Catalog also contains the schema and configuration naming contexts. The attributes in the Global Catalog are those most frequently used in search operations and those attributes that are required to locate a full replica of the object. The Global Catalog enables users and applications to find objects in Active Directory given one or more attributes of the target object, without knowing what domain holds the object.

Global Group

A global group can be granted permissions and rights for the domain controllers of its own domain, for other members of its own domain, and for trusting domains. A global group can become a member of local groups in any of these domains. However, it can contain user accounts only from its own domain. Only domain controllers maintain global groups.

See also *Group*.

Group Name

A group name must be unique among groups and user accounts in the domain. A valid group name contains letters (a-z, A-Z), numbers (0-9), and special characters, except for the following:
/ \ [ ] : ; | = , + * ? < >

Group

A collection of users, computers, contacts, and other groups. Groups can be used as security or as e-mail distribution collections. Distribution groups are used only for e-mail. Security groups are used both to grant access to resources and as e-mail distribution lists.

See also *Domain Local Group*, *Global Group*, *Local Group*, and *Universal Group*.

H

Home Folder (Home Directory)

The home folder is a folder that is accessible to the user and can contain files and programs for that user. A network home folder can be assigned to an individual user or can be shared by many users. If no local or network home folder is assigned, the default local home folder is located on the drive on the user's computer.

Hybrid

Hybrid environment refers to an environment which uses a mix of on-premises Active Directory and Azure Active Directory and allows synchronization of objects from the on-premises AD to the Azure AD.

I

Inherited Permissions

Inherited permissions are those that are propagated to an object from a parent object. Normally, an object inherits the permissions from the container where that object is placed. For example, when an object is created or moved in an Active Directory organizational unit (OU), the object automatically inherits the permissions from that OU. Defined on a parent object, inherited permissions can only be modified by changing the parent object's permission settings.

In Active Roles, permissions defined on a managed unit or inherited by a managed unit are also inherited by all the members of that managed unit. Due to this inheritance feature, objects' permissions change as objects change their memberships in managed units, providing the ability to regulate permission settings by using membership rules.

See also *Explicit Permissions* and *Permissions*.

L

Local Group

A local group can be granted permissions and rights only for its own computer on which the group resides. However, it can contain user accounts and global groups from its own domain and trusted domains.

See also *Group*.

Logon Script

A logon script allows an administrator to affect a user's environment without managing all aspects of it. When a logon script is assigned to a user account, it runs each time the user logs on. One logon script can be assigned to one or more user accounts. It can be a batch file (.cmd or .bat filename extension) or an executable program (.exe filename extension). When a user logs on, the computer authenticating the logon locates the logon script by following the logon script path.

M

Managed Domain

A domain registered for the management with Active Roles. Active Roles can be configured to manage multiple domains.

Managed Unit

A collection of objects managed with Active Roles defined by using membership rules, for the purposes of distribution of administrative responsibilities. Managed units provide large organizations with the flexibility they need to delegate network administration, enforce administrative policies, and manage complex network environments.

Member Server

A server that is joined to a domain but is not a domain controller. Member servers typically function as file servers, application servers, database servers, Web servers, certificate servers, firewalls, or remote access servers.

Membership Rules

Membership rules are criteria by which Active Roles evaluates whether or not a network object is a member of a particular managed unit or view. Each managed unit or view only includes the objects whose properties meet the membership rules for that unit or view.

Microsoft Management Console (MMC)

A framework for hosting administrative tools called *snap-ins*. A console might contain tools, folders or other containers, World Wide Web pages, and other administrative items. These items are displayed in the left pane of the console, called a *console tree*. A console has one or more windows that can provide views of the console tree. The main MMC window provides commands and tools for authoring consoles. The authoring features of MMC and the console tree itself might be hidden when a console is in User Mode.

See also *Console Tree*, *Details Pane*, and *Snap-in*.

MMC Interface

A Active Roles user interface that network administrators and trustees use to administer Active Directory data. This interface provides access to all the capabilities of Active Roles. The MMC interface is implemented as an MMC snap-in.

See also *Snap-in*.

N

Naming Context

See *Directory Partition*.

Network Object

A directory object or computer resource.

See also *Directory Object* and *Computer Resource*.

Non-Transitive Trust Relationship

A trust relationship in a multiple-domain environment that is restricted to just two domains. For example, if domain A has a non-transitive trust with domain B, and domain B trusts domain C, then there is no trust relationship between domain A and domain C.

See also *Trust Relationship* and *Transitive Trust Relationship*.

O

Object

An object is a named set of attributes that represents something concrete, such as a user, a printer, or a computer system. The attributes hold data describing the subject that is identified by the object. For example, attributes of a user might include the user's given name, surname, and e-mail address.

Organizational Unit (OU)

An Active Directory container object used within domains. An organizational unit is a logical container into which users, groups, computers, and other organizational units are placed. It can contain objects only from its parent domain. An organizational unit is the smallest scope to which a Group Policy object (GPO) can be linked, or over which administrative authority can be delegated.

P

Permissions

Permissions represent authorization to perform certain operations on specific network objects, such as user accounts, groups, or computer resources. Unless permission to perform an operation is explicitly granted, it is implicitly denied. Permissions can also be explicitly denied. There are two types of permissions: explicit and inherited.

See also *Explicit Permissions* and *Inherited Permissions*.

Policy Object

A policy object represents a collection of administrative policies. Active Roles enforces administrative policies by linking policy objects to managed units, individual directory objects, or container objects. When linked to a unit or container, a policy object affects all the member objects, including those that are located in the child containers.

Primary Domain Controller

In a Windows NT domain, a domain controller that maintains the master copy of the Security Accounts Manager (SAM) database. The primary domain controller is the only computer that directly receives the changes made to the SAM database. Within a domain, the primary domain controller periodically replicates its data to the other domain controllers, known as backup domain controllers.

Proxy Server

The service component of Active Roles operates as a permissions-based proxy server. When accepting requests from a client, the server component validates each request as against permissions the client has for network objects. If the client's permissions are

sufficient to perform the requested operation, the service component performs it by the using the operating system facilities.

S

Schema

See *Active Directory Schema*.

Secure Communication

In Active Roles, a network connection between the client and the server that requires packet privacy. When transmitting security-sensitive information, such as a user password, Active Roles uses standard DCOM mechanisms of data protection, including data encryption.

Security Descriptor

A data structure associated with a protected object to specify security information, including who is permitted to access the object and in what way, who owns the object, and what types of access will be audited.

Security ID (SID)

A data structure of variable length that identifies user, group, and computer accounts. Every account on a network is issued a unique SID when the account is first created. Internal processes in Windows refer to an account's SID rather than the account's user or group name.

Security Principal

An account holder that is automatically assigned a security identifier (SID) to control access to resources. A security principal can be a user, group, service, or computer.

Security Subsystem

A protected subsystem that authenticates and logs users on to the system, maintains information about the local security policy, and provides various services for translation between names and security identifiers.

Service

A process that performs a specific system function and often provides an application-programming interface (API) for other processes to call.

Service Account

The user account that a service uses to log on to the computer or network. The account must have the specific rights and permissions required by that service.

Shared Resource (Share)

Refers to a computer resource that is made available to network users, such as a folder, file, or printer.

Snap-in

A type of tool that you can add to a console supported by Microsoft Management Console (MMC). A stand-alone snap-in can be added by itself; an extension snap-in can be added only to extend the function of another snap-in.

See also *Microsoft Management Console (MMC)*.

Standalone Server

A server that runs the Windows operating system, but does not participate in a domain. A stand-alone server has only its own database of users, and it processes logon requests by itself. A stand-alone server does not share account information with other computers and cannot provide access to domain accounts.

See also *Domain* and *Member Server*.

Subtree

An unbroken path in the tree, including all child objects of any container in that path.

See also *Tree* and *Domain Tree*.

T

Transitive Trust Relationship

A trust relationship that flows throughout a set of domains, such as a domain tree, and forms a relationship between a domain and all domains that trust that domain. For example, if domain A has a transitive trust with domain B, and domain B trusts domain C, then domain A trusts domain C.

See also *Domain Tree*, *Forest*, and *Non-Transitive Trust Relationship*.

Tree

Tree is usually used to describe a hierarchy of objects. Nodes in the tree (points at which the tree branches) are container objects. For example, a computer network or domain is a container object. A tree shows how objects are connected or the path from one object to another. A contiguous sub-tree is any unbroken path in the tree, including all child objects of any container in that path.

Trustee

A group or user account that is authorized to perform specific administrative tasks for a specific set of network objects managed with Active Roles. Normally, Trustees are regular

users or groups that have no rights to perform administrative tasks by directly accessing Active Directory. This ensures that the only way for the Trustees to perform their tasks is by using Active Roles.

Trust Relationship

A logical relationship established between domains to allow pass-through authentication, in which a trusting domain honors the logon authentications of a trusted domain. User accounts and global groups defined in a trusted domain can be given rights and permissions in a trusting domain, even though the user accounts or groups don't exist in the trusting domain's directory.

Trusted Domain

See *Trust Relationship*.

Trusting Domain

See *Trust Relationship*.

Two-way Trust Relationship

A link between two domains that allows each domain to trust user accounts in the other domain to use its resources. A user can log on from computers in either domain to the domain that contains the user's account.

See also *Trust Relationship*.

U

UNC Name

A full name of a shared resource on a network. It conforms to the *servername**sharename* syntax, where *servername* is the server's name and *sharename* is the name of the shared resource. UNC names of folders or files can also include the directory path under the share name, with the following syntax:
`\\servername\sharename\directory\filename`

UNC is also called Universal Naming Convention.

Universal Group

A security or distribution group that can contain users, groups, and computers from any domain in its forest as members. Universal security groups can be granted rights and permissions on resources in any domain in the forest.

See also *Group*.

User Account

In Active Directory, an object that consists of all the information that defines a domain user, which includes user name, password, and groups in which the user account has membership. User accounts can be stored in either Active Directory or on a local computer.

User Profile

A file that contains configuration information for a specific user, such as desktop settings, persistent network connections, and application settings. Each user's preferences are saved to a user profile that Windows uses to configure the desktop each time a user logs on.

W

Wildcard Character

A character that represents one or more characters. The question mark (?) wildcard can be used to represent any single character and the asterisk (*) wildcard can be used to represent any character or group of characters that might match that position in other names. Wildcard characters are especially instrumental in defining membership rules. For example, when defining a membership rule to include all servers with names that begin with X, you would specify X* as the computer name. One more wildcard character, the number sign (#) represents any digit or the number sign itself.

Contacting us

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

Technical support resources

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

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

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