One Identity Active Roles 7.2

Product Overview 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 Product Overview Guide
Updated - December 2017
Version - 7.2

Contents

Preface

Active Roles simplifies and streamlines creation and ongoing management of user accounts and groups in Windows Active Directory (AD) centric environments by automating user and group account creation in AD, mailbox creation in Exchange, group population, and resource assignment in Windows. 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 offers point-and-click modular configuration for easy deployments, along with rules and a delegated administration model to ensure correct access and tight security. A multi-level approval workflow, easy-to-use Web interfaces, and integration points reduce costs associated with user and group account management, with no custom coding required.

This document is designed for IT managers, network administrators, operations managers, and security managers who are evaluating Active Roles and want to learn how it works. The document examines:

- Active Roles features and benefits
- The system's components and architecture
- Access Templates, Policy Objects, and Managed Units
- Support for Active Directory security management
- Customization with the Active Roles ADSI Provider and support for scripting
- Rule-based management of group membership lists
- Operation of Active Roles in multi-forest environments
- Capabilities of the Active Roles Web Interface
- Example scenarios in which Active Roles might be used

Summary

Active Roles delivers a reliable, policy-based administration and provisioning solution, allowing enterprises to fully benefit from Active Directory and Microsoft Exchange deployment.

One of the most valuable features of the product is the ability to automate provisioning tasks on directory objects in compliance with corporate administrative policies in corporate Active Directory and Exchange environments.

Active Roles provides consistent enforcement of corporate policies, a role-based administrative model, and flexible, rule-based administrative views, creating a reliable and secure environment for distributed administration and account provisioning.

Examples of use

Active Roles can be configured to provide a wide range of directory management solutions, allowing organizations to create more secure, productive, and manageable Active Directory and Microsoft Exchange environments. This section highlights how Active Roles helps to address the challenges faced by enterprises today.

Distributing administration

Suppose a large company wants to introduce distributed administration, but wants to avoid the large costs involved in training their Help Desk and business units to correctly use complex administrative tools. In this situation, there is the need for an easy-to-use tool, to control what actions the Help Desk and business units can perform, and to enforce company policies and procedures.

Solution

Active Roles allows organizations to create Managed Units and to designate Trustees over those Managed Units. Trustees only see the objects to which they have access. They are given only the rights they need for the objects within these Managed Units, down to individual properties. Unlike native Active Directory organizational units, Managed Units provide virtual boundaries that span across domains and forests, offering more flexible delegation capabilities.

Delegating limited control over Managed Units efficiently eliminates the need for high-level administrative user ID's, allowing organizations to securely distribute administrative authority to local management. To improve network security and make distributed administration safe, Active Roles defines and enforces customizable administrative polices.

Active Roles allows organizations to safely implement administration for business units. If a company has a number of different business units, each of equal importance and each located in a separate office, a single network administrator could support all of the sites. Active Roles allows the company to create a single Managed Unit, giving an administrator control over users and resources that span multiple domains.

Integrating with other systems

Suppose a company wants to integrate its HR system, administration, and physical security to provide a workflow that reduces repetitive data. Normally, the HR team creates a user profile, the IT team also creates a user profile in Windows and Exchange, and the security team activates an access card for the new employee. The three teams do not synchronize

with each another and instead duplicate their work. This results in increased administration costs and introduces security issues. For example, some individuals may no longer work for the company but may still have valid user ID’s and access cards. In this scenario, there is a need to integrate the company’s HR system and other systems, and to automate the execution of user provisioning tasks.

Solution

With Active Roles, a suitable property set can be established to include data from network data sources other than Active Directory. For instance, a property set might be configured to retrieve a user’s personal information from an HR database. When the user account is created, this data could then be passed to Active Directory and Microsoft Exchange. If these property values change, an update could be made to both Active Directory and to the HR system.

Active Roles also provides the ability to set up administrative policies that reduce the amount of input required to carry out a task. For example, when a user moves to a different location, Active Roles could automatically update the user's profile in the HR system, based only on the change to the user's site code or department in Active Directory. Additionally, when a user joins or leaves the company, their access card could automatically be enabled or disabled.

Managing a multi-forest Active Directory design

Suppose a host company has client customers who need to place domain controllers on their premises. In Active Directory, every domain controller holds a writable copy of the schema and configuration of the entire forest. Anyone with administrative or backup/restore rights on any domain controller, or physical access to any domain controller, could potentially disrupt the entire forest. For instance, they could attempt to circumvent Windows security, or they could edit the Active Directory database, and the changes would be propagated to all domains in the forest. To avoid such an incident, the company needs to create a separate forest for each client who requires domain controllers on their premises. Otherwise, the actions of one malicious user could affect directory service delivery for other clients in the same forest.

Having multiple forests increases the complexity of the Active Directory structure. This in turn leads to increased administration, as each forest needs separate directory service administration. In this case, there is a need for an administrative system that enables the cross-forest management of Active Directory.

Solution

Active Roles provides a unified management structure that can extend across multiple Active Directory forests. The Active Roles user interface provides a single interface for the management of Active Directory domains that belong to different forests. It offers administrative views (Managed Units) that can hold objects from multiple forests, thereby enabling the unified application of corporate rules and roles across forest boundaries.

With its ability to safely delegate administration in multi-forest environments, Active Roles provides the necessary level of control for the host company's customers, while enabling the company to implement role-based security, and restrict the customers' administrative actions based on corporate policies.

For security reasons, it may be unacceptable to have an administrative tool with the same level of rights as a domain administrator. This is because administrative access to an entire domain in a forest may be used to gain administrative access to the whole forest, via the elevation of privileges attack. Active Roles can operate in a multi-forest environment within a precisely defined scope of access to domains, with no special requirement to have administrative access to entire domains or security-sensitive containers. This addresses the need for a product that provides advanced administrative capabilities, while effectively preventing the elevation of privileges.

Simplifying Active Directory structure

Suppose a company wants to design an Active Directory structure based on physical location. As a rule, the administration/IT department, business units, and Exchange team would each prefer to have a different structure. As a result, they agree to a compromise that doesn't fully satisfy their requirements. Clearly, there is a need to simplify the Active Directory structural requirements.

Solution

In Active Roles, Managed Units allow organizations to achieve acceptable security boundaries without setting up extra domains or organizational units. This significantly simplifies the Active Directory structure and reduces security risks.

By using Managed Units for delegation purposes, Active Roles creates a rule-based overlay of Active Directory for administration. This simplifies the process of choosing an Active Directory structure. Different administrative tasks often require different OU structures. For instance, an OU structure designed purely for the delegation of administration differs from an OU structure shaped purely for Group Policy. It becomes much easier to design an Active Directory structure by using Managed Units to handle delegation issues.

Handling organizational changes

Consider a company in the process of re-organization. Multiple departments are changing names, merging, or separating from one another. Such reorganization involves an increase in administrative, security, and business liabilities, as well as the high cost of manually updating data. This situation demands a means to automatically update and move the data.

Solution

Active Roles provides the ability to define administrative policies that make organizational changes easier to handle. By using Managed Units, rule-based overlays of the actual data in Active Directory can be set up for both the current and planned organizational structures. Administrative policies can be specified so that when data moves from one Managed Unit to another, policy definitions will automatically be applied, based on the change. This will update properties, such as the user's manager, department, group memberships, and OU memberships.

As another example, consider a user who changes departments. Depending on the department to which the user moves, Active Roles could automatically move the user's data, change the user's group memberships, and specify to whom the user reports.

User Account Management

Suppose a company provides services based on Active Directory and Microsoft Exchange. The company relies on the Active Directory infrastructure as a basis for their service offerings.

Configuration of Active Directory involves setting security and partitioning the directory, so that any user has proper access to directory resources. It is paramount to have a framework that facilitates the creation of new user accounts and the assignment of appropriate access rights. There is a need for a robust system that maintains user creation and management with minimal administrative effort.

Solution

Active Roles offers a reliable solution to simplify and safely distribute user account management. It addresses the need to create and manage a large number of user accounts, and to ensure that each user can only access their own resources. By implementing an administrative model based on business rules, Active Roles allows domain-level administrators to easily establish and maintain very tight security, while facilitating the provisioning of new users with the appropriate access to IT resources

Active Roles has the ability to safely delegate routine user-management tasks to designated persons. By incorporating policy enforcement and role-based security, Active Roles allows the organization to restrict the administrative actions according to the corporate policies defined by the high-level administrators. In addition, it allows the administrators to change the policies, ensuring that new policy settings are automatically propagated and enforced without additional development.

Active Roles makes it simpler for the organization to delegate authority to administrative and support groups, while enhancing the overall security. The Web Interface can serve as an administrative tool that allows the assistant administrators to manage users, groups, and mailboxes. Active Roles ensures that all actions performed by a Web Interface user are in compliance with the corporate security policies.

Customizable Web Interface

The Active Roles Web Interface is a customizable Web-based application that facilitates administration, while taking full advantage of Active Roles' security, workflow integration, and reporting benefits. To help distribute administrative tasks, the Web Interface allows you to configure multiple Web sites with individual sets of user interface elements. Each Web site can be customized to meet specific business and organizational needs.

Key features

Key features of the Web Interface include the following.

Role-based suite of interfaces

Customized interfaces (Web Interface sites) can be installed and configured for administrators, help desk operators, and end users. Administrators use an interface that supports a wide range of tasks, whereas help desk operators use a tailored, dedicated interface to expedite the resolution of trouble tickets. Network end users have access to an interface for self-administration. Multiple interfaces with different configurations can be deployed so that there is no need to re-configure the Web Interface for particular roles.

Dynamic configuration based on roles

The Web Interface dynamically adapts to the specific roles assigned to the users. A user can see only the commands, directory objects, and object properties to which the user's role provides administrative access. Objects and commands beyond the scope of the user are removed from the Web Interface, streamlining the execution of administrative tasks.

Point-and-click customization

It is straightforward to configure the user interface. Administrators can set up a suitable set of user interface elements without writing a single line of code. Administrators can add and remove commands or entire menus, assign tasks and forms to commands, modify forms used to perform tasks, and create new commands, tasks, and forms. All configuration settings are saved in a persistent storage so that the Web Interface users are always presented with the properly configured interfaces that suite their roles.

Instant application of administrative policies

User input is efficiently supplemented and restricted based on administrative policies defined in Active Roles. The Web Interface displays property values generated in accordance with the policies, and prohibits the input of data that violates them. User input is checked against the policies before committing the operation request, and if a violation is detected, the user can immediately correct the input.

Fully-featured management solution

The Web Interface supports all administrative tasks on Active Directory objects such as users, groups, and computers, and on computer resources such as services, printers, network file shares, and local users and groups. With its advanced customization capabilities, the Web Interface serves as a complete administrative tool, providing suitable interfaces for any administrative role.

User Profile Editor

Provided they have the necessary Active Roles permissions, end users can view or change their personal data. Due to the reliable enforcement of business rules based directory entry, the Web Interface makes these tasks safe and secure. With User Profile Editor, Active Roles enables IT to manage, but not necessarily participate, in these time-consuming tasks, resulting in decreased help desk calls and IS administration time.

Support for multiple languages

The Web Interface allows users to select their preferred language. Changing the language affects all menus, commands, and forms associated with the Web Interface, as well as tool tips and help.

Different interfaces for different roles

The Web Interface allows multiple Web sites to be installed with individual, customizable configurations. The following configuration templates are available out-of-the box:

- **Site for Administrators** Supports a broad range of tasks, including the management of all directory objects and computer resources.
- **Site for Help Desk** Handles typical tasks performed by Help Desk operators, such as enabling or disabling accounts, resetting passwords, and modifying certain properties of users and groups.

- **Site for Self-Administration** Provides User Profile Editor, allowing end users to manage personal or emergency data through a simple-to-use Web interface.

Each Web site configuration template provides an individual set of commands installed by default. The Web site can be customized by adding or removing commands, and by modifying Web pages (forms) associated with commands.

Although the Web Interface dynamically adapts to roles assigned to users, the ability to tailor separate Web sites to individual roles gives increased flexibility to the customer. It helps streamline the workflow of directory administrators and help-desk personnel. Static configuration of interface elements ensures that Web Interface users have access to the specific commands and pages needed to perform their duties.

Role-based management of computer resources

Active Roles provides the ability to delegate administration of computer resources, such as services and printers. Delegated administrators can use the Active Roles Web Interface to manage computer resources with a single, consolidated tool. Active Roles, along with the Web Interface, enables the delegation of administrative tasks on the following computer resources:

- **Services** Start or stop a service, view or modify properties of a service.
- **Network File Shares** Create a file share, view or modify properties of a file share, stop sharing a folder.
- **Logical Printers** Pause, resume or cancel printing, list documents being printed, view or modify properties of a printer.
- **Documents being printed (print jobs)** Pause, resume, cancel or restart printing of a document, view or modify properties of a document being printed.
- **Local groups** Create or delete a group, add or remove members from a group, rename a group, view or modify properties of a group.
- **Local users** Create or delete a local user account, set a password for a local user account, rename a local user account, view or modify properties of a local user account.
- **Devices** View or modify properties of a logical device, start or stop a logical device.

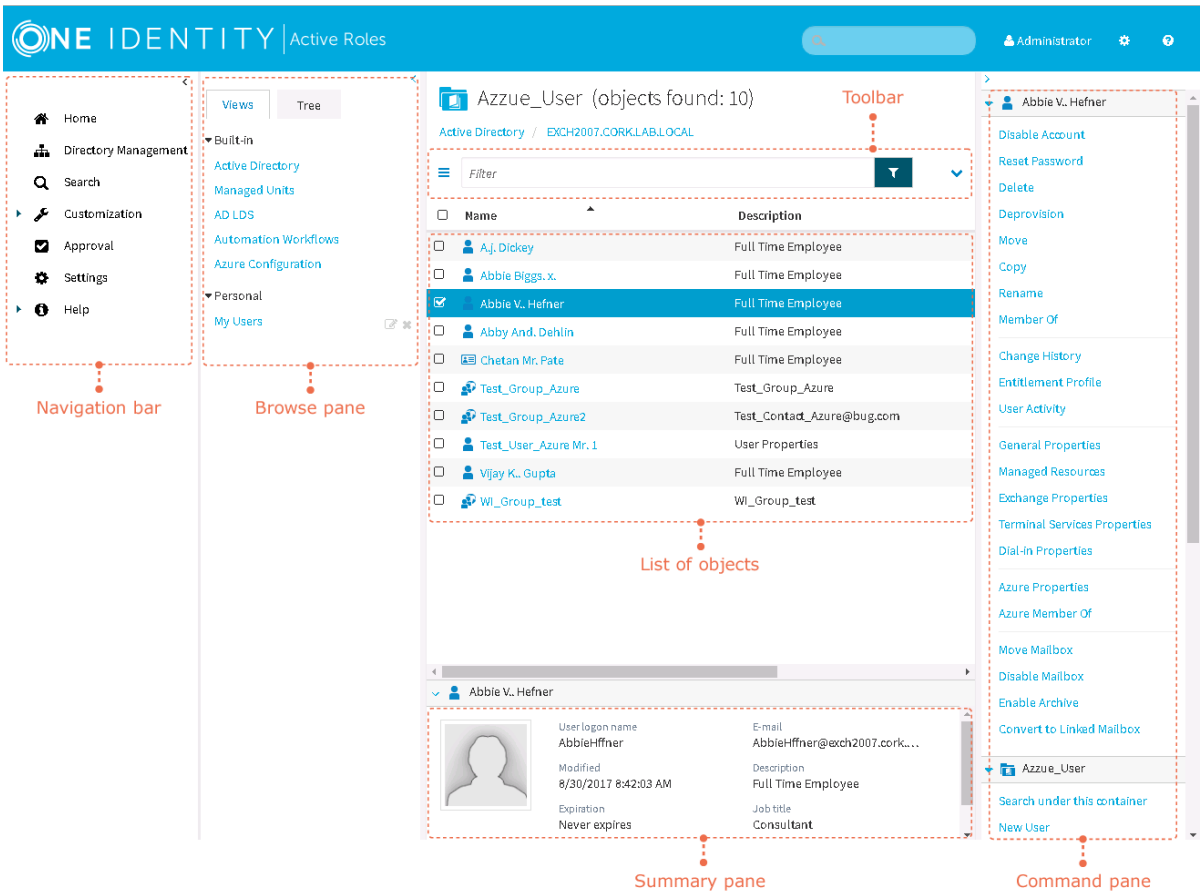
Active Roles provides a comprehensive set of Access Templates that are available out of the box for delegating computer management tasks. By applying Access Templates of the "Computer Resources" category to a computer account, the rights of delegated administrators can be specified on the corresponding computer's resources.

Delegated administrators should use the Web Interface rather than the Active Roles console (MMC Interface) to manage computer resources. Although the console provides certain tools for computer resources management, the console user needs the native administrator rights on the computer in order to use those tools. The rights specified

through “Computer Resources” Access Templates have no effect in the tools provided by the console for computer resources management.

Technical overview

Active Roles divides the workload of directory administration and provisioning into three functional layers—presentation components, service components, and network data sources.



The presentation components include client interfaces for the Windows platform and the Web, which allow regular users to perform a precisely defined set of administrative activities. The reporting solution facilitates automated generation of reports on management activities.

The service components constitute a secure layer between administrators and managed data sources. This layer ensures consistent policy enforcement, provides advanced automation capabilities, and enables the integration of business processes for administration of Active Directory, Microsoft Exchange, and other corporate data sources.

The Administration Database stores information about all permission and policy settings, and other data related to the Active Roles configuration.

On a very high level, the Active Roles components work together as follows to manipulate directory data:

1. An administrator uses the MMC interface or Web interface to access Active Roles.
2. The administrator submits an operation request, such as a query or data change to the Administration Service.
3. On receipt of the operation request, the Administration Service checks whether the administrator has sufficient permissions to perform the requested operation (access check).
4. The Administration Service ensures that the requested operation does not violate the corporate policies (policy enforcement).
5. The Administration Service performs all actions required by the corporate policies, before committing the request (policy enforcement).
6. The Administration Service issues operating system function calls to perform the requested operation on network data sources.
7. The Administration Service performs all related actions required by the corporate policies, after the request is processed by the operating system (policy enforcement).
8. The Administration Service generates an audit trail that includes records about all operations performed or attempted with Active Roles. Directory-change tracking reports are based on the audit trail.

Let us examine the three component layers.

Presentation components

The presentation components include user interfaces to serve a variety of needs. The user interfaces accept commands, display communication, and give results in a clear, concise fashion.

Active Roles console (MMC Interface)

The Active Roles console, also referred to as the MMC Interface, is a comprehensive administrative tool for managing Active Directory and Microsoft Exchange. It enables you to specify administrative roles and delegate control, define administrative policies and automation scripts, easily find directory objects, and perform administrative tasks.

Web Interface

Via the Web interface, intranet users with sufficient administrative rights can connect to Active Roles to perform basic administrative tasks, such as modifying user data or adding users to groups. The Web interface provides departmental and help-desk personnel with the administrative capabilities they need.

Custom Interfaces

In addition to the MMC and Web interfaces, Active Roles enables the development of custom interfaces that use the Active Roles ADSI Provider to access the features of Active Roles. Administrators familiar with scripting and programming can create custom interfaces to meet specific needs of the network administration.

Active Roles ADSI Provider

The Active Roles ADSI Provider operates as part of Presentation Components to enable custom user interfaces and applications to access Active Directory services through Active Roles. The Active Roles ADSI Provider translates clients' requests into DCOM calls and interacts with the Administration Service.

The Active Roles ADSI Provider allows custom scripts and applications, such as Web-based applications, to communicate with Active Directory, while taking full advantage of the security, workflow integration and reporting benefits of Active Roles. For example, using the Active Roles ADSI Provider, Web-based pages can be created such that user property modifications made by help-desk operators are restricted by the corporate rules enforced by Active Roles.

Reporting

Active Roles offers comprehensive reporting to monitor administrative actions, corporate policy compliance, and the state of directory objects. The Active Roles reporting solution includes Data Collector and Report Pack.

Report Pack provides report definitions for creating reports based on the data gathered by Data Collector. Active Roles comes with an extensive suite of report definitions that cover all administrative actions available in this product.

Report Pack is deployed on Microsoft SQL Server Reporting Services (SSRS). You can use the tools included with SSRS to view, save, print, publish, and schedule Active Roles reports.

Data Collector is used to gather data required for reporting. The Data Collector Wizard allows you to configure and schedule data collection jobs.

Once configured, Data Collector retrieves data from various sources, accessing them via the Active Roles Administration Service, and stores the data in a SQL Server database. Data Collector also provides a means for managing the gathered data, including the ability to export or delete obsolete data.

Service components

At the core of Active Roles lies the Administration Service. It features advanced delegation capabilities and ensures the reliable enforcement of administrative policies that keep data current and accurate. The Administration Service acts as a bridge between the presentation components and network data sources. In large networks, multiple Administration Services can be deployed to improve performance and ensure fault tolerance.

Data processing component

The data processing component accepts administrative requests and validates them by checking permissions and rules stored in the Administration Database. This component manages the network data sources, retrieving or changing the appropriate network object data based on administrative requests and policy definitions.

The data processing component operates as a secure service. It logs on with domain user accounts having sufficient privileges to access the domains registered with Active Roles (managed domains). The access to the managed domains is limited by the access rights of those user accounts.

Configuration database

The Administration Service uses the configuration database to store configuration data. The configuration data includes definitions of objects specific to Active Roles, assignments of administrative roles and policies, and procedures used to enforce policies. The configuration database is only used to store Active Roles configuration data. It does not store copies of the objects that reside in the managed data sources, nor is it used as an object data cache.

Active Roles uses Microsoft SQL Server to host the configuration database. The replication capabilities of SQL Server facilitate implementation of multiple equivalent configuration databases used by different Administration Services.

Audit trail

The data processing component provides a complete audit trail by creating records in the event log on the computer running the Administration Service. The log shows all actions performed and by whom, including actions that were not permitted. The log entries display the success or failure of each action, as well as which attributes were changed.

Network data sources

Through the Administration Service, Active Roles accesses and controls the object data stored in the following data sources:

- **Active Directory domains & forests** Provides the directory object information in Active Directory domains.
- **Microsoft Exchange servers** Provides information about mailboxes maintained by Microsoft Exchange.
- **Other data sources** Provides information about objects that exist outside of Active Directory. This includes information from corporate databases, such as human resources databases, and information about computer resources, such as services, printers, and network file shares.

Active Roles is designed to help with the use and management of these data sources. Directory administrators can define and enforce business rules and policies to ensure that the data in the managed data sources remains current and accurate.

With Active Roles, you can utilize the information stores from a wide variety of data sources in your network, such as human resource data or inventories. You can use scripting to integrate these important data sources. This reduces the duplication of work, reduces data pollution, and allows for the validation of information that is often stored in more than one database.

Active Roles makes it possible for a custom script to receive control upon a request to perform an administrative operation, such as object creation, modification, or deletion. Custom scripts can be invoked through Policy Objects, which Active Roles uses to enforce corporate rules. For example, you could implement a Policy Object containing a custom script that will receive control whenever Active Roles is requested to create a user object in a certain OU.

The Policy Object could be configured so that Active Roles continues with the user creation only after a certain piece of the script (the pre-create event handler) has successfully executed. In this way, the script prohibits the creation of user objects whose properties violate corporate rules. It prevents the population of object properties with values taken from external data sources, and generates default property values in accordance with the corporate rules.

The Policy Object may also be configured to pass control to another piece of the script (the post-create event handler) immediately after a user object is successfully created. This enables the script to trigger additional actions, required by corporate rules, after the object has been created. For example, it can update external data stores, provision the user with access to resources, and notify that the user object has been created.

Security and administration elements

Active Roles offers three key security and administration elements, which are stored as objects in the Administration Database:

- Access Templates
- Policy Objects
- Managed Units

These elements enable any user or group in Active Directory to be given limited and effectively controlled administrative privileges.

Users and groups that are given administrative permissions in Active Roles are referred to as *Trustees*. Trustees can be assigned to Managed Units or directory objects and containers.

Trustees do not need special administrative rights within Active Directory. To give Trustees access to Active Directory, Active Roles implements proxy mechanisms that use Access Templates to specify the level of access. When Trustees exercise their access permissions, these mechanisms use Policy Objects to trigger additional actions, such as running integration scripts and validating input data.

When designating a user or group as a Trustee, you must specify the Access Templates that control what the Trustee can do. Permissions granted to a group are extended to all members of that group. To reduce administration time, administrative control should be delegated to groups, rather than to individual users.

To implement policy constraints and automation, you must configure and apply Policy Objects that invoke built-in or custom procedures upon administrative requests. Policy procedures may include running custom scripts to synchronize Active Directory data with other data sources, performing a data validity checkup, and initiating additional administrative operations.

Access Templates for role-based administration

An *Access Template* is a collection of permissions that define what actions can be performed by an administrative role. Active Roles applies Access Templates to directory objects, containers, and administrative views (Managed Units) in relation to groups and users designated as Trustees.

Active Roles offers an extensive suite of preconfigured Access Templates that represent typical administrative roles, enabling the correct level of administrative authority to be delegated quickly and consistently. Access Templates significantly simplify the delegation and administration of management rights, speed up the deployment of the delegation model, and reduce management costs. The preconfigured Access Templates are discussed in the Active Roles Access Templates Available out of the Box document.

Access Templates enable centralized administrators to define administrative roles with various levels of authority, speeding up the deployment of access control and streamlining change tracking of permission settings across the enterprise.

It is also possible to create custom Access Templates based on business requirements. Custom Access Templates can be modified at any time. When an Access Template is modified, the permission settings on all objects where that Access Template is applied change accordingly.

Policy Objects to enforce corporate rules

A *Policy Object* is a collection of administrative policy definitions that specify corporate rules to be enforced. Access Templates define who can make changes to a piece of data, and Policy Objects control what changes can be made to the data. Active Roles enforces corporate rules by linking Policy Objects to:

- Administrative views (Managed Units)
- Active Directory containers
- Individual (leaf) directory objects

Policy Objects define the behavior of the system when directory objects are created, modified, moved, or deleted. Policies are enforced regardless of a Trustee's permissions.

A Policy Object includes stored policy procedures and specifications of events that activate each procedure. Based on policy requirements, a policy procedure could:

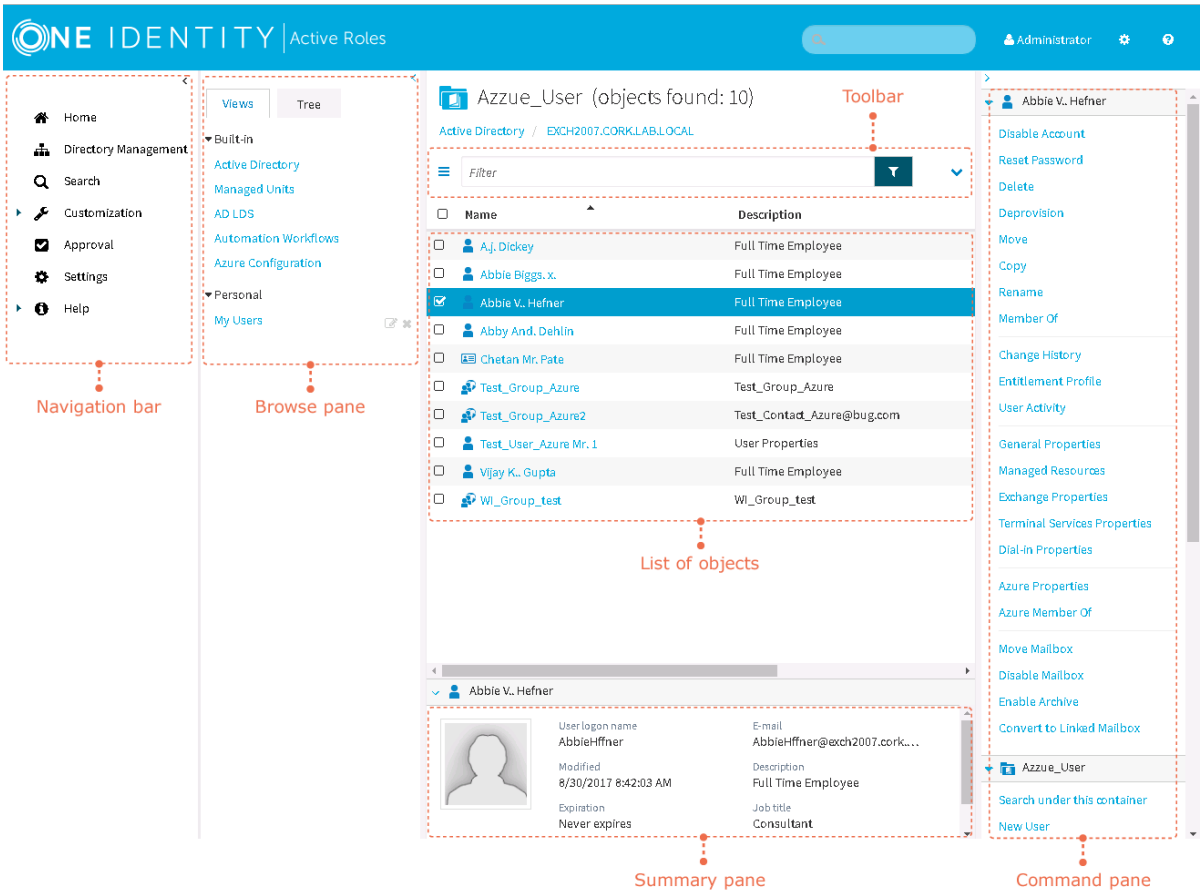
- Validate specific property values
- Allow or deny entire operations
- Trigger additional actions

A Policy Object associates specific events with its policy procedures, which can be built-in procedures or custom scripts. This provides an easy way to implement sophisticated validation criteria, synchronize different data sources, and combine a number of administrative tasks into a single batch.

Managed Units to provide administrative views

A *Managed Unit* is a collection of objects collectively managed with Active Roles, created for the distribution of administrative responsibilities, enforcement of business rules and corporate standards, and management of complex network environments. Using Managed Units, the management framework can be separated from the Active Directory design. Directory objects can easily be grouped into administrative views, regardless of their location in Active Directory.

For example, the Active Directory design might be based on geographic location, with domains named after cities or regions and organizational units named after corporate departments or groups. However, Managed Units could be designed to manage specific departments or groups that are divided across multiple geographic locations.



In this example, each AD domain has a Human Resources (HR) OU and a Sales OU. The Active Roles design has an HR MU and a Sales MU. The HR MU enables administrators to configure the policies and security restrictions needed for all HR users regardless of their location, while the Sales MU enables the same for all Sales users.

Managed Units are defined with the use of membership rules—criteria used by Active Roles to evaluate whether or not an object belongs to a given Managed Unit. This enables Managed Units to dynamically change as the network environment changes. For example, you can define a Managed Unit by specifying rules that include all objects whose properties match specific conditions. The specified rules will force the new or modified objects to be members of the correct Managed Unit.

Managed Units extend the functionality of organizational units (OUs), providing convenient scope to delegate administration and enforce corporate rules. A Managed Unit has the following characteristics:

- Represents a collection of objects (one object can belong to more than one Managed Unit)
- Supports rule-based specifications for its members (a Managed Unit only holds objects that satisfy the membership rules specified for the Managed Unit)
- Can hold directory objects that reside in different organizational units, domains, forests, and other Managed Units

Active Roles ensures that permission and policy settings specified for a Managed Unit are inherited by all objects that belong to that Managed Unit. When a directory container belongs to a Managed Unit, all child objects in that container inherit the permission and policy settings defined at the Managed Unit level. This inheritance continues down the directory tree within all container objects that are members of the Managed Unit.

Active Directory security management

The Active Roles MMC Interface makes it easy to examine and manage permission entries in Active Directory, by showing the access available to each user, along with the scope of their access. A centralized view of all permission entries for any given object helps with the analysis and administration of permissions in Active Directory. For each permission entry, the view displays a number of entry properties, including the permission description, origin, and security principal. From the main window, additional properties can be displayed and the native security editor can be accessed.

The centralized display of native security allows the administrator to quickly view permissions assigned to objects in Active Directory, and to determine whether the permission is inherited. The list of permission entries can be sorted by security principal name to determine who has access to the selected object. If a permission entry is inherited, Active Roles identifies the object from which the permission originates, so that the administrator can easily find and edit the permission entry for that object.

The Active Roles MMC Interface provides the capability to view the permissions for an object by simply clicking the object to display the permission entries in a centralized view. This makes it easier for the administrator to verify the permissions on security-sensitive objects, and to identify possible security problems.

Management of native security

Active Roles Access Templates can be used to specify permissions in Active Directory. Designed to support the role-based grouping of permissions, Access Templates provide an efficient mechanism for setting and maintaining access control, simplifying and enhancing the management of permissions in Active Directory.

To provide this capability, Active Roles gives the administrator the option to keep Active Directory native security updated with selected permissions specified using Access Templates. This option, referred to as Permissions Propagation, is intended to provision users and applications with native permissions to Active Directory. The normal operation of Active Roles does not rely on this option.

For Active Roles permission entries with the Permissions Propagation option set, Active Roles generates Active Directory native permission entries in accordance with the Active Roles permissions. Once set, the option ensures that every time Active Roles permission assignments or templates change, the associated native permission entries change accordingly.

Customization using ADSI Provider and script policies

Active Roles offers the facility to customize its off-the-shelf functionality using scripts and applications that interact with the Administration Service. It allows a high degree of customer modification to meet specific business and organizational needs. This gives customers greater flexibility when using the product, and enables them to build solutions that can easily be integrated with existing systems and data.

The following list shows some of the ways in which the product can be customized:

- Using the Active Roles ADSI Provider, the existing proprietary applications or custom Web-based interfaces could communicate with Active Roles to perform administration and provisioning tasks on user accounts and groups.
- Using policy scripts, custom corporate rules could be enforced to regulate data format and administrative workflows.
- Using policy scripts, the data stored in an HR database or ERP system could be incorporated into the administration and provision of users.

Active Roles makes it possible for user-developed scripts and applications to manipulate directory objects through the Administration Service (*persistent objects*), and to take control of objects that are in the process of being created, modified, or deleted with Active Roles (*in-process objects*).

Having programmatic access to persistent and in-process objects makes it easy for developers to customize Active Roles in these two areas:

- Creating custom applications and user interfaces
- Enforcing corporate administrative policies by running custom scripts (*script policies*)

Custom applications and user interfaces

A custom application or user interface can be created to manipulate directory objects in Active Roles. Active Roles offers the ADSI Provider to communicate with the Administration Service using standard COM interfaces that conform to the Microsoft ADSI 2.5 specification.

Custom applications are executables that provide data to the Administration Service or retrieve and process data from the Administration Service. For example, an organization with a separate Human Resources database could develop and deploy a custom application that extracts personal information from the database, and then passes it to the Administration Service in order to facilitate user account provisioning.

Custom user interfaces are usually Web-based interfaces that distribute certain tasks to users. Custom user interfaces can also be used to streamline the workflow of network administrators and help-desk operators. For example, Web-based pages could be created

so that help-desk operators only see the fields related to user properties that they can view and modify, according to the corporate standards.

Both custom applications and user interfaces rely on the Active Roles ADSI Provider to access the functionality of Active Roles.

Custom script policies

Active Roles provides the ability to implement administrative policies by running user-developed scripts. This makes it possible to:

- **Facilitate the provisioning of user accounts** Populate user properties through external database integration and automate multi-step provisioning tasks.
- **Maintain the integrity of directory content** Prevent inconsistency of Active Directory data by enforcing update-sequence and data-format policies across the enterprise.
- **Enforce business rules** Maintain security design and capture administration expertise by integrating business rules into the administrative workflow.

Once configured, the custom script-based policies are enforced without user interaction. Active Roles automatically handles the execution of policy scripts that supplement particular administrative operations and trigger additional administrative actions. For example, policy scripts can be used to:

- Perform a sophisticated validity check on input data
- Synchronously change information in multiple data sources, such as the Active Directory store, Microsoft Exchange server, and HR or ERP-system database
- Ensure that delegated administrators follow a prescribed administrative workflow
- Link multiple administrative tasks into one operator transaction

Dynamic groups

Active Roles helps streamline group maintenance by defining group membership dynamically, with rule-based membership criteria. Dynamic group membership eliminates the need to manually update membership lists for security and distribution groups.

To automate the maintenance of group membership lists, Active Roles provides:

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

The membership criteria fall into these categories:

- **Include Explicitly** Ensures that specified objects are included in the membership list regardless of any changes made to the objects.
- **Include by Query** Populates the membership list with objects that have certain properties. When an object is created, or when its properties are changed, Active Roles adds or removes it from the membership list depending on whether the object's properties match the search criteria.
- **Include Group Members** Populates the membership list with members of specified selected groups. When an object is added or removed from the selected groups, Active Roles adds or removes that object from the membership list.
- **Exclude Explicitly** Ensures that specified objects are not in the membership list regardless of any changes made to the objects.
- **Exclude by Query** Ensures that objects with certain properties are not in the membership list. Active Roles automatically removes objects from the membership list depending on whether the objects' properties match the search criteria.
- **Exclude Group Members** Ensures that members of specified groups are not in the membership list. When an object is added to any one of the selected groups, Active Roles automatically removes that object from the membership list.

These membership criteria are also applicable to Managed Units.

Workflows

Active Roles provides a rich workflow system for directory data management automation and integration. Based on Microsoft's Windows Workflow Foundation technology, this workflow system enables IT to define, automate and enforce management rules quickly and easily. Workflows extend the capabilities of Active Roles by delivering a framework that enables combining versatile management rules such as provisioning and de-provisioning of identity information in the directory, enforcement of policy rules on changes to identity data, routing data changes for approval, e-mail notifications of particular events and conditions, as well as the ability to implement custom actions using script technologies such as Microsoft Windows PowerShell or VBScript.

Suppose you need to provision user accounts based on data from external systems. The data is retrieved and then conveyed to the directory by using feed services that work in conjunction with Active Roles. A workflow can be created to coordinate the operations in account provisioning. For example, different rules can be applied for creating or updating accounts held in different containers.

Workflows may also include approval rules that require certain changes to be authorized by designated persons (approvers). When designing an approval workflow, the administrator specifies which kind of operation causes the workflow to start, and adds approval rules to the workflow. The approval rules determine who is authorized to approve the operation, the required sequence of approvals, and who needs to be notified of approval tasks or decisions.

By delivering e-mail notifications, workflows extend the reach of management process automation throughout the enterprise. Notification activities in a workflow let people be

notified via e-mail about events, conditions or tasks awaiting their attention. For example, approval rules can notify of change requests pending approval, or separate notification rules can be applied to inform about data changes in the directory. Notification messages include all necessary supporting information, and provide hyperlinks enabling message recipients to take actions using a standard Web browser.

The logic of an automated management process can be implemented by using administrative policies in Active Roles. Yet creating and maintaining complex, multi-step processes in that way can be challenging. Workflows provide a different approach, enabling IT administrators to define a management process graphically. This can be faster than building the process by applying individual policies, and it also makes the process easier to understand, explain and change.

Operation in multi-forest environments

Active Directory organizes network elements into a hierarchical structure based on the concept of containers, with the top-level container being referred to as a forest. Today, many real-world Active Directory implementations consist of several forests. Common reasons for multi-forest deployments are the isolation of the administrative authority, organizational structure issues (e.g., autonomous business units and decentralized IT departments), business policy, or legal and regulatory requirements.

This section provides information on the features and benefits of Active Roles as applied to environments where multiple Active Directory forests have been deployed.

With Active Roles, you can create a scalable, secure, and manageable infrastructure that simplifies user and resource management in a multi-forest environment. Benefits of deploying Active Roles in such environments include:

- Centralized management of directory data in domains that belong to different forests
- Administrative views spanning forest boundaries
- The ability to delegate administrative control of directory data where appropriate, without regard to forest boundaries
- Policy-based control and automation of directory data management across forest boundaries

By registering Active Directory domains with Active Roles, you form a collection of managed domains that represents an Active Roles security and administrative boundary in Active Directory. The collection need not be restricted to domains from a single forest. Rather, you can register domains from any forest in your environment, configuring the Active Roles Administration Service to use the appropriate administrative credentials on a per-domain basis.

To centralize management of directory data across the managed domains, Active Roles retrieves and consolidates the Active Directory schema definitions from all forests to which those domains belong. The consolidated schema description is stored in the Active Roles configuration database, and contains information about the object classes and the attributes of the object classes that can be stored in the managed domains. By using the

consolidated schema, Active Roles extends the scope of its administrative operations to cover the entire collection of managed domains regardless of forest boundaries.

Active Roles allows administrators to organize directory objects (such as users, groups, computers, and so on) into a relational structure made up of rule-based administrative views (referred to as Managed Units), each of which includes only the objects that meet certain membership criteria defined by the administrator. This structure can be designed independently from the logical model of Active Directory, which is based on the concept of containers and thus implies rigid boundaries between containers, be it forests, domains or organizational units. Administrators can configure Managed Units so that each Unit represents the appropriate collection of directory objects that reside in the same Active Directory container or in different containers, with different forests not being the exception.

To facilitate the management of directory data, Active Roles provides for administrative delegation at the Managed Unit level as well as at the level of individual containers in Active Directory. Through delegation, authority over directory objects held in a given Unit or container can be transferred to certain users or groups. Delegation of control over Managed Units provides the ability to distribute administration of directory data among individuals trusted to perform management of specific groups and types of objects, without taking into account the location of the objects in the Active Directory structure. Thus, Active Roles makes it easy to delegate control of directory data from one forest to users or groups located in the same forest or in a different forest.

Active Roles also allows policy-based control and automation of directory data management to be implemented at the Managed Unit level. By applying policy and automation rules to Managed Units, administrators can ensure consistent control of the well-defined collections of directory objects located in different organizational units, domains, or forests. In addition, policy and automation rules can be consistently applied to different containers, whether in the same forest or in different forests, which provides the platform for complex automation scenarios that involve cross-forest operations. An example could be provisioning users from one forest with resources in another forest.

When adding objects to a group, Active Roles allows you to select objects from different managed domains, including those that belong to different forests. This operation requires a trust relationship between the domain that holds the group and the domain that holds the object you want to add to the group. Otherwise, Active Directory denies the operation and, therefore, Active Roles does not allow you to select the object. Note that Active Directory automatically establishes trust relationships between domains within one forest. As for domains in different forests, administrators must explicitly establish trust relationships as needed.

The rule-based mechanisms that Active Roles provides for auto-populating groups can also be freely used in multi-forest environments. You can configure rules to have Active Roles populate groups with objects that reside in different domains, whether in the same forest or in different forests. However, the capabilities of Active Roles to automatically manage group membership lists are also restricted by the Active Directory constraints that only allow a group to include objects from the domain that holds the group or from the domains trusted by that domain. In other words, unless a trust relationship is established between the domain that holds the group and the domain that holds a given object, the object cannot be added to the group, neither manually nor automatically by Active Roles.

Features and benefits

Active Roles provides out-of-the-box user and group account management, strictly enforced administrator-based role security, day-to-day identity administration and built-in auditing and reporting for Windows-centric environments. The following features and capabilities make Active Roles a practical solution for secure management of users and groups in Active Directory (AD) and AD-joined systems:

- **Secure access** Acts as a virtual firewall around Active Directory, enabling you to control access through delegation using a least privilege model. Based on defined administrative policies and associated permissions generates and strictly enforces access rules, eliminating the errors and inconsistencies common with native approaches to AD management. Plus, robust and personalized approval procedures establish an IT process and oversight consistent with business requirements, with responsibility chains that complement the automated management of directory data.
- **Automate account creation** Automates a wide variety of tasks, including:
  - Creating user and group accounts in Active Directory (AD)
  - Creating mailboxes on Exchange Server
  - Populating groups
  - Assigning resource in Windows

  Active Roles also automates the process of reassigning and removing user access rights in AD and AD-joined systems (including user and group de-provisioning) to ensure an efficient and secure administrative process over the user and group lifetimes. When a user's access needs to be changed or removed, updates are made automatically in Active Directory, Exchange, SharePoint, Skype for Business and Windows, as well as any AD-joined systems such as Unix, Linux and Mac OS X.
- **Day-to-day directory management** Simplifies management of:
- Exchange recipients, including mailbox assignment, creation, movement, deletion, permissions and distribution list management
- Groups
- Computers, including shares, printers, local users and groups
- Active Directory, including AD LDS

  Active Roles also includes intuitive interfaces for improving day-to-day administration and help desk operations via both an MMC snap-in and a Web interface.
- **Manage groups and users in a hosted environment** Provides Synchronization Service to operate in hosted environments where accounts from client AD domains are synchronized with host domains. Active Roles enables user and group account management from the client domain to the hosted domain, while also synchronizing attributes and passwords.

The solution uses out-of-the-box connectors to synchronize your on-premises AD accounts to cloud-based services such as Microsoft Office 365, Skype for Business Online and SharePoint Online.

- **Consolidate management points through integration** Complements your existing technology and identity and access management strategy. Simplifies and consolidates management points by ensuring easy integration with many One Identity products, including One Identity Manager, Privileged Password Manager, Authentication Services, Defender, Password Manager, and ChangeAuditor. Active Roles also automates and extends the capabilities of PowerShell, ADSI, SPML, and customizable Web interfaces.

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