Authentication Services ActiveRoles Integration Pack 2.1.x

Administration 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.

Integration Pack Administration Guide
Updated - June 2018
Version - 2.1.x

Contents

1

About this guide

The Authentication Services ActiveRoles Integration Pack Administration Guide is intended for Windows, UNIX, Linux, and Mac system administrators, network administrators, consultants, analysts, and any other IT professionals installing the Integration Pack for the first time.

NOTE: To perform the exercises described in this guide, One Identity assumes you have the necessary permissions to manage users or groups.

The Authentication Services ActiveRoles Integration Pack integrates ActiveRoles Server and Authentication Services. This chapter explains the key features of the Integration Pack and summarizes how it provides value by lowering costs and simplifying management.

Prerequisites

This version of the Authentication Services ActiveRoles Integration Pack has been updated to take advantage of the latest features of both Authentication Services and ActiveRoles Server.

You must install the following software on the computer where you will install the Integration Pack:

- ActiveRoles Server 7.0 or higher, including the Administration Service, Web interface, and ActiveRoles Server console.
- Authentication Services 4.1.0 or higher.

You must install the Integration Pack on a computer running the ActiveRoles Server Administration Service. The Administration Service must be running to make all the necessary changes to ActiveRoles Server.

NOTE: For older versions of ActiveRoles Server or Authentication Services, install the Authentication Services Support Pack for ActiveRoles Server Web Interface 2.0.5.

About ActiveRoles Server

ActiveRoles Server offers a practical approach to automated user provisioning and administration, for maximum security and efficiency. It provides total control of user provisioning and administration for Active Directory.

ActiveRoles Server can help you manage, automatically provision, re-provision and, more importantly, de-provision users quickly, efficiently and securely in Active Directory, AD LDS (formerly ADAM) and beyond. ActiveRoles Server provides strictly enforced role-based security, automated group management, change approval and easy-to-use Web interfaces for self service to achieve practical user and group lifecycle management for the Windows enterprise.

About Authentication Services

Authentication Services integrates native UNIX and Linux authentication and identity subsystems with Active Directory. It eliminates key vulnerabilities and end-user downtime, to minimize risk and lower costs.

At its core Authentication Services provides centralized authentication for Unix, Linux, and Mac systems to Active Directory (AD). With more than 500 current customers and 3 million seats, Authentication Services is the clear market leader in Active Directory integration.

Key Features of the Integration Pack

The Authentication Services ActiveRoles Integration Pack extends the capabilities of the ActiveRoles Server Web interface to include the management of Unix and Linux identities such as Unix-enabled users and groups. You define all management operations by means of the ActiveRoles Server console. Then when managing the users and groups in the Web interface, the defined provisioning and security policies will be followed.

You can also use the ActiveRoles Server change-tracking features, such as management history, to monitor changes made to Unix-related data. ActiveRoles Server gives you a clear log, which documents the changes made to a given identity, such as a Unix-enabled user account. The log includes entries detailing actions performed, success or failure of the actions, as well as which properties were changed.

The Integration Pack provides ActiveRoles policy types that enable automatic provisioning and de-provisioning of Unix account attributes for users and groups. You can incorporate these provisioning actions into custom work flows.

The following sections describe these Integration Pack components:

- Access Templates
- Managed Units

- Policy Types
- Web Interface Extension

NOTE: Refer to Administration Tasks for procedures on how to use these Integration Pack components.

Access Templates

You use standard ActiveRoles Server functionality to delegate management tasks on Unix data. You implement a delegation scheme by applying Access Templates included with the integration pack. For example, to delegate all Unix-related management tasks on Windows user accounts, link the **Users - Modify All Unix Properties** template to a certain organizational unit and select the appropriate group as Trustee. As a result, any member of that group is authorized to perform the tasks on any user account held in that organizational unit.

To locate the Access Templates provided by the Integration Pack, in theActiveRoles Server Console, navigate to **Configuration | Access Templates | Authentication Services Integration v2.1.x**.

The following table summarizes the Access Templates included with the Integration Pack.

Table 1: Access templates included with the integration pack

Access template	Description
Groups-Modify All Unix Properties	Permissions to view and modify these Unix-related properties of Windows groups: • Unix name • Group ID
Users-Modify All Unix Properties	Permissions to view and modify these Unix-related properties of Windows user accounts: • Unix name • User ID • Primary Group ID • Comments (GECOS) • Home Directory • Login Shell

Managed Units

Managed Units allow you to locate the Unix users and groups in your ActiveRoles Server managed environment.

You use standard ActiveRoles Server functionality to provide administrative views of user and group accounts with Unix attributes.

To locate the Managed Units provided by the Integration Pack, in the ActiveRoles Server Console, navigate to **Configuration | Managed Units | Authentication Services Integration v2.1.x**.

The following table summarizes the Managed Units included with the Integration Pack.

Table 2: Managed units included with the integration pack

Managed unit	Description
Unix-enabled groups	Administrative view of all Unix-enabled groups that exist in the domains registered with ActiveRoles Server (managed and unmanaged domains).
Unix-enabled users	Administrative view of all Unix-enabled users that exist in the domains registered with ActiveRoles Server (managed and unmanaged domains)

Policies

Use standard ActiveRoles Server functionality to provide Unix data management policies. You can create custom policy objects based on the policy types provided to allow for automated Unix account provisioning and de-provisioning.

To locate the Policy Types provided by the Integration Pack, in the ActiveRoles Server Console, navigate to **Configuration | Server Configuration | Policy Types | Authentication Services Integration v2.1.x**.

The following table summarizes the Policy Types included with the Integration Pack.

Table 3: Policy types included with the integration pack

Policy type	Description
Deprovision Unix Group	Enables automatic de-provisioning of Unix attributes when group objects are de-provisioned.
Deprovision Unix User	Enables automatic de-provisioning of Unix attributes when users are de-provisioned.
Provision Unix	Enables automatic provisioning of Unix attributes when new group

Policy type	Description
Group	objects are provisioned.
Provision Unix User	Enables automatic provisioning of Unix attributes when new user objects are provisioned

Refer to Administration Tasks for procedures on how to enable automatic provisioning and de-provisioning of Unix account attributes for users and groups.

Web Interface Extensions

The integration pack extends the ActiveRoles Server Web interface to include pages and commands that allow you to perform management tasks.

Tasks specific to Unix user accounts:

- Enable or disable Unix account
- View or modify Unix account properties
- Clear all Unix attributes

Tasks specific to Unix groups:

- Enable or disable Unix group
- View or modify Unix properties
- Clear all Unix attributes

The Integration Pack uses Access Templates to delegate these tasks.

NOTE: The Integration Pack installation process configures the Web interface extensions. To remove the Web interface extensions after the Integration Pack is installed and functioning, click **Customization | Restore** in the Web interface. To regain the Web interface extension functionality, run the ActiveRoles Integration Configuration Wizard from the Start menu.

Deploying the Integration Pack

The Integration Pack consists of a single Windows .msi installer. This installer checks that the necessary prerequisite software is installed on the local machine before it installs the Integration Pack.

There are two steps to deploying the Integration Pack:

1. Install the Integration Pack configuration modules and Web Interface extensions.
2. Configure ActiveRoles Server.

Installing the Integration Pack

To install the Authentication Services ActiveRoles Integration

1. Click `arsqas-2.1.x.msi` file to start the InstallShield Wizard.
2. At the **Welcome** page, click **Next**.
3. At the **Licence Agreement** page, accept the terms in the license and click **Next**.
4. At the **Ready to Install** page, click **Install**.
5. When the InstallShield Wizard completes, leave the **Launch setup wizard** option selected and click **Finish**.

   Wait while the ActiveRoles Integration Configuration Wizard starts.
6. Select the ActiveRoles Server web sites that you want to extend for Authentication Services and click **Continue**.

   NOTE: You can manage your ActiveRoles Server web sites using standard ActiveRoles Server functionality. From the **Start** menu, navigate to **All Programs | Quest Software | Authentication Services ActiveRoles Integration | ActiveRoles Integration Configuration Wizard** to start the wizard which will help you configure web sites including newly created web sites for the ActiveRoles Server web interface.

NOTE: Every time you create and configure a new web site for the ActiveRoles Server Web Interface, you must run the ActiveRoles Integration Configuration Wizard.

7. When the configuration setup wizard completes, click **Restart ActiveRoles Now**.
8. When it becomes active, click the **Close** button and wait for a minute while ActiveRoles Server loads the startup information.

   NOTE: Once the service restarts, wait a few minutes before you open the ActiveRoles Server console.

9. There are two ways to start the ActiveRoles Server Console:

   a. From the **Start** menu, navigate to **All Programs | Quest Software | ActiveRoles Server | ActiveRoles Server Console**.

   -OR-

   b. You can also access the ActiveRoles Server Console from the Authentication Services Control Center. Navigate to **Start | All Programs | Quest Software | Quest Authentication Services | Authentication Services Control Center**.

Once the console is open, look for the **Authentication Services Integration Pack v2.1.x** folder under these nodes:

- Access Templates
- Managed Units
- Policies | Administration
- Script Modules
- Server Configuration | Policy Types
- Applications

Upgrading the Integration Pack

The Integration pack is not meant to be upgraded. Each version of the Integration Pack installs its policy objects, access templates, scripts and managed units into a version-specific container to isolate the data objects for each version. However, the Integration Pack shares Web interface modifications between all versions. For this reason, One Identity recommends that you uninstall the previous version before installing the new version.

When upgrading from one version of the Integration Pack to another, any customizations to Integration Pack data objects will be lost. To preserve Integration Pack customizations, One Identity recommends that you backup the modified objects before you uninstall the previous version. That is, copy or move the Access Templates, Policy Objects, Script Modules, or Virtual Attributes created by the old version of the Authentication Services Support Pack for ActiveRoles Server Web Interface to a new location using ActiveRoles

Server management console. These objects are located in the ActiveRoles Server configuration container.

Uninstalling

To uninstall the Authentication Services ActiveRoles Integration

1. Navigate to the **Control Panel | Programs | Programs and Features**.
2. Right-click **Authentication Services ActiveRoles Integration** and choose **uninstall**.
3. Click **Yes** on the Programs and Features dialog to confirm your decision.
4. When prompted,
    a. Click **Yes** to remove the ActiveRoles Server configuration.

       This removes the server and Web interface extensions from ActiveRoles Server.

    b. Click **No** to uninstall the Integration Pack but retain the ActiveRoles Server configuration.

       This leaves the ActiveRoles Server integration extensions in the console.

3

Administration Tasks

The Integration Pack enables you to automate the provisioning and de-provisioning of UNIX account attributes. You can also delegate rights to manage Unix accounts that reside in Active Directory. Managed Units allow you to locate the Unix users and groups in your ActiveRoles Server managed environment. This chapter explains how to accomplish these tasks with the Integration Pack.

To access the ActiveRoles Server Console

1. From the **Start** menu, navigate to **Program Files | Quest Software | ActiveRoles Server | ActiveRoles Server Console**.

Provisioning Unix Users

You can automatically Unix-enable users that are provisioned in ActiveRoles Server.

To automatically Unix-enable users

1. From the ActiveRoles Server Console, navigate to **Configuration | Policies | Administration**.
2. From the **Action** menu, select **New | Provisioning Policy**.
3. When the **New Provisioning Policy Object Wizard** starts, click **Next**.
4. On the **Name and Description** page, enter `Unix-enable new users` in the **Name** box and click **Next**.
5. On the **Policy to Configure** page, locate the Authentication Services Integration Pack and select the **Provision Unix User** policy type and click **Next**.
6. On the **Policy Parameters** page, select the **AutoUnixEnable** parameter and click **Edit**.
7. On the **Edit Parameter** page, open the **Value:** drop-down menu, select **True** and click **OK**.
8. On the **Policy Parameters** page, click **Next**.
9. On the **Enforce Policy** page, click the **Add** button.

10. On the **Select Objects** page, click **Browse**, select **Active Directory** (to apply this policy to all new Active Directory users), and click **OK**.
11. On the **Select Objects** page, select the **Active Directory** item at the top of the list, click **Add** and then click **OK**.
12. On the **Enforce Policy** page, click **Next**.
13. Click **Finish** to create the new policy object.
14. On the ActiveRoles Server dialog, click **OK** to return to the ActiveRoles Server Console.

    When you provision a new user account, the Integration Pack automatically Unix-enables that account. That is, it populates the user's Unix attributes.

Deleting Policy Objects

To delete policy objects

1. From the ActiveRoles Server Console, navigate to **Configuration | Policies | Administration**.
2. Right-click a Policy Object and choose **Policy Scope**.

   This displays the links in which the Policy Object occurs.
3. Select the link, click **Remove**, **Yes**, **OK**, and then **OK** again.

   This deletes the links to the policy object.
4. Right-click the policy object and click **Delete**.
5. Click **Yes** to confirm your decision.

De-provisioning Unix Users

You can automatically disable Unix accounts when users are de-provisioned in ActiveRoles Server.

To de-provision Unix users

1. From the ActiveRoles Server Console, navigate to **Configuration | Policies | Administration**.
2. From the **Action** menu, select **New | Deprovisioning Policy**.
3. When the New Deprovisioning Policy Object Wizard starts, click **Next**.
4. On the **Name and Description** page, enter *Disable Unix accounts for deprovisioned users* in the **Name** box and click **Next**.
5. On the **Policy to Configure** page, locate the Authentication Services Integration Pack and select the **Deprovision Unix User** policy type and click **Next**.

6. On the **Policy Parameters** page, select the **UnixDisable** parameter and click **Edit**.
7. On the **Edit Parameter** page, open the **Value:** drop-down menu, select **True** and click **OK**.
8. On the **Policy Parameters** page, select the **PrimaryGidNumber** parameter and click **Edit**.
9. On the **Edit Parameter** page, specify an integer value for the Primary GID number and click **OK**.
10. On the **Policy Parameters** page, click **Next**.
11. On the **Enforce Policy** page, click the **Add** button.
12. On the **Select Objects** page, click **Browse**, select **Active Directory** (to apply this policy to all new users), and click **OK**.
13. On the **Select Objects** page, select the **Active Directory** item at the top of the list, click **Add** and then click **OK**.
14. On the **Enforce Policy** page, click **Next**.
15. Click **Finish** to create the new policy object and close the wizard.

    When you de-provision a user account, the Integration Pack automatically disables the user's Unix attributes.

Provisioning Unix Groups

To automatically Unix-enable groups

1. From the ActiveRoles Server Console, navigate to **Configuration | Policies | Administration**.
2. From the **Action** menu, select **New | Provisioning Policy**.
3. When the New Provisioning Policy Object Wizard starts, click **Next**.
4. On the **Name and Description** page, enter *Unix-enable new groups* in the **Name** box and click **Next**.
5. On the **Policy to Configure** page, locate the Authentication Services Integration Pack and select the **Provision Unix Group** policy type and click **Next**.
6. On the **Policy Parameters** page, select the **AutoUnixEnable** parameter and click **Edit**.
7. On the **Edit Parameter** page, open the **Value:** drop-down menu, select **True** and click **OK**.
8. On the **Policy Parameters** page, click **Next**.
9. On the **Enforce Policy** page, click the **Add** button.
10. On the **Select Objects** page, click **Browse**, select **Active Directory** (to apply this policy to all new Active Directory groups), and click **OK**.

11. On the **Select Objects** page, select the **Active Directory** item at the top of the list, click **Add** and then click **OK**.
12. On the **Enforce Policy** page, click **Next**.
13. Click **Finish** to create the new policy object.
14. On the ActiveRoles Server dialog, click **OK** to return to the ActiveRoles Server Console.

    When you provision a new group account, the Integration Pack automatically Unix-enables the users associated with that account. That is, it populates the user's Unix attributes.

De-provisioning Groups

You can automatically disable Unix accounts when groups are de-provisioned in ActiveRoles Server.

To de-provision Unix groups

1. From the ActiveRoles Server Console, navigate to **Configuration | Policies | Administration**.
2. From the **Action** menu, select **New | Deprovisioning Policy**.
3. When the New Deprovisioning Policy Object Wizard starts, click **Next**.
4. On the **Name and Description** page, enter *Disable Unix accounts for deprovisioned groups* in the Name box and click **Next**.
5. On the **Policy to Configure** page, locate the Authentication Services Integration Pack and select the **Deprovision Unix Group** policy type and click **Next**.
6. On the **Policy Parameters** page, select the **UnixDisable** parameter and click **Edit**.
7. On the **Edit Parameter** page, open the Value: drop-down menu, select **True** and click **OK**.
8. On the **Policy Parameters** page, click **Next**.
9. On the **Enforce Policy** page, click the **Add** button.
10. On the **Select Objects** page, click **Browse**, select **Active Directory** (to apply this policy to all new groups), and then click **OK**.
11. On the **Select Objects** page, select the **Active Directory** item at the top of the list, click **Add** and click **OK**.
12. On the **Enforce Policy** page, click **Next**.
13. Click **Finish** to create the new policy object and close the wizard.

When you de-provision a group account, the Integration Pack automatically clears the group's Unix attributes rendering it Unix-disabled.

Delegating Rights to Manage Unix Objects

Use Access Templates to grant permissions to users and groups. When you add a user to an Access Template, you add all the attributes and permissions of that template to that user. When you apply Access Templates to a folder, you configure the permission settings to propagate from the folder to its child objects, down the directory structure.

You implement a delegation scheme by applying Access Templates included with the Integration Pack. For example, to delegate all Unix-related management tasks on Windows user accounts, link the **Users - Modify All Unix Properties** Access Template to a certain organizational unit and select the appropriate group as **Trustee**. As a result, any member of that group is authorized to perform the tasks on any user account held in that organizational unit.

To delegate rights to manage Unix objects

1. From the ActiveRoles Server Console, navigate to **Active Directory**.
2. From the **Action** menu, choose **Delegate Control**
3. On the **Access Template links** page, click **Add**.
4. When the Delegation of Control Wizard starts, click **Next**.

   The Delegation of Control Wizards helps you delegate control of directory objects. Grant permission to manage users, groups, computers, organizational units, and other objects administered with ActiveRoles Server.
5. On the **Users or Groups** page, click **Add**
6. On the **Select Objects** page, click the link to display the objects.
7. Select objects, click **Add** and then **OK**.
8. On the **Users or Groups** page, click **Next**.
9. On the **Access Templates** page, expand **Authentication Services Integration v2.x** and select **Group** or **User** or both and click **Next**.
10. On the **Inheritance Options** page, specify whether you want child objects to inherit the permission settings from the selected Access Templates and click **Next**.
11. On the **Permissions Propagation** page, leave the **Propagate permissions to Active Directory** option unselected and click **Next**.
12. On the "Complete" page, click **Finish** if you are satisfied with the delegation of control.
13. On the **Access Template links** page, click **OK** to return to the console

Users or groups with delegated rights to manage Unix objects can enable, disable, or change Unix attributes on users and groups in either the ActiveRoles Server Console or the Web interface.

NOTE: Each delegated user must have read access to the application configuration.

Locating Unix Objects

Managed Units allow you to locate the Unix users and groups in your ActiveRoles Server managed environment.

To locate Unix objects

1. From the ActiveRoles Server Console, navigate to **Configuration | Managed Units | Authentication Services Integration v2.x**.
2. Right-click either **Unix-enabled Groups** or **Unix-enabled Users** and choose **Find...**.
3. You use standard ActiveRoles Server functionality to search for objects of different types. For details on using the Find Users, Contacts, and Group dialog, open the **Help** menu, choose **Help Topics**, and open the **Finding Objects** topic.

Using the Web Interface Extensions

Authentication Services provides Microsoft Management Console (MMC) extensions that support the ActiveRoles Server web interface allowing you to:

- Enable, disable, or clear the Unix properties for a Windows user account
- View or modify Unix-related properties of a Windows user account
- Enable or clear the Unix group properties for a Windows group
- View or modify Unix-related properties of a Windows group

After you install the Integration Pack, you must publish the Web interface extensions.

Configure New Web Sites for the Web Interface

Every time you create and configure a new Web site for the ActiveRoles Server Web Interface, you must run the ActiveRoles Integration Configuration Wizard.

To configure new Web sites for the Web interface

1. From the **Start** menu, navigate to **All Programs | Quest Software | Authentication Service ActiveRoles Integration | ActiveRoles Integration Configuration Wizard** to start a wizard that will help you configure newly created Web sites for the ActiveRoles Server Web interface.
2. When the configuration setup wizard completes, click **Restart ActiveRoles Now**.
3. When it becomes active, click the **Close** button and wait for a minute while ActiveRoles Server loads the startup information.

NOTE: Once the service restarts, wait a few minutes before you open the ActiveRoles Server console.

Publish Web Interface Extensions

Installing and then publishing the Web interface extensions adds a number of pages and commands to the ActiveRoles Server Web interface, enabling the management of Unix-specific information in Active Directory.

These pages and commands include:

- Unix Properties on User Account.

  View or modify Unix-related properties of a Windows user account.

- Unix Properties on Group.

  View or modify Unix-related properties of a Windows group.

To publish Web interface extensions

1. Start the ActiveRoles Server Web interface in Windows Internet Explorer.

   NOTE: The PROD.NAME only works with Internet Explorer.

   a. Start Internet Explorer.

   b. Navigate to the following URL:

      `http://<IP Address>/ARServerAdmin`

   c. At the login screen, enter your user name and password.

2. From the **Customization** menu on the main page of the ActiveRoles Server Web Interface, choose the **Reload** option.

   NOTE: If you do not see the **Customization** link on the ActiveRoles Server Web interface on Windows 2008 R2, run the browser with elevated privileges.

Unix-Enable a User

You can manage the Unix-specific information for a Windows user account from the ActiveRoles Server web interface.

To Unix-enable a user

1. Click the **Directory Management** link on the home page of the ActiveRoles Server.
2. From the ActiveRoles Server directory tree, navigate to **Active Directory** and select the **Users** folder under your managed domain.
3. In the details pane, click a user name link.
4. From the drop-down menu, select **Unix Properties**.
5. On the **Unix Account** tab, select the **Unix Enabled** option.

6. Modify any of the Unix-related properties.

   The *UID Number* is the unique identifier for a Unix user. Ideally, each Windows user is assigned a unique UID number. By default the Integration Pack generates a unique ID automatically. If you change the User ID, the Integration Pack checks to ensure the specified value is unique among Unix-enabled users.

   NOTE: The **Primary Group** box displays the Domain Name of the group corresponding to the Primary Group ID. You can click **Change** to browse Unix-enabled groups to find the Primary Group by name.

7. Click **Save** to commit your changes.

Unix-Disable a User

To Unix-disable a user

1. Click the **Directory Management** link on the home page of the ActiveRoles Server.
2. From the ActiveRoles Server directory tree, navigate to **Active Directory** and select the **Users** folder under your managed domain.
3. In the details pane, click a user name link.
4. From the drop-down menu, select **Unix Properties**.
5. On the **Unix Account** tab, deselect the **Unix Enabled** option.
6. Click **Save** to commit your changes.

Unix-disabling a user changes his login shell to `bin/false`.

Clear Unix Attributes

After you Unix-disable a user, you may want to clear that user's Unix attributes.

To clear Unix attributes

1. Click the **Directory Management** link on the home page of the ActiveRoles Server.
2. From the ActiveRoles Server directory tree, navigate to **Active Directory** and select the **Users** folder under your managed domain.
3. In the details pane, click a user name link.
4. From the drop-down menu, select **Unix Properties**.
5. Clear the text of each Unix-related property and click **Save**.

NOTE: When you click **Save**, if there is a Unix property in any of the fields, the Integration Pack makes no changes to the user's Unix properties.

Unix-Enable a Group

You can manage the Unix-specific information for a Windows user account from the ActiveRoles Server web interface.

To Unix-enable a group

1. Click the **Directory Management** link on the home page of the ActiveRoles Server.
2. From the ActiveRoles Server directory tree, navigate to **Active Directory** and select the **Users** folder under your managed domain.
3. In the details pane, click a group name link.
4. From the drop-down menu, select **Unix Properties**.
5. On the **Unix Account** tab, select the **Unix Enabled** option.
6. Modify any of the Unix-related properties.

   The *GID Number* is the unique identifier for a Unix group. Ideally, each Windows group is assigned a unique Group ID number. By default the Integration Pack generates a unique ID automatically. If you change the GID Number, the Integration Pack checks to ensure the specified value is unique among Unix-enabled groups.
7. Click **Save** to commit your changes.

Unix-Disable a Group

To Unix-disable a group

1. Click the **Directory Management** link on the home page of the ActiveRoles Server.
2. From the ActiveRoles Server directory tree, navigate to **Active Directory** and select the **Users** folder under your managed domain.
3. In the details pane, click a group name link.
4. From the drop-down menu, select **Unix Properties**.
5. On the **Unix Account** tab, deselect the **Unix Enabled** option.
6. Click **Save** to commit your changes.

Unix-disabling a group clears the GID.

Troubleshooting

To help you troubleshoot, One Identity recommends the following resolutions to some of the common problems you might encounter as you deploy and use the Authentication Services ActiveRoles Integration Pack .

No Application Configuration Found for Authentication Services

The Integration Pack must have an Authentication Services Application Configuration available for each managed forest. During the Authentication Services Integration Setup for ActiveRoles Server, if you do not have an application configuration in list of domains, the ActiveRoles Integration Configuration Wizard displays an error message that says, "No Application Configuration Found for Authentication Services".

To make the Authentication Services Application Configuration available to the Integration Pack

1. Using standard ActiveRoles Server functionality, add the Active Directory domain in which the Authentication Services Application Configuration resides to the list of domains managed by ActiveRoles Server.

   -OR-

2. Delete the Authentication Services Application Configuration from its current location and re-create it in the domain where ActiveRoles Server resides.

Unix Properties Menu Not Visible in Web Interface

After installing the Integration Pack, whenever you select a user or group in the ActiveRoles Server Web interface, a new menu entry appears called **Unix Properties**. If

you do not see this menu entry, ensure that you configured the web site for Authentication Services ActiveRoles Integration.

To configured the web site for Authentication Services ActiveRoles Integration

1. From the **Start** menu on the machine where the Integration Pack is installed, navigate to **All Programs | Quest Software | Authentication Services ActiveRoles Integration | ActiveRoles Integration Configuration Wizard** to start the wizard.

If you still do not see the Unix Properties extension

1. Start the ActiveRoles Server Web interface in Windows Internet Explorer.
2. From the **Customization** menu on the main page of the ActiveRoles Server Web Interface, choose the **Reload** option.

The Customization Link is Not Available in Web Interface

To see the **Customization** link on the ActiveRoles Server web interface on Windows 2008 R2, run the browser with elevated privileges.

Web Interface Extension Changes Are Not Saved

The Web interface extensions for the Integration Pack are based on ActiveRoles virtual attributes. This allows the Unix attributes to map to the correct LDAP attributes in Active Directory based on the Authentication Services configuration. However, if the virtual attribute maps to a read-only LDAP attribute then any changes to the virtual attribute will not be propagated to the directory. User and group objects from unmanaged domains are read-only.

Restoring Integration Pack Web Interface Configuration

To restore the Authentication Services ActiveRoles Integration extensions to the Web interface, run ActiveRoles Integration Configuration Wizard from the **Start** menu on the ActiveRoles Server. This tool allows you to re-configure the Web interface extensions.

CAUTION: Do not select Customization | Restore Default in the ActiveRoles Server web interface unless you want to uninstall the Integration Pack. If you select Customization | Restore Defaults, all extensions are removed and the web interface is reset to the defaults.

Repairing Integration Scripts

If you modify an Authentication Services ActiveRoles Integration script and it becomes corrupt, causing errors when it is run, you can repair it.

To repair integration scripts

1. From the command line, run

   ```
   "C:\Program Files\Quest Software \Authentication Services Integration
   2.1.x\SetupUi.exe" -force
   ```

Delegated User Unable to Modify Unix Attributes

To be able to manage Unix users within his delegated domain, you must assign a delegated user read permissions to the Application Configuration.

Problem: Even though a user or group has a **Unix Account** tab, when you select the tab, the Unix attributes do not display. Instead you see a message that says, "The Configuration Setting for Authentication Services could not be found in Active Directory" even though there is a configuration in the forest. At times a user is delegated permission to manage Unix attributes for users and/or groups within an organizational unit but that user does not have *read* access to other containers in the domain.

Solution: You must delegate permission to the user by means of ActiveRoles Server so he can list and read the Authentication Services Application Configuration. For more information about the Authentication Services Application Configuration see **Configure Active Directory for Authentication Services** in *Authentication Services Installation Guide*.

About us

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

Contacting us

For sales 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 at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Index

T

U

W