Security Manager

GE VERNOVA

Contents

Copyright Digital, part of GE Vernova

THIS DOCUMENT AND ITS CONTENTS ARE PROVIDED "AS IS," WITH NO REPRESENTATION OR WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF DESIGN, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. ALL OTHER LIABILITY ARISING FROM RELIANCE UPON ANY INFORMATION CONTAINED HEREIN IS EXPRESSLY DISCLAIMED.

Access to and use of the software described in this document is conditioned on acceptance of the End User License Agreement and compliance with its terms.

Chapter 1

Overview

Topics:

About Security Manager

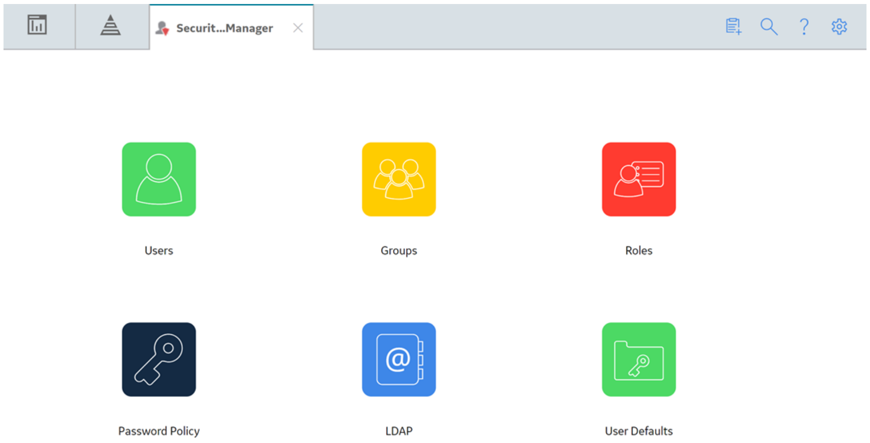
Security Users and Security Groups serve as the foundation for the APM security model.

- Security Users represent the individuals who will be accessing APM.
- Security Users can be associated with Security Groups, which grant Security Users the permissions needed to perform their roles within APM. You can use Security Groups to group together Security Users with similar roles and give all those users access to the same features.

Access the Security Manager Page

Procedure

In the **Applications** menu, navigate to **ADMIN** > **Security Manager**.
The **Security Manager** page appears.



Chapter 2

Users

Topics:

About Security Users

A Security User is an individual in your organization who has a user account for accessing APM. An APM Security User account stores the ID and password for the user, which are used to authenticate the Security User when he or she logs in, and identifying information including the name, contact information, and job details.

Creating Security User accounts is the first step in configuring system security. After you have created Security Users, you can assign those Security Users to Security Groups, organizing Security Users according to their roles within the system.

After you set up Security Users and Groups, you can assign data permissions for those Security Users and Groups.

Each Security User account is actually a record that belongs to the Security User family. When you create a Security User, three things happen:

- A Security User record is created.
- A corresponding Human Resource record is created.
- A link between the Security User record and the Human Resource record is created using the Is a User relationship family.

Because Security User records are actual records in APM, they can be searched, queried, viewed, and modified just like any other type of record.

Access the Security Users Page

Procedure

In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Users**.
The **Security Users** page appears.

Security Users Workflow

Before You Begin

If needed, create the sites, groups, and roles that you want to assign to the user that you will create.

Steps

1. Create a Security User.
2. As needed, assign roles to the Security User.
3. As needed, assign groups to the Security User.

Create a Security User

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Users**.

2. In the left pane, select +.
   The **New User** workspace appears, displaying a blank Security User datasheet.
3. If you want the Security User to be prompted to change password after login, select the **Must Change Password** check box.
4. If you want the Security User to have access to all APM features and functionality, select the **Super User** check box.
5. In the workspace for the new Security User, select the **Sites** tab.
   The **Sites** section appears.
6. In the **Sites** section, select +.
   The **Assign Sites** window appears, displaying the available sites.
7. Beside each site to which you want to assign the Security User, select the check box, and then select **Update**.

   Note: You can assign multiple sites to a Security User.

   The updated Security User properties are saved, the **Assign Sites** window closes, and the assigned sites appear in the **Sites** section.
8. Select the **Details** tab.
   The **Details** section appears.
9. As needed, enter values in the available fields.

   Important:

   After the appropriate sites have been assigned to the Security User, one site must be selected as the default site. In the **Details** section for the Security User, ensure that you have selected the appropriate option in the **Default Site** box.
10. Select 💾.
    The Security User is saved, and added automatically to the Everyone Security Group.

    Note: If you want to include an image for the new Security User, you can do so using the **Upload Photo** button that appears after you save the user.

Security User Records

A Security User record contains information related to each user who has been granted access to APM. The table describes the baseline state and behavior of the fields.

Field	Data Type	Description	Behavior and Usage
Active	Boolean	The field indicates whether the Security User account is active.	If selected, the Security User account is active.
Address	Character	The address of the Security User.	You can enter text to define this value manually.
Area of Responsibility	Character	The area of responsibility assigned to the Security User.	You can enter text to define this value manually.
Business Unit	Character	The business unit to which the Security User belongs.	You can enter text to define this value manually.
City	Character	The city where the Security User resides.	You can enter text to define this value manually.

Field	Data Type	Description	Behavior and Usage
Comment	Character	Additional information on the user, if any.	You can enter text to define this value manually.
Company	Character	The company to which the Security User belongs.	You can enter text to define this value manually.
Country	Character	The country where the Security User resides.	You can enter text to define this value manually.
Culture	Character	The field identifies the preferred culture of the Security User. This setting determines the time zone and number formats that are displayed when the user logs in to APM.	While creating the user account for a Security User, by default, the **Culture** drop-down list box displays the value that is selected in the **Default Culture** drop-down list box of the **User Defaults** page. You can change the default culture setting by selecting one of the options available in the **Culture** drop-down list box.
Default Site	Character	The default site assigned to the Security User.	While creating the user account for a Security User, by default, the **Default Site** drop-down list box displays the value that is selected in the **Default Site** drop-down list box of the **User Defaults** page. You can change the default site by selecting one of the options available in the **Default Site** drop-down list box. **Important:** A default site must be selected. For more information, see the Assign Sites to a Security User topic.
Department	Character	The department to which the Security User belongs.	You can enter text to define this value manually.
Domain	Character	The domain associated with the Security User.	You can enter text to define this value manually.
Email	Character	The Email ID of the Security User.	You can enter text to define this value manually.
Facility	Character	The facility to which the Security User belongs.	You can enter text to define this value manually.
Fax	Numeric	The fax number of the Security User.	You can enter text to define this value manually.

Field	Data Type	Description	Behavior and Usage
First Name	Character	The first name of the Security User.	You can enter text to define this value manually.
Job Title	Character	The job title given to the Security User.	You can enter text to define this value manually.
Language	Character	The field identifies the preferred language of the Security User. This setting determines the language that is displayed when the user logs in to APM.	While creating the user account for a Security User, by default, the **Language** drop-down list box displays the value that is selected in the **Default Language** drop-down list box of the **User Defaults** page. You can change the default language by selecting one of the options available in the **Language** drop-down list box.
Last Name	Character	The last name of the Security User.	You can enter text to define this value manually.
Locked	Boolean	Indicates whether the Security User account is locked. If a Security User account is locked, the Security User will not be able to log in. **Note:** If a Security User account is created when the LDAP synchronization process is run, the **Locked** check box does not appear in the corresponding Security User record.	If a Security User account is locked, the Security User will not be able to log in. If a Security User repeatedly attempts to log in using an incorrect password, the user account of the Security User is locked. The account will be unlocked automatically after 20 minutes. If needed, an administrative user can manually unlock an account by clearing the **Locked** check box.
Middle Initial	Character	The middle name or initial of the Security User.	You can enter text to define this value manually.
Must Change Password	Boolean	Indicates whether the password for the Security User account must be changed before the Security User can log in.	If selected, the password for the Security User account must be changed before the Security User can log in.
Password	Character	Must meet the criteria that is defined in the password policy.	This field is required, and the value must be unique among APM Security Users. You will be asked to confirm your password.
Phone	Numeric	The phone number for the Security User.	You can enter text to define this value manually.

Field	Data Type	Description	Behavior and Usage
Postal Code	Numeric	The postal code for the Security User.	You can enter text to define this value manually.
Query Privilege	Character	Specifies restrictions that apply when this user is working with queries.	This field is disabled when the user is a Super User and the query privilege is set to unrestricted. You can select from the following options: • **Unrestricted:** The Security User can save new or modified queries without restriction. • **Restricted By Timeout Limit:** The Security User can save new and modified queries only if the query results are returned within a specified amount of time. • **Execute Only:** The Security User cannot create or modify queries. Instead, he or she can only view the result of existing queries.
State	Character	The state where the Security User resides.	You can enter text to define this value manually.
Super User	Boolean	Indicates whether the Security User has Super User privileges.	If selected, the Security User has Super User privileges.
Timezone	Character	The time zone the user expects to see in the APM. It is the time zone set up on the user record in the database. Note that this is not the browser or server time zone.	You can select any available time zone. **Note:** • While creating the user account for a Security User, by default, the **Timezone** drop-down list box displays the value that is selected in the **Default time zone assigned to a new user** drop-down list box of the **User Defaults** page. You can change the default timezone by selecting one of the options available in the **Timezone** drop-down list box.

Field	Data Type	Description	Behavior and Usage
UOM Conversion Set	Character	Indicates the units associated with the value(s) stored in that field.	While creating the user account for a Security User, by default, the **UOM Conversion Set** drop-down list box displays the value that is selected in the **Default UOM Conversion Set** drop-down list box of the **User Defaults** page. You can change the default UOM conversion set by selecting one of the options available in the **UOM Conversion Set** drop-down list box. The following Units of Measurement (UOM) conversion sets are available for the user: • **None**: Default Conversion Set. • **API RBI Connector**: API RBI Connector Conversion set for API RBI Metric Users. • **Metric**: Metric conversion set.
User ID	Character	The ID for the Security User.	This field is required, and the value must be unique.

Copy an Existing Security User

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Users**.
2. In the left pane, select the Security User that you want to copy.
   The workspace for the selected Security User appears, displaying the corresponding Security User form.
3. In the workspace heading, select .
   The Security User is copied, and the properties for the new Security User appear in a form. The new Security User belongs to all Security Groups to which the template Security User belongs.

   All values from the template Security User are copied to the new Security User, except the following:

   - First Name
   - User ID
   - Middle Initial
   - Password

- Last Name
- Email

4. Enter or modify the values in the available fields.
5. Select 💾.
   The Security User is saved.

Modify Security User Properties

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Users**.
2. In the left pane, select the Security User whose properties you want to modify.
   The workspace for the selected Security User appears, displaying the corresponding Security User form.
3. As needed, modify the available values, and then select 💾.
   The updated Security User properties are saved.

Activate or Deactivate a Security User

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Users**.
2. In the left pane, select the Security User that you want to activate or deactivate.
   The workspace for the selected Security User appears, displaying the corresponding Security User form.
3. Select or clear the **Active** check box as necessary, and then select 💾.
   Depending on your selection, the Security User is activated or deactivated.

Assign Groups to a Security User

Before You Begin

- Create a Security User
- Create a Security Group

About This Task

This topic describes how to assign multiple Security Groups to a Security User on the **Security Users** page. You can also assign a Security Group to multiple Security Users on the Security Groups page.

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Users**.
2. In the left pane, select the Security User that you want to add to the Security Group.
   The workspace for the selected Security User appears.
3. In the workspace for the selected Security User, select the **Groups** tab.
   The **Groups** section appears.

4. Select +.
   The **Assign Groups** window appears, displaying the available Security Groups.
5. Beside each Security Group to which you want to assign the Security User, select the check box.
6. Select 💾.
   The updated Security User properties are saved.

Remove Groups from a Security User

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Users**.
2. In the left pane, select the Security User whose Security Groups you want to remove.
   The workspace for the selected Security User appears.
3. In the workspace for the selected Security User, select the **Groups** tab.
   The **Groups** section appears.
4. Beside each Security Group that you want to remove, select the check box.
5. Select 🗑.
   The Security Group is no longer assigned to the Security User.
6. Select 💾.
   The updated Security User properties are saved.

Assign Sites to a Security User

Before You Begin

- Create a Security User

About This Task

This topic describes how to assign multiple sites to a Security User on the **Security Users** page. You can assign a site to multiple Security Users on the **Configuration Manager Sites** page.

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Users**.
2. In the left pane, select the Security User to whom you want to assign sites.
   The workspace for the selected Security User appears, displaying the **Details** section.
3. In the workspace for the selected Security User, select the **Sites** tab.
   The **Sites** section appears.
4. Select +.
   The **Assign Sites** window appears, displaying the available sites.
5. Beside each site to which you want to assign the Security User, select the check box, and then select **Update**.

   Note: You can assign multiple sites to a Security User.

   The updated Security User properties are saved, the **Assign Sites** window closes, and the assigned sites appear in the **Sites** section.

   Important:

After the appropriate sites have been assigned to the Security User, one site must be selected as the default site. In the **Details** section for the Security User, ensure that you have selected the appropriate option in the **Default Site** box.

Remove Sites from a Security User

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Users**.
2. In the left pane, select the Security User for which you want to remove sites.
   The workspace for the selected Security User appears.
3. In the workspace for the selected Security User, select the **Sites** tab.
   The **Sites** section appears.
4. Beside each site that you want to remove from the Security User, select the check box.
5. Select 🗑.
   The site is removed from the Security User.
6. Select 💾.
   The updated Security User properties are saved.

Assign Roles to a Security User

Before You Begin

- Create Security Roles
- Create a Security User

About This Task

This topic describes how to assign multiple Security Roles to a Security User on the **Security Users** page. You can assign a Security Role to multiple Security Users on the **Security Roles** page.

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Users**.
2. In the left pane, select the Security User to whom you want to assign the Security Role.
   The workspace for the selected Security User appears.
3. In the workspace for the selected Security User, select the **Roles** tab.
   The **Roles** section appears.
4. Select +.
   The **Assign Roles** window appears, displaying the available Security Roles.
5. Beside each Security Role that you want to assign to the Security User, select the check box.
6. Select 💾.
   The updated Security User properties are saved.

Remove Roles from a Security User

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Users**.
2. In the left pane, select the Security User for which you want to remove Security Roles.
   The workspace for the selected Security User appears.
3. In the workspace for the selected Security User, select the **Roles** tab.
   The **Roles** section appears.
4. Beside each Security Role that you want to remove, select the check box.
5. Select 🗑.
   The selected Security Roles are removed.
6. Select 💾.
   The updated Security User properties are saved.

Chapter 3

Groups

Topics:

About Security Groups

A Security Group is a group of APM Security Users who share similar responsibilities or perform similar tasks in APM. After you create a Security Group, you can assign Security Users to the Security Group. Any Security User who is a member of a given Security Group will be granted the permissions defined for that Security Group. Security Groups can streamline the assignment of Security User permissions and help you organize Security Users according to their roles in the system.

Note: Each Security User must be a member of at least one Security Group.

Security Groups serve two main purposes:

- They can have functional permissions, which control member access to certain features in the system.
- They can be associated with data permissions so that you can assign the same permissions to a group of similar Security Users.

Some of the Security Groups that are included in the baseline APM database have specific functional permissions associated with them that control access to certain features of the system. For example, members of the MI PROACT Administrator Security Group will have access to the Administrative Tools in RCA. Any user who is not a member of the MI PROACT Administrator Security Group will not be able to access the RCA Administrative Tools.

Note: Functional permissions are typically defined in the APM code and cannot be modified.

Data permissions determine each member's ability to access data. Data permissions are provided for many of the baseline APM Security Groups, and can also be defined for any Security Groups that you create. Data permissions that are associated with baseline Security Groups can be modified.

Data permissions are spread down from Security Groups to Security subgroups. A Security Group should be given the lowest level of permissions allowed for any single member of that group. You can expand Security User permissions for individual Security Group members, but you cannot revoke from a Security User the permissions that are granted through any of its Security Groups. The more role-specific and task-specific you make your Security Groups, the easier it will be to define permissions for all of its members.

About the Everyone Security Group

The Everyone Security Group is included in the baseline APM database. When you create a new Security User in the Security Manager, that user will be assigned automatically to the Everyone Security Group. While membership in the Everyone Group is not required (i.e., Security Users can be removed from this Security Group), we recommend that you accept this default group assignment and keep all Security Users assigned to the Everyone Security Group. Membership in the Everyone Security Group meets the basic requirements needed to access the APM system and provides users with View-level privileges to the APM Foundation families (e.g., Equipment and Functional Location).

The following table illustrates the families to which members of the Everyone Security Group have permissions.

Family	Permissions
Entity Families	
Asset Group	View
Asset Group Tag	View

Family	Permissions
Asset Hierarchy	View
Components	View
Equipment	View
Family Policy	View
Finding	View
Functional Location	View
Group Definition	View
Human Resource	View
Inspection	View
Inspection Profile	View
Inspection Team Member	View
MI Applications	View
Observation	View
Personnel Certification	View
Recommendation	View
Reference Document	View
Resource Role	View
Security Group	View
Security User	View
Taxonomy References	View
Technical Characteristics	View
Virtual Asset	View
Work History	View
Work History Detail	View
Relationship Families	
Equipment Has Equipment	View
Functional Location Has Equipment	View
Functional Location Has Functional Location(s)	View
Group Assignment	View
Group Has Asset	View
Has Asset Group Tag	View
Has Certifications	View
Has Event Detail	View

Family	Permissions
Has Findings	View
Has Inspection Profile	View
Has Inspections	View
Has Observations	View
Has Reference Documents	View
Has Roles	View
Has Sub-Inspection	View
Has Taxonomy Hierarchy Element	View
Has Taxonomy Mapping	View
Has Team Member	View
Has Work History	View
Is a User	View
User Assignment	View

Access the Security Groups Page

Procedure

In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Groups**.
The **Security Groups** page appears.

Create a Security Group

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Groups**.
2. In the left pane, select +.
   The **New Group** workspace appears, displaying a blank Security Group form.

   -or-

   If you want to create a new subgroup, in the left pane, select the Security Group to which you want to add the subgroup, and then select **New Group**.

   The **New Group** workspace appears, displaying a blank Security Group form.
3. As needed, enter values in the available fields.
4. Select 💾.
   The Security Group is created. When you create a Security Group, a corresponding folder is created at the following Catalog location: `Public/Meridium/Security Groups/<Group ID>`.

Security Group Records

Security Group records contain information related to each unique Security Group in APM. This topic provides an alphabetical list and description of the fields that exist for the Security Group family. The information in the table reflects the baseline state and behavior of these fields.

Field	Data Type	Description	Behavior and Usage
Caption	Character	A title or explanation that identifies the Security Group. A property that specifies how the Security Group is labeled throughout the software interface.	This field is required. You can enter text to define this value manually.
Description	Character	A detailed description of the Security Group.	This field is optional. You can enter text to define this value manually.
Group ID	Character	The ID for the Security Group.	This field is required. You can enter text to define this value manually.

Modify a Security Group Properties

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Groups**.
2. In the left pane, select the Security Group whose properties you want to modify.
   The workspace for the selected Security Group appears, displaying the corresponding Security Group form.
3. As needed, modify the available fields, and then select 💾.
   The updated Security Group properties are saved.

Activate or Deactivate a Security Group

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Groups**.
2. In the left pane, select the Security Group that you want to activate or deactivate.
   The workspace for the selected Security Group appears, displaying the corresponding Security Group form.
3. Select or clear the **Active** check box as needed, and then select 💾.
   Depending on your selection, the Security Group is activated or deactivated.

Assign Security Users to a Security Group

Before You Begin

- Create a Security User
- Create a Security Group

About This Task

This topic describes how to assign multiple Security Users to a Security Group on the **Security Groups** page. You can also assign a Security User to multiple Security Groups on the **Security Users** page.

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Groups**.
2. In the left pane, select the Security Group to which you want to add Security Users.
   The workspace for the selected Security Group appears.
3. In the workspace for the selected Security Group, select the **Users** tab.
   The **Users** section appears.
4. Select +.
   The **Assign Users** window appears, displaying the list of available Security Users.
5. Beside each Security User that you want to assign to the Security Group, select the check box.
6. Select **Save**.
   The updated Security Group properties are saved.

Remove Security Users from a Security Group

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Groups**.
2. In the left pane, select the Security Group from which you want to remove Security Users.
   The workspace for the selected Security Group appears.
3. In the workspace for the selected Security Group, select the **Users** tab.
   The **Users** section appears.
4. Beside each Security User that you want to remove from the Security Group, select the check box.
5. Select 🗑.
   The selected Security Users are removed.
6. Select 💾.
   The updated Security Group properties are saved.

Assign Roles to Security Group

Before You Begin

- Create a Security Role
- Create a Security Group

About This Task

This topic describes how to assign multiple Security Roles to a Security Group on the **Security Groups** page. You can also assign a Security Role to multiple Security Groups on the **Security Roles** page.

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Groups**.
2. In the left pane, select the Security Group to which you want to add Security Roles.
   The workspace for the selected Security Group appears.
3. In the workspace for the selected Security Groups, select the **Roles** tab.
   The **Roles** section appears.
4. Select +.
   The **Assign Roles** window appears, displaying the list of available Security Roles.
5. Beside each Security Role that you want to assign to the Security Group, select the check box.
6. Select **Save**.
   The updated Security Group properties are saved.

Remove Security Roles from a Security Group

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Groups**.
2. In the left pane, select the Security Group from which you want to remove Security Roles.
   The workspace for the selected Security Group appears.
3. In the workspace for the selected Security Group, select the **Roles** tab.
   The **Roles** section appears.
4. Beside each Security Role that you want to remove, select the check box.
5. Select 🗑.
   The selected Security Roles are removed.
6. Select 💾.
   The updated Security Group properties are saved.

Remove a Security Group

About This Task

Note: Each Security Group has a corresponding folder at the following Catalog location:`Public/Meridium/Security Groups/<Group ID>`. Before you can delete a Security Group, you must delete all Catalog items stored at this location, and must remove all Catalog folder permissions from the Catalog folder.

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Groups**.
2. In the left pane, select the Security Group that you want to remove.
   The workspace for the selected Security Group appears, displaying the corresponding Security Group form.
3. Select 🗑.

The Security Group is removed.

Chapter 4

Roles

Topics:

Roles

About Roles

Roles can be associated with numerous Security Groups. When a Security Role is assigned to a Security User, the user is granted all the privileges that have been granted to the Security Groups associated with the Security Role. Assigning Security Roles to Security Users is an efficient way to provide data permissions to the users that they will need to execute tasks in APM.

Note: Regardless of the Security Group membership, Super Users have access to all the APM features and functionalities.

The following tables list the baseline Security Roles available for the users within APM, the baseline Security Groups assigned to each Security Role, and the privileges associated with each Security Role.

Important: To avoid granting unintended privileges to a Security User, before assigning a Security User to a Security Role, make sure that you review all the privileges granted to the Security Groups that are assigned to the Security Role. Additional Security Roles, as well as Security Groups assigned to existing Security Roles, can be added via Security Manager.

Analytics

Role	Group	Role Privileges
MI Analytics Administrator	MI Cognitive Administrator	The users can view, create, update, and delete cognitions, cognition-related logs, and standard lists.
MI Analytics Power	MI Cognitive User	The users can: • View, create, update, and delete cognitions. • View the cognition-related logs and standard lists.

APM Viewer

Role	Group	Role Privileges
MI APM Viewer	• MI ACA Member • MI AHI Viewer • MI AMS Asset Portal Viewer • MI ASI Viewer • MI ASM Viewer • MI Calibration Viewer • MI eLog Viewer • MI GAAViewer • MI GE Viewer • MI Hazards Viewer • MI Inspection Viewer • MI LCC Viewer • MI Metrics Viewer • MI MOC Viewer • MI Policy Viewer • MI PROACT Viewer • MI Production Loss Accounting Manager • MI RBI Viewer • MI RCM Viewer • MI Reliability Viewer • MI Rounds Designer Viewer • MI SIS Viewer • MI Thickness Monitoring Viewer	The users have the view privileges for most of the APM records.

APMNow

Role	Group	Role Privileges
MI APMNow Admin	• MI APMNow Admin • MI Metrics Administrator • MI Policy Designer	The users can access Tools and certain administrative features.

Data Loader

Role	Group	Role Privileges
MI Data Loader Admin	• MI Calibration Administrator • MI CMMS Interface Admin • MI Site Reference User	The users have all the privileges applicable to the users assigned to the MI Data Loader User role. Additionally, the users can delete the data load configuration records and interface log records. To use a data loader specific to a module, the users need additional permissions specific to that module. For more information, refer to the appropriate Mappings documentation.
MI Data Loader User	• MI Calibration User • MI CMMS Interface User • MI Site Reference User	The users can access to the Data Loaders feature, and can view, update, and create data load configuration records and interface log records. To use a data loader specific to a module, the users need additional permissions specific to that module. For more information, refer to the appropriate Requirements Mappings documentation.

Reliability

Role	Group	Role Privileges
MI FE Administrator	• MI GAA Administrator • MI Policy Designer • MI Policy User • MI Policy Viewer • MI PROACT Administrator • MI PROACT Team Member • MI Production Loss Accounting Administrator • MI Production Loss Accounting Manager • MI Production Loss Accounting User • MI PROACT Viewer • MI Production Loss Accounting Service • MI Reliability Administrator • MI Reliability User • MI Reliability Viewer	The users have all the privileges applicable to the users assigned to the MI FE PowerUser role. Additionally, the users have administrative privileges for the Generation Availability Analysis, Root Cause Analysis, Production Loss Analysis, and Reliability Analytics features.
MI FE PowerUser	• MI GAA Analyst • MI Policy User • MI Policy Viewer • MI PROACT Team Member • MI Production Loss Accounting Manager • MI Production Loss Accounting User • MI PROACT Viewer • MI RCM Viewer • MI Reliability User • MI Reliability Viewer	The users have all the privileges applicable to the users assigned to the MI FE User role. Additionally, the users can: • Create, update, and delete Root Cause Analyses, Production Plans, Production Events, Production Losses, Production Analyses, System Reliability Analyses, Spares Analyses, Reliability Distribution Analyses, Probability Distribution Analyses, Reliability Growth Analyses, and Automation Rules. • Update Production Data and link Production Events to Root Cause Analyses. • Create and update GAA Events and GAA Performance records.
MI FE User	• MI GAA Analyst • MI GAA Viewer • MI Policy User • MI Policy Viewer • MI PROACT Team Member • MI Production Loss Accounting User • MI PROACT Viewer • MI RCM Viewer • MI Reliability User • MI Reliability Viewer	The users can access the GAA Company, GAA Plants, GAA Units, GAA Events, GAA Performance records, Root Cause Analyses, Production Loss Analyses, Production Analyses, System Reliability Analyses, Spares Analyses, Reliability Distribution Analyses, Probability Distribution Analyses, Reliability Growth Analyses, and Automation Rules features.

Foundation

Role	Group	Role Privileges
MI Foundation Admin	- MI Site Reference User - MI ACA Administrator - MI ACA Member - MI ACA Owner - MI SAP Interface User - MI Configuration Role - MI Security Role - MI Catalog Administrator - MI Metrics Administrator - MI Policy Administrators - MI eLog Administator - MI eLog Contributor - MI eLog Viewer - Security Group for Query Export	The users have all the privileges applicable to the users assigned to the MI Foundation Power role. Additionally, the users can configure mappings for the devices and view the SAP System records. In addition, the users have administrative privileges for the Catalog, Tasks, and ACA records features.
MI Foundation Power	- Everyone - MI Devices Power Users - MI Devices Users - MI Recommendation Management User - MI Task Manager User - MI Site Reference User - MI Policy Designer - MI ACA Member - MI ACA Owner - MI SAP Interface User - MI Power User Role - MI Metrics User - MI eLog Contributor - MI eLog Viewer - Security Group for Query Export	The users have all the privileges applicable to the users assigned to the MI Foundation User role. Additionally, the users can: - Save data from the devices in the APM database. - Create and manage the Site Reference records. - Update, add, and delete the ACA records. - View the SAP System records. - Add the users to the states. - Remove the users from the states.
MI Foundation User	- Everyone - MI Devices Power Users - MI Devices Users - MI Recommendation Management User - MI Task Manager User - MI ACA Member - MI Policy User - MI ACA Owner - MI Metrics User - MI SAP Interface User - MI eLog Contributor - MI eLog Viewer - Security Group for Query Export	The users can: - Send and receive data from the devices. - Create and manage the recommendations - Create and update the tasks. - View and create the ACA records. - View the KPIs, Scorecards, and Metric Views. - View the SAP System records.

Health

Role	Group	Role Privileges
MI Health Admin	• MAPM Security Group • MI AHI Administrator • MI AMS Suite APM Administrator • MI GE Administrator • MI Lubrication Management Administrator • MI Lubrication Management User • MI Operator Rounds Administrator • MI Operator Rounds Mobile User • MI Policy Administrator • MI Policy Designer	The users have all the privileges applicable to the users assigned to the MI Health Power role. Additionally, the users can access the Rounds and Asset Health Manager features.
MI Health Power	• MI Operator Rounds Mobile User • MAPM Security Group • MI AHI User • MI Policy Designer • MI GE User • MI Lubrication Management User	The users have all the privileges applicable to the users assigned to the MI Health User role. Additionally, the users can create, update, and delete policies, policy instances, policy recommendations, and health indicator values.
MI Health User	• MI Operator Rounds Mobile User • MAPM Security Group • MI AHI User • MI Policy Designer • MI GE User	The users can: • Access the Rounds Data Collection mobile features. • Create recommendations and acknowledge heath indicators in Asset Health Manager. • View policy data. • Create policy instances in Policy Designer. • Create and modify AMS Asset recommendations.

Integrity

Role	Group	Role Privileges
MI Mechanical Integrity Administrator	- Criticality Calculator - MI Inspection - MI Policy Viewer - MI RBI Administrator - MI RBI Analyst - MI RBI Calculation Policy Viewer - MI RBI Recommendation Policy Viewer - MI RBI Risk Mapping Policy Viewer - MI Thickness Monitoring Administrator - MI Thickness Monitoring Inspector - MI Thickness Monitoring User	The users have all the privileges that are applicable to the MI Mechanical Integrity Power role. Additionally, users have administrative privileges for the Thickness Monitoring and RBI features and can access the RBI data mapping and reference tables.
MI Mechanical Integrity Power	- Criticality Calculator - MI Inspection - MI Policy Viewer - MI RBI Analyst - MI RBI Calculation Policy Viewer - MI RBI Recommendation Policy Viewer - MI RBI Risk Mapping Policy Viewer - MI Thickness Monitoring Inspector - MI Thickness Monitoring User	- The users have all the privileges that are applicable to the MI Mechanical Integrity User. Additionally, users can access the criticality calculator family and RBI features (except data mapping). - The users have view privileges for all the RBI families.
MI Mechanical Integrity User	- MI Inspection - MI Thickness Monitoring Inspector - MI Thickness Monitoring User	The users can access the T-Min Calculator, Archive Corrosion Rates, Exclude TMLs, and Renew TMLs features. Additionally, users have basic access to the Inspection and Thickness Monitoring features.
MI Mechanical Integrity Viewer	- MI Inspection Viewer - MI RBI Viewer - MI Thickness Monitoring Viewer	The users have view privileges to all the families in Risk Based Inspection, Thickness Monitoring, and Inspection Management.
MI Inspection Viewer	MI Inspection Viewer	The users have view privileges to all the families in Inspection Management.
MI Inspection	MI Inspection	The users have access to all the families in Inspection Management. Additionally, users can access Compliance Strategy and Compliance Policy Mapping.
MI Inspection Supervisor	MI Inspection Supervisor	The users are populated in the Reviewers Name field of the baseline inspection workflow, and can create, update, review, and approve an inspection. **Note:** This role does not have an added group. To access a specific module or a feature, add the relevant group to the user.

Role	Group	Role Privileges
MI Inspector	MI Inspector	The users are populated in the Inspection Report Owner field of the baseline inspection workflow, and can create, update, review, and send inspections for approval. **Note:** This role does not have an added group. To access a specific module or a feature, add the relevant group to the user.
MI Contract Inspector	MI Contract Inspector	The users have privileges to create and update an inspection as a third-party inspector. **Note:** This role does not have an added group. To access a specific module or a feature, add the relevant group to the user.
MI Thickness Monitoring Administrator	MI Thickness Monitoring Administrator	The users have all the privileges that are applicable to the MI Thickness Monitoring Inspector. Additionally, users have administrative privileges for Thickness Monitoring features and can access the TM Rules Lookup, data mapping, and reference tables.
MI Thickness Monitoring Inspector	MI Thickness Monitoring Inspector	The users have all the privileges that are applicable to the MI Thickness Monitoring Viewer. Additionally, users can access the Thickness Measurement Locations, Datapoints, T-Min Calculator, Archive Corrosion Rates, Exclude TMLs, and Renew TMLs features along with other basic TM features.
MI Thickness Monitoring User	MI Thickness Monitoring User	The users have all the privileges that are applicable to the MI Thickness Monitoring Inspector. However, the Thickness Monitoring User is restricted from deleting some of the Thickness Monitoring records like Datapoint Measurement.
MI Thickness Monitoring Viewer	MI Thickness Monitoring Viewer	The users have view privileges to all the families in Thickness Monitoring.
MI Compliance Administrator	MI Compliance Administrator	The users have all the privileges that are applicable to the MI Compliance Analyst. Additionally, users can create, update, or delete Compliance Strategy Templates and link/unlink assets to the Compliance Strategy Template. **Note:** This role does not have an added group. To access a specific module or a feature, add the relevant group to the user.

Role	Group	Role Privileges
MI Compliance Analyst	MI Compliance Analyst	The users have privileges to suggest and apply Compliance Strategy Templates, create Inspection Plans, and update Compliance Recommendations. **Note:** This role does not have an added group. To access a specific module or a feature, add the relevant group to the user.
MI Inspection Plan Approver	MI ASM Analyst	The users have privileges to update and approve an Inspection Plan. Additionally, users have view privileges for Compliance Management, Inspection Management, and Risk Based Inspection.
MI RBI Administrator	MI RBI Administrator	The users have all the privileges that are applicable to the MI RBI Analyst. Additionally, users have administrative privileges for RBI features and can access the RBI data mapping and reference tables, but cannot update an Inspection Plan.
MI RBI Analyst	MI RBI Analyst	The users have all the privileges that are applicable to the MI RBI Viewer. Additionally, users have privileges for calculating RBI Analysis and associated functionalities related to an RBI Analysis such as Duplicate Analysis, Apply Analysis, and Create What-If Analysis. Users can also update an Inspection Plan.
MI RBI Viewer	MI RBI Viewer	The users have view privileges to all the families in Risk Based Inspection.

Safety

Role	Group	Role Privileges
MI Safety Admin	• MI Calibration User • MI Calibration Administrator • MI Calibration Viewer • MI HA Administrator • MI HA Facilitator • MI HA Member • MI HA Owner • MI Hazards Viewer • MI MOC Administrator • MI MOC Viewer • MI SIS Administrator • MI SIS Engineer • MI SIS User • MI SIS Viewer	The users have all the privileges applicable to the users assigned to the MI Safety Power role. Additionally, the users can create, modify, and delete all the records in Calibration Management, Hazards Analysis, LOPA, MOC, and SIS Management.
MI Safety Power	• MI Calibration User • MI Calibration Viewer • MI HA Facilitator • MI HA Member • MI HA Owner • MI Hazards Viewer • MI MOC Approver • MI MOC Viewer • MI SIS Engineer • MI SIS User • MI SIS Viewer	The user can access the following records: • Initiating Event • Consequence Adjustment Probabilities • IPL Checklist • Active IPL • Passive IPL • Human IPL • Asset Safety Preferences Additionally, the users have all the privileges applicable to the users assigned to the MI Safety User role, and can create, modify, and delete all other records in Calibration Management, Hazards Analysis, LOPA, and SIS Management.
MI Safety User	• MI Calibration User • MI Calibration Viewer • MI HA Facilitator • MI HA Member • MI Hazards Viewer • MI MOC User • MI MOC Viewer • MI SIS Engineer • MI SIS User • MI SIS Viewer	The users can access the Recommendations, Calibration Templates, Risk Threshold records, Protective Instrument Loops, SIL Assessments, and SIL Threshold records features. Additionally, the users can access, create, modify, and delete all other records in Calibration Management, Hazards Analysis, LOPA, MOC, and SIS Management. In MOC, the users can access, create, modify, and delete General Recommendations.

State Management

Role	Group	Role Privileges
SM_Analyst	None	The users can transition states using State Management.
SM_Approver		
SM_Assessor		
SM_Coordinator		
SM_Facilitator		
SM_Implementor		
SM_Initiator		
SM_Owner		
SM_Planner		
SM_Team Leader		

Strategy

Role	Group	Role Privileges
MI Strategy Admin	• MI AHI Administrator • MI AHI User • MI ASI Administrator • MI ASI User • MI ASI Viewer • MI ASM Administrator • MI ASM Analyst • MI ASM Reviewer • MI ASM Viewer • MI Calibration User • MI Calibration Viewer • MI Inspection • MI LCC Administrator • MI LCC User • MI LCC Viewer • MI Lubrication Management Administrator • MI Operator Rounds Administrator • MI RBI Analyst • MI RCM Administrator • MI RCM User • MI RCM Viewer • MI SIS User	The users have all the privileges applicable to the users assigned to the MI Strategy Power role. Additionally, the users have administrative privileges for the Reliability Centered Maintenance, Failure Modes and Effects Analysis, Asset Strategy Implementation, and Life Cycle Cost Analysis features.
MI Strategy Power	• MI AHI Administrator • MI AHI User • MI ASI User • MI ASI Viewer • MI ASM Analyst • MI ASM Reviewer • MI ASM Viewer • MI Calibration User • MI Calibration Viewer • MI Inspection • MI LCC User • MI LCC Viewer • MI Lubrication Management Administrator • MI Operator Rounds Administrator • MI RBI Analyst • MI RCM User • MI RCM Viewer • MI SIS User	The users have all the privileges applicable to the users assigned to the MI Strategy User role, and the administrative privileges for the Asset Health Manager feature.

Role	Group	Role Privileges
MI Strategy User	• MI AHI User • MI ASI User • MI ASI Viewer • MI ASM Analyst • MI ASM Viewer • MI Calibration User • MI Calibration Viewer • MI Inspection • MI LCC User • MI LCC Viewer • MI Lubrication Management Administrator • MI Operator Rounds Administrator • MI RCM User • MI RCM Viewer • MI SIS User	The users have the view, create, update, and delete privileges for the Reliability Centered Maintenance, Failure Modes and Effect Analysis, Asset Strategy Implementation, Asset Strategy Management, and Life Cycle Cost Analysis features. Additionally, the users have the administrative privileges for Rounds feature, and view privileges for Asset Health Manager and Calibration Management features.

Managing Roles

Access the Security Roles Page

Procedure

In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Roles**.
The **Security Roles** page appears.

Create a Security Role

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Roles**.
2. In the left pane, select +.
   The **New Role** workspace appears, displaying a blank Security Role form.

   -or-

   If you want to create a new subgroup, in the left pane, select the Security Role to which you want to add the subgroup, and then select **New Role**.

   The **New Role** workspace appears, displaying a blank Security Role form.
3. As needed, enter values in the available fields.
4. Select 💾.
   The Security Role is saved.

Next Steps

- Assign Security Users to Roles.

Security Role Records

Security Role records contain information related to each unique Security Role in APM. This topic provides an alphabetical list and description of the fields that exist for the Security Role family. The information in the table reflects the baseline state and behavior of these fields.

Field	Data Type	Description	Behavior and Usage
Caption	Character	A title or explanation that identifies the Security Role. A property that specifies how the Security Role is labeled throughout the software interface. Note that most captions can be localized.	This field is required. You can enter text to define this value manually.
Description	Character	A detailed description of the Security Role	This field is optional. You can enter text to define this value manually.
ID	Character	The ID for the Security Role	This field is required. You can enter text to define this value manually.

Assign Security Users to Roles

Before You Begin

- Create a Security User on page 4
- Create a Security Role on page 36

About This Task

This topic describes how to assign multiple Security Users to a Security Role on the **Security Roles** page. You can also assign multiple Security Roles to a Security User on the **Security Users** page.

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Roles**.
2. In the left pane, select the Security Role that you want to assign to the Security User.
   The workspace for the selected Security Role appears.
3. In the **Security Users** section, select +.
   The **Assign Users** window appears, displaying the available users.
4. Beside each Security User that you want to assign the to the Security Role, select the check box.
5. Select 💾.
   The updated Security Role properties are saved.

Remove Security Users from Roles

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Roles**.

2. In the left pane, select the Security Role from which you want to remove Security Users.
   The workspace for the selected Security Role appears.
3. In the **Security Users** section, beside each Security User that you want to remove, select the check box.
4. Select 🗑.
   The selected Security Users are removed.
5. Select 💾.
   The updated Security Roles properties are saved.

Assign Security Groups to Security Roles

Before You Begin

- Create a Security Group
- Create a Security Role

About This Task

This topic describes how to assign multiple Security Groups to a Security Role on the **Security Roles** page. You can also assign multiple Security Roles to a Security Group on the **Security Groups** page.

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Roles**.
2. In the left pane, select the Security Role that you want to add to the Security Group.
   The workspace for the selected Security Role appears.
3. In the **Security Group** section, select +.
   The **Assign Groups** window appears.
4. Beside each Security Group that you want to assign the to the Security Role, select the check box.
5. Select 💾.
   The updated Security Role properties are saved.

Remove Security Groups from Roles

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Roles**.
2. In the left pane, select the Security Role for which you want to remove the Security Group.
   The workspace for the selected Security Role appears.
3. In the **Security Groups** section, beside each Security Group that you want to remove, select the check box.
4. Select 🗑.
   The Security Groups are removed.
5. Select 💾.
   The updated Security Roles properties are saved.

Chapter 5

Password Policy

Topics:

About the Password Policy

To access APM, a user must have a valid user ID and password.

When you create or change a password, consider the following requirements:

- Do not include spaces.
- Do not use the first name, last name, or user ID of the user.

Baseline Password Policy

The following table describes the recommended baseline settings for a password, which an administrative user can modify.

Parameters	Baseline Value
Minimum password length	5
Require upper and lower case letters	False
Require numeric values	False
Require symbols (%,*, etc.)	False
Maximum number of sequential characters (ex: abc, 123)	2
Maximum number of characters that can be reused from a previous password	3 Example: If your previous password was June1, your new password cannot be June2 because you cannot reuse the four characters June.
Minimum number of days a password change will be kept on file	365
Number of failed login attempts before an account is locked	1000
Maximum number of days before a password must be changed	0
Amount of time in minutes a user will be locked out due to invalid login attempts	20

Customize the Password Policy

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **Password Policy**.
   The **Password Policies** page appears, displaying the password properties that you can configure.
2. As needed, enter values in the available fields.
3. Select 💾.
   The password policy is saved.

Next Steps

- Create a Security User.

Chapter 6

Lightweight Directory Access Protocol (LDAP)

Topics:

About LDAP

Lightweight Directory Access Protocol (LDAP) is used for querying and managing directories that run over TCP/IP. Microsoft Active Directory represents one implementation of LDAP. APM supports integration with Microsoft Active Directory to facilitate automatic login and synchronization of user information.

LDAP is not limited to contact information, or even information about people. LDAP is used to look up encryption certificates, pointers to printers and other services on a network, and to enable same sign-on, where one password for a user is shared between many services. LDAP is appropriate for any type of directory-like information, where fast look-ups and less-frequent updates are standard.

As a protocol, LDAP does not define how programs work on either the client or server side. It defines the "language" used for client programs to talk to servers (as well as servers to servers). On the client side, a client may be an email program, a printer browser, or an address book. The server may speak only LDAP, or have other methods of sending and receiving data; LDAP may just be an add-on method.

LDAP continues to be a popular standard for communicating record-based, directory-like data between programs.

About Domain Records

Domain records store identifying information about the Microsoft Active Directory domains that exist in your organization.

For LDAP integration to work properly:

- At least one Domain record must exist to identify the Active Directory domain that contains user accounts that you want to synchronize with APM. You can create as many Domain records as needed to identify all the domains from which you want to retrieve user information.

The baseline APM product contains a Domain record that you can use as the basis for creating the one required Domain record.

- If you have only one Microsoft Active Directory domain, you can simply modify the baseline Domain record.
- If you have multiple Active Directory domains, you can modify the baseline Domain record and create new records to identify your additional domains. When you create a new Domain record, the default values will match those of the baseline Domain record to provide a guideline for specifying values in the new record.

About LDAP Field Mapping Records

LDAP Mapping records define how fields in Microsoft Active Directory user accounts correspond to fields in APM user records. The mappings that are defined in LDAP Mapping records are used to synchronize data between Microsoft Active Directory and APM. The LDAP Mapping records determine what information should be retrieved from Microsoft Active Directory and where it should be stored in APM.

Each LDAP Field Mapping record contains the following types of fields:

- **LDAP Field**: Defines the source fields in Microsoft Active Directory.
- **Meridium Field**: Defines the target fields for the corresponding Active Directory fields in APM.

When LDAP synchronization occurs, data is pulled from the source fields (values defined in the **LDAP Field** boxes) and used to populate the value in the corresponding target fields (defined by the **Meridium Field** boxes).

An LDAP Mapping record must exist for each Microsoft Active Directory field that you want to map to a APM field. APM provides a set of baseline LDAP Mapping records that map standard Microsoft Active Directory fields to fields in APM. If you want to change the mappings that are defined through the baseline records, you can modify the records as needed. However, we recommend that you retain the standard field mappings defined in the baseline LDAP Mapping records.

Important: If you want to map additional information to APM, you can create new field mapping records using only the reserved APM fields that are available for mapping with LDAP fields. You must not use any APM fields other than the reserved fields to create Field Mapping records.

About the LDAP Synchronization Process

When a scheduled or manual synchronization is run, LDAP will gather updated information from Microsoft Active Directory, import it into APM, and update the corresponding Security User records. When the synchronization process is run, APM Security User properties and status will be updated to reflect the last saved information in Microsoft Active Directory.

Note: To ensure that your APM system is in sync with the Microsoft Active Directory system, schedule the synchronization process to run on a frequent basis (every hour or more).

The synchronization process will import to APM only the changes (i.e., new users and updated information) that have been made in Microsoft Active Directory since the last synchronization ran, based on the Last Execution date in the job schedule item. Because only changes are imported to APM, the more often you run the synchronization process, the faster it will be (i.e., the fewer the changes, the faster the process). If you need to perform a full update in APM, you will need to delete and recreate the scheduled item to clear the Last Execution date. Performing a full synchronization will take longer than performing an update synchronization.

What Happens During Synchronization?

When a synchronization operation is performed:

- The APM system will retrieve the information for the Microsoft Active Directory users associated with the Microsoft Active Directory domains that have been defined in APM. The corresponding Security User records will be updated. Fields in APM will be updated with the information in Microsoft Active Directory using LDAP Field Mapping records.
- If the APM system finds a user in Microsoft Active Directory who does not have a corresponding Security User record in APM:
    - A Security User record will be created in the APM database.
    - The Security User record will be linked to the Domain record that identifies the Microsoft Active Directory domain in which the user exists.
    - The Security User will be associated with each APM Security Role whose name matches exactly the name of a Microsoft Active Directory Group to which that user belongs.
    - The Security User will be removed from each APM Security Role whose name does not match exactly the name of a Microsoft Active Directory Group to which that user belongs.
- If the Microsoft Active Directory user is locked out of Microsoft Active Directory, the user will not be locked in APM database.
- All the settings specified in the User Defaults page, including Time Zone, UOM, Culture, Language, and Site are assigned to new users.

Note: The default site in the User Defaults page is assigned to new users only if the default site is not configured in the Microsoft Active Directory or in the domain record in LDAP Manager.

About Synchronization and Authentication

APM Security Users are authenticated at log-in. In addition to validating status for a user (whether the **Active** check box is selected in the Security User record for that user), at log-in, the APM system initializes all the information and permissions for that user. If any of that information changes while the Security User is logged in to the APM system, those changes will not be reflected immediately. The changes will not take effect until the user logs out of APM and then logs back in. This behavior applies to changes made manually and automatically through the LDAP synchronization process. In other words, regardless of when or how often the LDAP synchronization process runs, changes made to a user account will not be applied until the next time a user logs in to the APM system.

About LDAP Authentication and Same Sign-On

LDAP authentication is generally used by Same Sign-On (SSO) systems. The enterprise user logs on initially using a form-based enterprise login screen. The user enters an ID and password, and the SSO software then takes the information and sends it to the security server using an encrypted connection. The security server then logs on to the LDAP server on behalf of the user by providing the LDAP server with the user's ID and password. If successful, the security server then proceeds with any authorization and/or lets the user proceed to the application or resource that he or she wants to access.

About LDAP Log Records

About This Task

To access LDAP Log records, you must enable LDAP integration and logging, and then run the LDAP synchronization process. If you would like detailed Log records related to LDAP to be created, on the **LDAP Manager** page, you should also select the **Enable informational messages** check box before running the LDAP synchronization process.

To access LDAP Log records, on the APM Server, navigate to **C:\ProgramData\Meridium**, and then select the Log file whose file name contains the date that corresponds to the time at which the LDAP synchronization process was run (e.g., **Meridium_2015-12-20.txt**).

When the LDAP synchronization process begins, the following line of text is added to the Log. Based on the information being synced, the values within brackets will vary.

- `{0} – SyncUsers`

When the LDAP synchronization process finishes, the following line of text is added to the Log. Based on the information that was synced, the values within brackets will vary.

- `{0} - Finished SyncUsers. Found {1} actions`

Note: If the **Enable informational messages** check box is cleared when the LDAP synchronization process occurs, the Log records will only contain the records described previously, which define the beginning and end of the LDAP synchronization process.

When the LDAP synchronization process is running, if the **Enable informational messages** check box is selected, additional LDAP-related records will be added to the Log. In the Log, these additional records will appear between the records described previously, which define the beginning and end of the LDAP synchronization process. The following are examples of additional LDAP-related records that could be created in the Log. This list is not comprehensive.

- `Found {0} domains to process`
- `Found {0} users in the {1} domain`
- `Found {0} APM users associated with the domain {1}`
- `Found {0} actions for the domain {1}`

After opening a Log file containing LDAP information, you can use the Find... feature in Notepad to search the Log for instances LDAP-related records (i.e., you could search for syncusers or domains to process to find lines of text containing those terms).

Access the LDAP Page

Procedure

- In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **LDAP**.
  The **LDAP** page appears.

Next Steps

- Enable LDAP Integration and Logging.

LDAP Workflow

This topic provides a basic workflow for using this module, as well as links to the available procedures, concepts, and reference topics.

Steps

1. Enable LDAP integration and logging.

   Note: LDAP integration will not be available until it has been enabled.
2. If you did not select the **Enable APM Security** check box, determine which existing Microsoft Active Directory Groups you want to map to APM Security Roles, and for each of those Microsoft Active Directory Groups, create a APM Security Role whose name matches exactly a Microsoft Active Directory Group name. When LDAP synchronizes Microsoft Active Directory and APM, each user will be assigned to the APM Security Roles whose names match exactly the names of the Microsoft Active Directory Groups to which they belong. If you selected the **Enable APM Security** check box, this step is not required, and you will manage Security Role assignment in APM .
3. Create a Domain record in APM for each Active Directory domain that contains users whose information should be synchronized with records in APM. Domain records store identifying information about the Microsoft Active Directory domains that exist in your organization.
4. Schedule an LDAP synchronization process to periodically update APM with user information from Microsoft Active Directory.

   Important: After implementing LDAP synchronization, do not modify Security User information in APM; instead, modify the user information in Microsoft Active Directory, and then synchronize. Synchronization overwrites all APM Security User site assignments, Security Role assignments, and all other mapped information with the most recent information in Microsoft Active Directory.

Enable LDAP Integration and Logging

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **LDAP**.
2. On the **LDAP Manager** page, select the **Enable LDAP Integration** check box.
3. If you would like detailed Log records related to LDAP to be created, select the **Enable informational messages** check box.

   Note: The **Enable informational messages** check box can be selected only if the **Enable LDAP Integration** check box is also selected.
4. If you will manage APM Security Role assignment in APM, rather than via LDAP, select the **Enable APM Security** check box.

   Note: If you do not select this check box, you must complete step 2 in the LDAP workflow.
5. If your LDAP is synchronized and you do not want to change your expired Microsoft Active Directory password through the APM login screen, clear the **Enable Password Change** check box.

   Note: The **Enable Password Change** check box is selected by default. If your LDAP password expires in the Microsoft Active Directory file system, you will be prompted to change the password when you attempt to log in to APM. If the **Enable Password Change** check box was not selected during LDAP synchronization and you attempt to log in to APM after your password expires, you will encounter an error. You will then need to contact the Microsoft Active Directory administrator to change the password.
6. In the upper-right corner of the page, select 💾.
   LDAP integration and logging is enabled.

Next Steps

- Create a Domain Record.

About Managing Users When LDAP Integration is Enabled

About This Task

The LDAP integration feature is intended to simplify the APM user management process. It allows you to manage APM users through your existing, primary user management system: Microsoft Active Directory.

User information may change periodically in Microsoft Active Directory (e.g., group assignment, site assignment, address, phone number, job title, etc.).

One advantage of configuring LDAP integration is the ability to synchronize APM Security User records with the information in Microsoft Active Directory. The changes made in Microsoft Active Directory will be reflected in APM after synchronization.

Note:

- If you did not select the **Enable APM Security** check box, Security Role assignment will not be modified during synchronization, and you will manage Security Role assignment in APM .
- LDAP integration is designed to ensure that these the systems (APM and Microsoft Active Directory) are synchronized. Always be sure to follow the recommended workflow for managing users.

User Status after LDAP Synchronization

About This Task

When the LDAP synchronization process runs, a APM Security User's status (i.e., whether the **Active** check box is selected or cleared in the **Details** section of the Security User record for that user) will be updated based upon various conditions in Microsoft Active Directory.

The **Active** check box for a APM Security User will be cleared when:

- The Microsoft Active Directory account for the user is disabled.
- The user is not assigned to any Microsoft Active Directory Groups.

The **Active** check box for a APM Security User will be selected automatically after these conditions are resolved in Microsoft Active Directory and the synchronization process runs again.

Create a Domain Record

Procedure

1. Access the LDAP Page on page 46.
2. In the pane that displays the list of domain records, select +.
   The workspace for a new Domain record appears.
3. In the **Name** drop-down list box, select the name of the cross domain that contains your Active Directory data.

   Note: The domain names that appear in the **Name** drop-down list box are configured in the **Cross Domains** page. For more information, refer to the **Configure a New Cross Domain** section of the documentation.
4. If you want users belonging to a particular Microsoft Active Directory Group to be assigned the Super User privileges in APM (that is, you want the **Super User** check box to be selected in the **Details** section of the Security User record for that user), then, in the **Super User Role** box, select the APM Security Role whose name matches the Active Directory Group whose members should be granted Super User privileges in APM.
5. In APM, each Security User must be assigned to at least one site, and must be assigned to a default site. If you want the default site for each Security User associated with a Domain record to be set to a site during synchronization, then, in the **Default Site** box, select the site that should be set as the default site.
6. As needed, in the **<domain name>** section, enter values in the available fields.
7. As needed, in the **Field Mappings** section, enter values in the available fields. The section is populated automatically with LDAP baseline Field Mapping records. To remove a Field Mapping record, in the row for the Field Mapping record that you want to remove, select 🗑, and then, in the **Confirm Delete** dialog box, select **Yes**. To add a Field Mapping record, in the **Field Mappings** section, select +, then enter values in the available fields, and then, below the row for the new Field Mapping record, select **Save**.

   Important:

   To successfully log in to APM, Security Users must be assigned to at least one site, and must be assigned to a default site.

If your APM system contains only one site and you selected a default site in step 4, creating Microsoft Active Directory Groups to map site assignments from Microsoft Active Directory to APM is not required.

Additionally, you can run the LDAP synchronization process without selecting a default site in the **Default Site** box or creating the Microsoft Active Directory Groups described in this note. If you do so, APM will assign the first user-created site in the database as the default site for each synchronized user. If no user-created site exists in the database, then the Meridium Default site will be assigned as the default site for each synchronized user.

To create Microsoft Active Directory Groups to map site assignments from Microsoft Active Directory to APM:

a. Ensure that you have created, in APM, each site that you want to associate with users during synchronization.
b. In Microsoft Active Directory, create a Group whose name is **<data source>_Default_<site>**, where:

    - **<data source>** is the name of the data source to which you will be connected during synchronization.
    - **Default** is mandatory text. Microsoft Active Directory users who are associated with this group will be assigned to **<site>** during synchronization, and will be assigned **<site>** as their APM default site.
    - **<site>** is the exact name of a site in APM that you want to assign as the default site for some users during synchronization.

    Ensure that the Microsoft Active Directory Group name matches the naming convention. For example, to assign users the default site Plant, which exists in a data source named Industry, you would create a Microsoft Active Directory Group named Industry_Default_Plant.
c. In Microsoft Active Directory, if needed, create a Group whose name is **<data source>_<site>**, where:

    - **<data source>** is the name of the data source to which you will be connected during synchronization.
    - **<site>** is the exact name of a site in APM that you want to assign to some users during synchronization. It will not be assigned as the default site for the users.

    Ensure that the Microsoft Active Directory Group name matches the convention. For example, to assign users the site Plant, which exists in a data source named Industry, you would create a Microsoft Active Directory Group named Industry_Plant.
d. As needed, repeat steps b and c.
e. In Microsoft Active Directory, associate the Groups with users. Each Microsoft Active Directory user whose information will be synchronized with APM must be associated with exactly one Group whose name is <data source>_Default_<site>. Each user can be associated with any number of additional groups whose names are <data source>_<site>.

    The Groups are assigned to users in Microsoft Active Directory. When you perform an LDAP synchronization, APM site assignments will be made based on the logic described in these steps.

Note:

Each APM Security User must have a unique User ID. You can either allow these User IDs to be generated automatically, or you can create a field mapping that will generate User IDs based on the values in a selected Microsoft Active Directory field.

If you do not create the field mapping described in the steps below, User IDs will still be generated automatically during synchronization. If the userPrincipalName Microsoft Active Directory field has a value, that value will become the APM Security User ID for the user. If the userPrincipalName Microsoft

Active Directory field does not have a value, the value in the sAMAccountName Microsoft Active Directory field will become the APM Security User ID for the user.

If you would like to use a different Microsoft Active Directory field to populate the User IDs of APM Security Users during synchronization:

a. In Microsoft Active Directory, choose a field that exists for every Microsoft Active Directory user and whose values you want to be used as the APM User IDs for those users.
b. In APM, for the appropriate Domain record, in the upper-right corner of the **Field Mappings** section, select +.
   A new row appears in the section, containing the **LDAP Field** and **Meridium Field** boxes.
c. In the **LDAP Field** box, enter the name of the Microsoft Active Directory field that you chose in step a.
d. In the **Meridium Field** box, enter USERID, and then, below the row for the new Field Mapping record, select **Save**.
   The Field Mapping record used to map User IDs is created.

8. In the workspace, select 💾.
   A new Domain record is created.

Next Steps

- Schedule an LDAP Synchronization Process.

LDAP Domain Records

This topic provides an alphabetical list and description of the fields that exist in Domain records. The information in the table reflects the baseline state and behavior of these fields.

Field	Data Type	Description	Behavior and Usage
Caption	Character	A short description of the domain.	You can define this value manually to help distinguish this domain from any other domains that you define.
Default Site	Character	The default site that will be assigned to new Security Users created during LDAP synchronization.	None
Root	Character	The starting point of the container in which APM will look for user objects in Microsoft Active Directory.	The APM system will use this information to find user objects in Microsoft Active Directory.
User Filter	Character	This filter is used to locate users within the specified directory.	This filter is used during the synchronization process to locate Microsoft Active Directory users that belong to a specific group within the domain. You can accept the default value in this field.

LDAP Field Mapping Records

This topic provides an alphabetical list and description of the fields that exist in LDAP Field Mapping records. The information in the table reflects the baseline state and behavior of these fields. For more information on the baseline LDAP Field Mapping records, refer to the LDAP Baseline Field Mapping Records on page 51 topic.

Field	Data Type	Description	Behavior and Usage
LDAP Field	Character	The name of Microsoft Active Directory field that will serve as the source field for mapping.	The baseline Field Mapping records that appear in the Domain records by default contain a set of Active Directory fields that are mapped to the corresponding APM fields. However, if you want to create additional Field Mapping records, you can manually define the Active Directory field that you want to map to a reserved APM field. You can obtain a list of available Active Directory fields from Microsoft.
Meridium Field	Character	The field ID of the field in APM that will serve as the target field for mapping.	The baseline Field Mapping records that appear in the Domain records by default contain a set of Active Directory fields that are mapped to the corresponding APM fields. However, if you want to create additional Field Mapping records, you can use the reserved APM fields to map to the Active Directory fields. You must specify the field ID, not the field caption.

LDAP Baseline Field Mapping Records

This topic provides an alphabetical list and description of the fields that exist in LDAP Baseline Field Mapping records. The information in the table reflects the baseline state and behavior of these fields.

LDAP Field	APM Field	Notes
company	MI_HR_COMPANY_CHR	None
department	MI_HR_DEPT_CHR	None
givenName	MI_HR_FIRST_NAME_CHR	None

LDAP Field	APM Field	Notes
l	MI_HR_CITY_CHR	None
mail	MI_HR_EMAIL_TX	None
postalAddress	MI_HR_ADDR1_CHR	None
postalCode	MI_HR_POSTCODE_CHR	None
sn	MI_HR_LAST_NAME_CHR	None
st	MI_HR_STATE_CHR	None
telephoneNumber	MI_HR_PHONE1_CHR	None
title	MI_HR_JOB_TITLE_CHR	None

Note: When you configure a custom attribute for **Culture** or **Timezone** fields in the Microsoft Active Directory, you can map it to SEUS_CULTURE_ID or SEUS_TIME_ZONE_CHR fields respectively, else the **Culture** and **Timezone** values will be set from the **User Defaults** workspace.

Reserved APM Fields for LDAP Mapping

The following table lists the reserved APM fields that are available for mapping with LDAP fields.

Reserved APM Field	Description	Notes
MI_HR_ADDR2_CHR	Address2	None
MI_HR_AREA_RESPONSIBILITY_TX	AreaOfResponsibility	None
MI_HR_BADGE_ID	BadgeId	None
MI_HR_BUSINESS_UNIT_TX	BusinessUnit	None
MI_HR_COMMENTS_TX	Comments	None
MI_HR_COUNTRY_CHR	Country	None
MI_HR_FAX_CHR	FaxNumber	None
MI_HR_MID_INIT_CHR	Initial	None
SEUS_LANGUAGE_ID	LanguageId	None
MI_HR_PHONE2_CHR	PhoneNumber2	None

Remove a Domain Record

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **LDAP**.
2. In the left pane, select the Domain record that you want to remove.
   The workspace for the selected Domain record appears.
3. In the upper-right corner of the workspace, select 🗑.
   The **Confirm Delete** dialog box appears.

4. On the **Confirm Delete** dialog box, select **Yes**.
   The Domain record is removed.

Run the LDAP Synchronization Process Manually

About This Task

The synchronization process can be managed either by manually running the LDAP synchronization or by scheduling the synchronization process.

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **LDAP**.
2. In the **LDAP** workspace, select **Run LDAP Sync**.
   The **Run LDAP Sync** dialog box appears.
3. Select **Yes**.
   The LDAP synchronization is run.

Schedule an LDAP Synchronization Process

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **LDAP**.
2. In the **LDAP** workspace, in the **LDAP's Job Schedule** section, select ✎.
   The **Edit Schedule** window appears. Enter the values in the required fields. For more information on creating a schedule, see Schedule a Job.

   In the **LDAP's Job Schedule** section, the job schedule item appears.
3. Beside the job schedule item, select 💾.
   The job schedule item is saved.
4. If you want to receive email about the failed scheduled job, select the **Notify when LDAP job fails** check box.
   The **+ users/group** link appears. You can select this link to select the users or groups to whom you want to send the email notification.
5. Select the **+ users/group** link and in the **Select users or group** window, select the names of the users or groups.
   The names of the selected users or groups appear. When a scheduled job fails, an email will be sent to these users or groups.

Results

- When the job schedule item is active, the synchronization will be executed based on the defined schedule.

Configure Notifications for the Failed LDAP Jobs

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **LDAP**.

The **LDAP** page appears.

2. Select the **Enable Notification When LDAP Job Fails** check box.
   The **+ User/Group** link appears.
3. Select the **+ User/Group** link.
   The **Select users or group** window appears, displaying a list of users in the **User** section.
4. In the **User** section, select the Security Users whom you want to notify when a scheduled LDAP synchronization job fails, and then select **OK**.

   Note: If you want to notify the groups, select the appropriate groups in the **Group** section.

   The **Select users or group** window disappears and the names of the selected users or groups appear in the **LDAP** page. When a scheduled LDAP synchronization job fails, the selected users or groups are notified.

Remove an LDAP Synchronization Job Schedule Item

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **LDAP**.
2. In the **LDAP** workspace, in **LDAP's Job Schedule** section, beside the job schedule item that you want to remove, select 🗑.
   The **LDAP** dialog box appears.
3. Select **Yes**.
   The job schedule item is removed.

Deactivate Security User Accounts

About This Task

This task describes how to deactivate a security user account that is not associated with any Security Groups in APM but the corresponding user account in Microsoft Active Directory is active.

Procedure

1. Access the **LDAP** page.
2. In the **LDAP** page, in the pane that displays a list of APM domains, select the domain for which you want to deactivate the security user accounts.
   The <Domain Name> workspace appears.
3. In the **User Filter** box, make sure that all the active security user accounts in APM appear in the user filter query.

   Note: If an active user account is not available in the user filter query, the user account is deactivated.
4. In the **LDAP Sync Domain Settings** drop-down list box, select **Deactivate Unsynced Users**.
5. Select 💾.
   The Security User accounts are deactivated.

Chapter 7

User Defaults

Topics:

About Setting Default Values for APM Users

Default value for a field provides a point of reference for a APM user. The values that appear for the corresponding fields in the **Users** page are based on the values that you configure in the **User Defaults** page for a Security User. The user can modify these settings any time based on their requirement.

> If a Security User is based in San Ramon, California, and if a large number of members of the team to which the user belongs are based in Roanoke, Virginia, you can set the default time zone to reflect the time zone where most of the Security Users are located. In this way, the time within APM will be consistent regardless of the physical location of a user. Similarly, when you specify a home dashboard for the users, all the team members can use the same dashboard, regardless of their location or device using which each team member accesses the APM application.

Access the User Defaults Page

Procedure

In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **User Defaults**..
The **User Defaults** page appears.

Specify a Default Site for Security Users

This topic describes how to specify a default site for the Security Users.

Procedure

1. Access the **User Defaults** page.
2. In the **Default Site** drop-down list box, select the site that you want to assign to the new Security Users by default.
3. Select 💾.
   The default site is specified for the Security Users.

   When you create a Security User, the specified site is automatically selected in the **Default Site** drop-down list box for the user.

Specify a Default UOM Conversion Set for Security Users

This topic describes how to specify a default UOM conversion set for the Security Users.

Procedure

1. Access the **User Defaults** page.
2. In the **Default UOM Conversion Set** drop-down list box, select the UOM conversion set that you want to associate with the new Security Users by default.
3. Select 💾.
   The default UOM conversion set is specified for the Security Users.

When you create a Security User, the specified UOM conversion set is automatically selected in the **UOM Conversion Set** drop-down list box for the user.

Specify a Default Culture Setting for Security Users

This topic describes how to specify a default culture setting for the Security Users.

Procedure

1. Access the **User Defaults** page.
2. In the **Default Culture** drop-down list box, select the culture setting that you want to associate with the new users by default.
3. Select 💾.
   The default culture is specified for the Security Users.

   When you create a Security User, the specified culture is automatically selected in the **Culture** drop-down list box for the user.

Specify a Default Language for Security Users

This topic describes how to specify a default language for the Security Users.

Procedure

1. Access the **User Defaults** page.
2. In the **Default Language** drop-down list box, select the language that you want to associate with the new users by default.
3. Select 💾.
   The default language is specified for the Security Users.

   Note: When you create a Security User, the specified language is automatically selected in the **Language** drop-down list box for the user.

Specify the Default Time Zone for New Users

About This Task

If most users of APM are located within the same time zone, you can specify a time zone that should be assigned to new users by default.

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **User Defaults**.
2. In the **Default time zone assigned to a new user** box, select the time zone that should be assigned to new users by default.
3. Select 💾.
   The default time zone has been specified. Now, when you create a new user, the Timezone field is populated automatically with the specified time zone.

Specify a Default Home Dashboard

About This Task

You can specify the dashboard that will appear on the home page by default when a new user logs in to APM.

Note: If you do not specify a default dashboard, the APM dashboard will appear. This dashboard is stored in the following Catalog location: **//Public/Meridium/Modules/Core/Dashboards/APM Foundation Dashboard**

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Security Manager** > **User Defaults**.
2. In the **Default Home Dashboard** box, select ⋯.
   The **Select a dashboard from the catalog** window appears.
3. Navigate through the Catalog, and then select the Dashboard that you want to set as the default dashboard.
4. Select **Open**.
   The default dashboard is specified.

Chapter 8

Cross Domains Configuration

Topics:

About Cross Domains

You can add and configure multiple domains to retrieve user information from multiple Active Directory servers to APM during the LDAP synchronization process.

Configuring Multiple Cross Domains for Synchronizing User Information

You can add and configure multiple cross domains in the **Cross Domains** page. The configured cross domains are used to create multiple LDAP domain records. After the LDAP domain records are created, using the LDAP synchronization process, you can retrieve the user information for the Microsoft Active Directory users associated with the Microsoft Active Directory domains that have been defined in APM.

Note: If Single Sign-On (SSO) authentication is enabled for the users to access APM, you can use only one cross domain to retrieve user information from the associated Active Directory server using the LDAP synchronization process.

Access the Cross Domains Page

Procedure

In the **Applications** menu, navigate to **ADMIN** > **Operations Manager** > **Cross Domain Configuration**. The **Cross Domains** page appears.

Configure a New Cross Domain

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Operations Manager** > **Cross Domain Configuration**.
2. In the pane that displays the list of domain names, select +.
   The workspace to configure a new domain appears.
3. In the **Domain Name** box, enter the name of the server or the domain that you want to configure.

   Note: The Domain name includes a domain suffix. For example, enter `domain.com` instead of `domain` in the **Domain Name** box.
4. In the **User Name** box, enter the user name of the domain administrator.
5. In the **Password** box, enter the password that is associated with the specified User Name.
6. In the **Used For** drop-down list box, select an appropriate value for which you want to use the domain.

   Note: If you want to configure the domain to synchronize user information by running the LDAP synchronization process, select **LDAP**.
7. Select 💾.

Modify a Cross Domain

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Operations Manager** > **Cross Domain Configuration**.
2. In the pane that displays the list of domain names, select the domain that you want to modify.
   The workspace for the selected domain appears.
3. As needed, modify the fields.
4. Select 💾.
   The domain is modified.

Delete a Cross Domain

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Operations Manager** > **Cross Domain Configuration**.
2. In the pane that displays the list of domain names, select the domain that you want to delete.
   The workspace for the selected domain appears.
3. Select 🗑.
   The **Confirm Delete** window appears.
4. Select **Yes**.
   The domain is deleted.

Chapter 9

Data Loader

Topics:

About the Role Data Loader

The Role Data Loader allows existing or new Security Roles to be delivered to APM. You can load data into APM via the Excel workbook.

The data loader is used in the following scenarios:

- To create new Security Roles and associate them with existing Security Users and Security Groups.
- To modify the Security Users and Security Groups associated with existing Security Roles.

Important: If you are using an export file generated from a version of APM prior to V4.0.0.0 (e.g. V3.6.0.0.0), then that Excel file needs to be modified to match the current Role Data Loader template.

About the Role Data Loader Requirements

To use the Role Data Loader, the Security Users and Security Groups that you want to associate with new and existing Security Roles must already exist in your APM system.

Mapping

The Role Data Loader maps the datasheet columns in the Excel workbook to fields in APM families.

Security Settings

The Security User performing the data load operation must be associated with either the MI Data Loader User or MI Data Loader Admin Security Role.

About the Role Data Loader General Loading Strategy

This section describes any prerequisites to loading the data and the order in which the data will be loaded.

Note: Before reading this section, refer to the Data Model section.

Prerequisites

- The Security Users and Security Groups that you want to associate with new and existing Security Roles already exist in your APM system.

About the Role Data Loader Workbook Layout and Use

This section provides a high-level overview and explanation of how the data loader workbook is constructed.

To import data using the Role Data Loader, APM provides an Excel workbook, **Role.xlsx**, which supports the Security Role feature in APM. This workbook must be used to perform the data load. You can modify the Excel template to include custom fields used by your organization.

The following table lists the worksheets that are included in the **Role** workbook.

Worksheet	Description
Role	This worksheet is used to specify data for import to the Security Role family.
RoleGroup	This worksheet is used to specify the Security Groups that should be associated with the Security Roles.
RoleUser	This worksheet is used to specify the Security Users that should be associated with the Security Roles.

Each worksheet in the Role Data Loader Template workbook contains field values that must be mapped to the appropriate APM family/field combination.

Role Worksheet

On the Role worksheet, you will specify the information for the Security Role record.

Note: Each row in this worksheet represents a unique role. Do not include the same role more than once.

Field Caption	Field ID	Data Type (Length)	Comments
ID	ROLE_ID	Character (255)	This field is required, and represents the ID for the Security Role.
Caption	ROLE_CAPTION_TX	Character (255)	This field is required. A title or explanation that identifies the Security Role. A property that specifies how the Security Role is labeled throughout the software interface. Note that most captions can be localized.
Description	ROLE_DESC_TX	Character (255)	This field is optional, and can contain a detailed description of the Security Role.

RoleGroup Worksheet

On the RoleGroup worksheet, you will specify existing Security Group records that you want to associate with Security Roles.

Field Caption	Field ID	Data Type (Length)	Comments
RoleId	ROLE-ID	Character (255)	This field is required. Enter the ID of the Security Role with which Security Groups will be associated.
GroupId	SEGR_ID	Character (255)	This field is required. Enter the GroupId of the Security Group with which Security Role will be associated.

RoleUser Worksheet

On the RoleUser worksheet, you will specify existing Security User records that you want to associate with Security Roles.

Field Caption	Field ID	Data Type (Length)	Comments
RoleId	ROLE_ID	Character (255)	This field is required. Enter the ID of the Security Role with which Security Users will be associated.
UserId	SEUS_ID	Character (255)	This field is required. Enter the UserId of the Security User with which Security Role will be associated.