SIEMENS

User Management Component 2.9.2

UMC Web UI User Manual

Contents

09/2020
A5E50361215-AA

Guidelines

This manual contains notes of varying importance that should be read with care; i.e.:

Important:

Highlights key information on handling the product, the product itself or to a particular part of the documentation.

Note: Provides supplementary information regarding handling the product, the product itself or a specific part of the documentation.

Trademarks

All names identified by ® are registered trademarks of Siemens AG.

The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/industrialsecurity.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E50361215-AA
20200903_45861

Contents

1 Concepts You Need to Know About

The following concepts are considered prerequisites to understand how to configure UMC:

- User Manager Domain
- User Manager User
- User Manager Group
- User Manager Role
- User Manager Function Rights

1.1 User Manager Domain

A User Manager domain (UM domain) is a collection of computers defined by the administrator of a network that shares a common directory database. A UM domain provides access to the centralized user accounts and group accounts maintained by the UM domain administrator.

Important:

UM domains are different entities with respect to Windows domains that are defined at operating system level.

1.2 User Manager User

A User Manager user (UM user in what follows) is a user in the User Manager Component database, identified by a user name. Note that UM users are different entities with respect to Windows users, which are defined at operating system level.

Custom attributes can be associated with UM users. Example of custom attributes are common user properties such as phone number, department, and so on.
To apply Secure Application Data Support (SADS), access to encrypted application data can be granted to authorized users to allow them to decrypt it using specific Subject Keys.

UM User Types

You can distinguish three types of UM users:

- **users created from scratch** in UMC or created via csv file;
- **Windows local users** that are imported into UMC (via umx): in this case the user name follows the pattern *<machineName>\<localUserName>*;
- **Active Directory users** that are imported into UMC (via umx or via Web UI): in this case the user name follows the pattern *<ADdomainName>\<ADuserName>*.

UM User Passwords

Users created within UMC have also an associated password. Empty passwords are not allowed. Users imported from Windows authenticate against Windows and do not have a UMC password. Imported Windows local users authenticate **only** locally against Windows on the machine where they are present. They can be used **only** for configuration purposes, for instance to be associated with a Windows service running on the machine.

Offline Users

When you create a UMC user you can flag the user as *offline*. UMC provisioning service checks if the offline user exists in Active Directory:

- if the user is present, user data are synchronized and the user becomes online,
- otherwise the user remains offline.

Important:

Users created as *offline* are enabled by design: they can therefore perform the actions allowed by their function rights.

The user name of offline users must follow the AD pattern <*domainName*>\<*ADuserName*>. They do not have a UMC password, as they cannot authenticate until they become online. The User Security Identifier (SID, see Microsoft Documentation on Security Identifiers for more details) property is set to a default value (S-1-0-0) that is synchronized with the actual AD value by the UMC provisioning service.

Users are also flagged *offline* if they are deleted from AD. In this case users are permanently deleted from UMC database after an amount of time that can be configured (default is12 hours). See the additional provisioning configuration in the *User Management Component Installation Manual* for more details.

User Limits

Description	Maximum
Number of groups assigned to a user	50
Number of roles assigned to a user	50

1.3 User Manager Group

A User Manager group (UM group in what follows) is a container of users and is identified by a name. Note that UM groups are different entities with respect to Windows groups that are defined at operating system level.

To apply Secure Application Data Support (SADS), access to encrypted application data can be granted to authorized groups to allow them to decrypt it using specific Subject Keys.

UM Group Types

There are two types of UM groups:

- **groups created from scratch** in UMC or created via csv file;
- **Active Directory groups** that are imported into UMC (via umx or via Web UI).

Offline Groups

When creating a UMC group, you can flag the group as *offline*. UMC provisioning service checks if the offline group exists in Active Directory:

- if the group is present, group data are synchronized, the AD users members of the groups are imported into UMC and the group becomes online,
- otherwise the group remains offline.

The group name of offline users must follow the AD pattern <*ADdomainName*>\<*ADgroupName*>. The UMC provisioning service searches for the AD group by its Common Name (CN).

If required, the description field of the created group can be used to configure how the UMC provisioning service must query the AD group and import its users into UMC. In this case the description must follow the pattern:

{{Q=<ldap query>

where {{Q= is a fixed prefix and <ldap query> is the query to be applied. The group name in this case can be <*ADdomainName*>\<*GroupName*>, where GroupName can be chosen by the user.

Group Limits

Description	Maximum
number of groups assigned to a user	50
number of roles assigned to a group	50
number of users bound to a group	1000

1.4 User Manager Role

A User Manager role groups a set of function rights. Function rights are the capabilities to perform operations. They are associated with roles so that the set of UM users with a specific UM role is allowed to perform the set of operations associated with it. UM roles can be associated with UM users or with UM groups so that all the users belonging to such groups inherit the UM role function rights. UM roles are used to define the function rights within UMC, for instance, to define whether a user can configure UMC or not.

The following roles are automatically created by the system while configuring UMC:

- **Administrator**: built-in "root" role, can perform any operation. The user that has this role is a root user that can perform any operation. This role cannot be associated with any group. It can be associated with a user if the user performing the association has in turn the **Administrator** role. The **Administrator** role cannot be deleted. Only users having the **Administrator** role can modify other users having this role.
- **UMC Admin**: can manage users, groups and all the other UMC entities.
- **UMC Viewer**: can access the user management configuration without making modifications.

1.5 User Manager Function Rights

Function rights are the capabilities to perform operations. They are associated with roles so that the set of UM users having a specific UM role is allowed to perform the set of operations associated with it. The following table contains a list of UM Function Rights:

Name	Description
UM_ADMIN	Allows you to display the UMC database data and to configure the UMC database, that is to create users, groups and so on, to import and export data via file, to register UMC station clients. This function right allows you to execute all **umx** commands.
UM_VIEW	Allows you to display the UMC database data related to users, groups, roles and account policies.
UM_RESETPWD	The user can reset the password of another user. The user must also have associated the **UM_VIEW** function right.
UM_UNLOCKUSR	The user can unlock any other user. The user must also have associated the **UM_VIEW** function right.
UM_ATTACH	The user can attach a machine to a UM domain, the machine is promoted to the *UM agent role*.
UM_JOIN	The user can promote a machine to a *UM server role*. If the machine is not yet attached to the UM domain, it is attached. This function right incorporates the **UM_ATTACH** function right.
UM_RESETJOIN	The user can downgrade a machine from the UM ring server or UM server role to the UM agent role.
UM_IMPORT	The user can import the UM Configuration via package. The user must also have associated the **UM_VIEW** function right.
UM_EXPORT	The user can export the UM Configuration into a package. The user must also have associated the **UM_VIEW** function right.
UM_BACKUP	The user can back up the UM Configuration (Full backup). *This function right is not used, as the functionality controlled by it has not yet been implemented.*
UM_EXPORTCK	The user can export Claim Key. *This function right is not used, as the functionality controlled by it has not yet been implemented.*
UM_EXPORTDK	The user can export Domain Key. *This function right is not used, as the functionality controlled by it has not yet been implemented.*

Name	Description
UM_RA	Login from Remote Authentication. *This function right is not used, as the functionality controlled by it has not yet been implemented.*
UM_RINGMNG	The user can promote a machine to a *UM ring server role*. If the machine is not yet attached to the UM domain, it is attached.
UM_ADSYNC	The user can perform the background AD provisioning synchronization.
UM_VIEWELG	The user can display event logging data. The user must also have associated the **UM_VIEW** function right.
UM_CLAIMAUTH	The user can create an identity from a valid claim.
UM_REGCLIENT	The user can register UMC station clients.

2 Quick Start to Using the User Management Component Web User Interface

This manual provides a general outline of the main steps that must be executed to use the User Management Component Web UI.

How to Access UMC Web UI

After you have configured the Web UI (for more details, see *User Management Component Installation Manual*), you can open the login page of the Web UI at the following address: **http://<myServer>/umc** or **https://<myServer>/umc** depending on the configuration.

You can also use a query string in order to automatically login using Windows Authentication, Custom plugins or Teamcenter integration. See Logging in to User Management Component Web UI for more information.

Before you Login

Before accesing UMC working environment, make sure you have followed a set of general recommendations for the security and the correct usage of UMC.

Workflow

1. Login to User Management Component Web UI
2. Perform the operations available in the Home Page

2.1 General Recommendations

In this page you can find a set of general recommendations to be followed to ensure UMC Web UI correct and secure functioning.

CAUTION:

Consider that when you login on UMC you are entering a protected environment. To exit you must logout, because simply closing the browser does not guarantee you have exited this protected environment. In addition, the following security information has to be taken into account.

Security Information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Additional Important Recommendations

- The browser used to display the UMC Web UI must allow the pop-up display.
- While using the UMC Web UI do not select the option **Prevent this page from creating additional dialogs**. The selection of this option causes Web UI malfunctions.
- Disable the **Autocomplete** option in your browser settings.
- Disable the password saving option in your browser settings.
- Do not use the back and forward navigation buttons of the browser.
- Do not copy and paste a UMC Web UI url into another browser window.
- Empty passwords are not allowed.

2.2 Logging in to User Management Component Web UI

Prerequisites

At least one of the following function rights has to be owned by the user to login to the UMC Web UI.

- **UM_ADMIN**: the user can perform all the available Web UI operations.
- **UM_VIEW**: the user can view the data displayed by the Web UI but cannot perform modifications.

Depending on the function right owned by the user, some operations may be allowed or not.

Note that, if custom plugins are used to authenticate some may not have a sufficiently high security level to log in to the web UI.

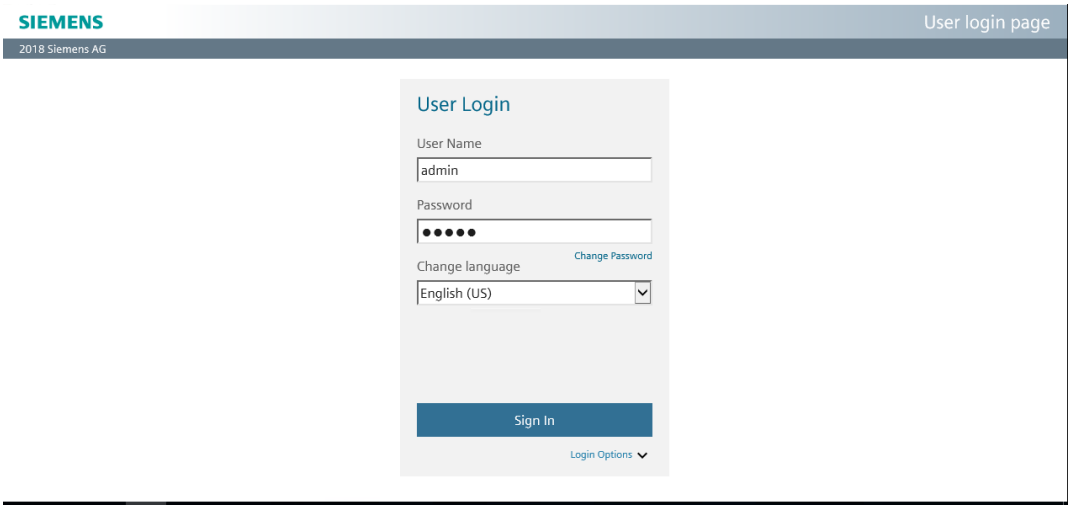
Note: The machine is automatically added to UMC whitelisting when you authenticate as a user with the UMC Administrator role.

Procedure

You can login to UMC Web UI in either of the following ways:

- Insert the user name and the password of a UMC user;
- Click **Use your current Windows session to Login**.

Depending on the type of authentication method you have configured (smart card and/or plugin), additional links may be displayed on the login page.



UMC Web UI Language

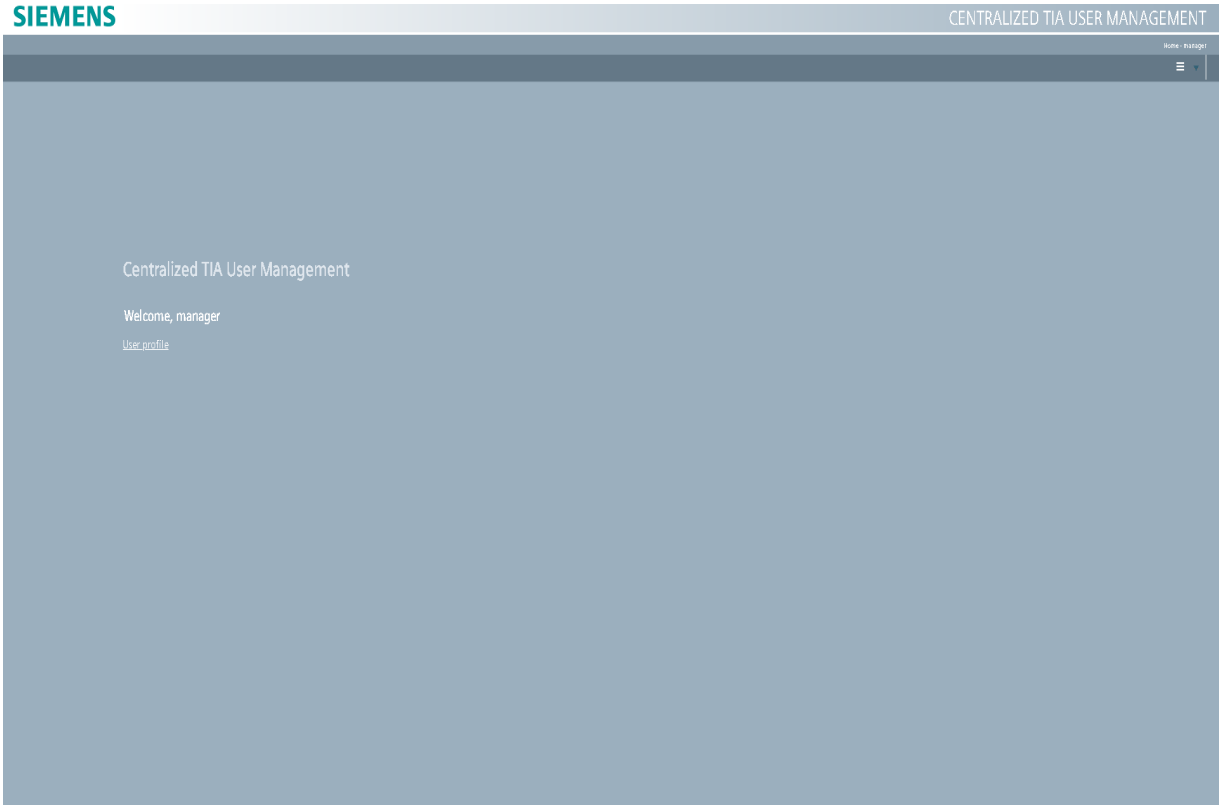
The login page (Identity Provider component) is displayed according to the language selected in your browser settings. If no browser settings are defined, the default language is **en-US**.

From the menu on the upper right-hand corner of the page, you can change the language in which the login page and related messages are displayed.

After you have logged in, the UMC pages are displayed according to the user language property of the logged-in user. If the user language property has not been defined, the language of UMC pages is the one of the login page.

2.3 UMC Web UI Home Page

After you have logged in, the UMC Web UI Home Page is displayed:



Available Operations

From the menu on the upper right-hand corner of the page, you can select the following operations:

- logout;
- access to the User Profile page.

In addition, depending on the function rights you own, you can access the Web UI pages from which you can perform the following operations:

- Manage Users
- Manage Groups
- Manage Roles
- Manage Account Policies
- Manage IdP Configurations
- Manage System Users
- Display Event Log

Additional Operations

Under particular conditions (UMC installed software on the client machine and user access rights), on the upper left-hand corner, the **Register client** button allows you to register the machine as a trusted machine that can provide logon station information. Refer to the *User Management Component Installation Manual* for more information on UMC station client.

3 How to Modify User Profile

Accessing the page

From the menu, on the upper right-hand corner of **UMC Home page**, select **User Profile** or click the **User Profile** button on the welcome page. The **User Profile** page is displayed.

Available Operations

In this page you can perform the following operations:

- Change Password
- Change Language
- Generate a Secret Key

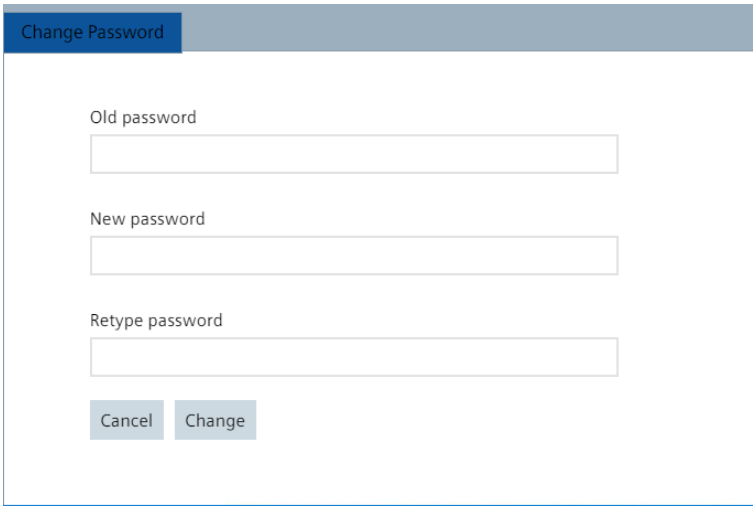
3.1 Changing Password

Allows a user to change his/her password. Empty password are not allowed.

Accessing the page

From the menu on the upper right-hand corner of **UMC Home page**, select **User Profile** or click **User Profile** link button on the welcome page. The **User Profile** page is displayed.

Select the **Change Password** Tab.

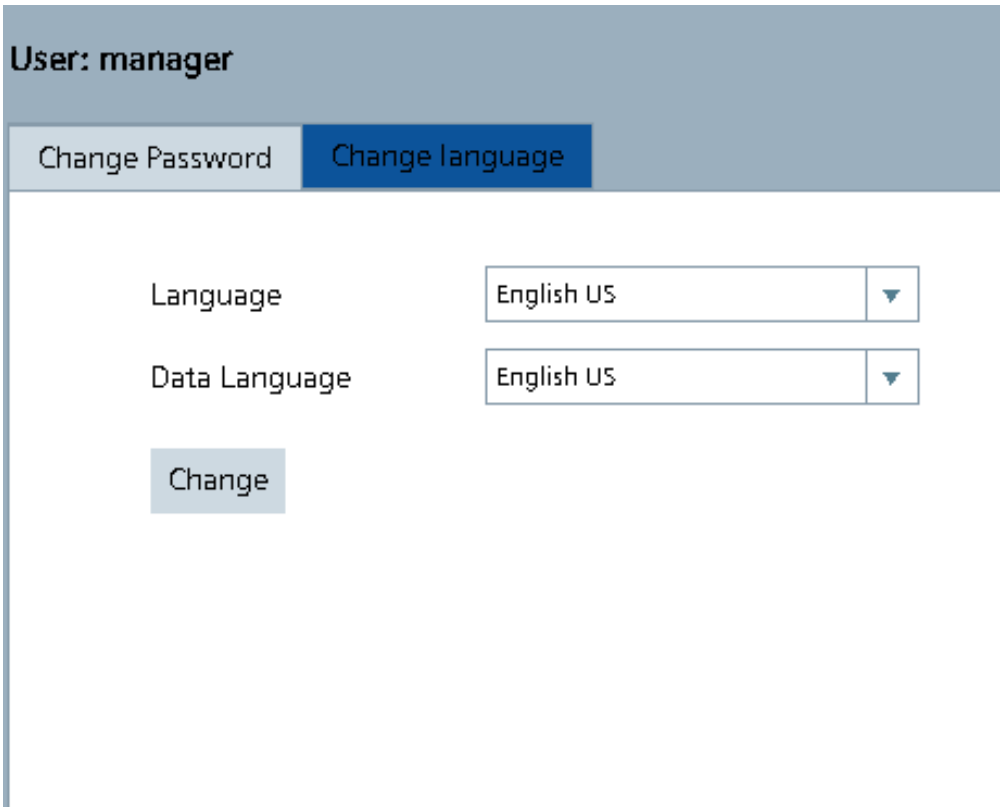


3.2 Changing Language

Allows a user to change his/her Language and Data Language.

Accessing the page

From the menu, on the upper right-hand corner of **UMC Home page**, select **User Profile** or click **User Profile** button on the welcome page. The **User Profile** page is displayed.



Procedure

1. Click the **Change language** tab.
2. Select the preferred language from the **Language** drop-down list.
3. Select the preferred data language from the **Data Language** drop-down list.
4. Click **Change**.

3.3 Generating a Secret Key

Allows you to create or reset the secret key for a user. The key can then be used to generate tokens for the two factor authentication by TOTP (time-based one-time password).

Accessing the page

From the menu on the upper right-hand corner of **UMC Home page**, select **User Profile** or click **User Profile** link button on the welcome page. The **User Profile** page is displayed.

Prerequisites

- SADS has been enabled in Account Policies via Web or UMX, it is required for secret protection.
- The Two Factor Authentication has been enabled as an authentication method via Web or UMConf centralized configuration management.
- The Two Factor authentication has enabled for the user in their account policies via Web or Encryption has been enabled for the user from UMX.

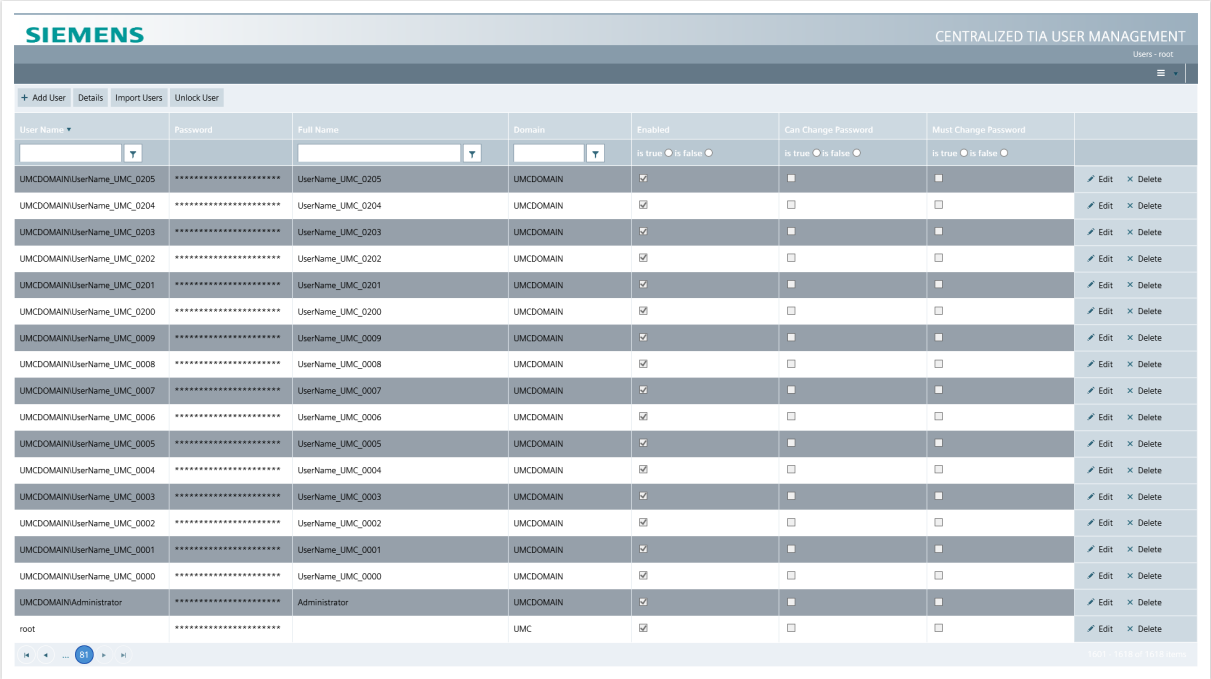
Procedure

1. Click the **Manage 2FA** tab.
2. Click **Display QR Code**.
3. If required click **Show Secret Key** or **Reset Secret Key**.

4 How to Manage Users

Accessing the Page

From the menu on the upper right-hand corner of **UMC Home Page**, select **Users**. The **Users** page is displayed.



Available Operations

Below each column name, a filter box allows you to filter the content of the selected column. In this page you can perform the following operations:

- create a user;
- update a user;
- import a user from Active Directory;
- unlock a user;
- delete a user (users imported via an AD group cannot be deleted).

When you manage users, refer to the corresponding **umx** commands for field constraints (see *UMX User Manual*).

Note: System Users that have been imported into UMC (via umx) like Windows local Users, Virtual service Accounts, IIS App Pool Identities, are not listed in the Users page. The System Users page can be used for visualizing them.

4.1 Creating a User

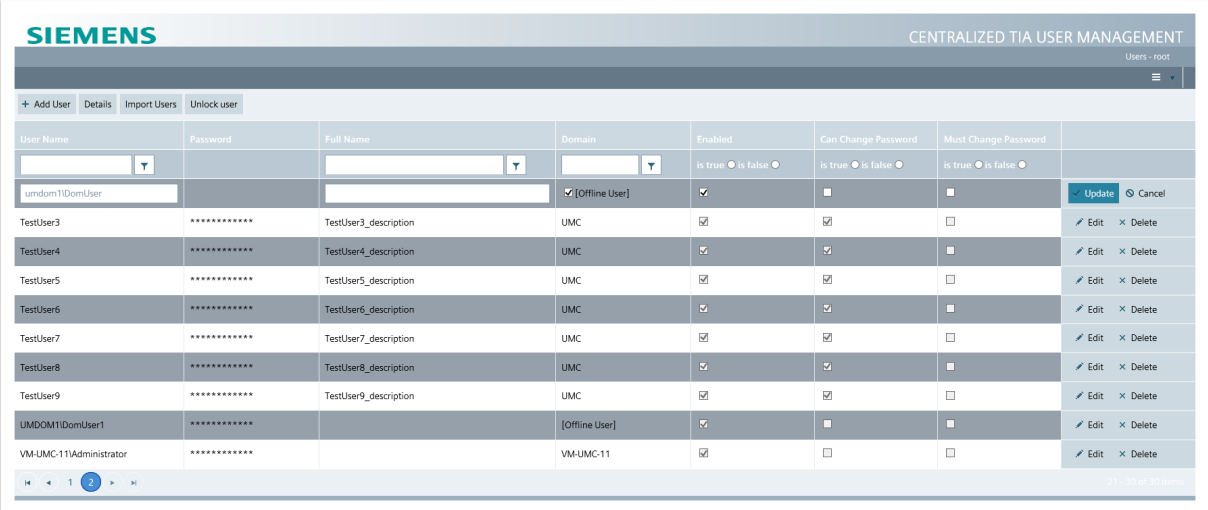
You can create one or more users by following this procedure.

Procedure

1. Click **Add User**.
2. In the new blank boxes that are displayed on top of the columns, add the user details.
3. (Optional) You can flag the user as offline in the **Domain** column; offline users are automatically enabled.
4. Perform either of the following actions:
   – click **Update** to confirm the creation;
   – click **Cancel** to cancel the insertion.

Important:

- The default domain for new users is **UMC**.
- if **Must Change Password** is selected the user must set a new password the next time they login.
- if **Can Change Password** is selected the password can be re-set by the user.
- The password specified by an Administrator during the creation or update of a user are not bound to password policies unless password the check has been enabled.



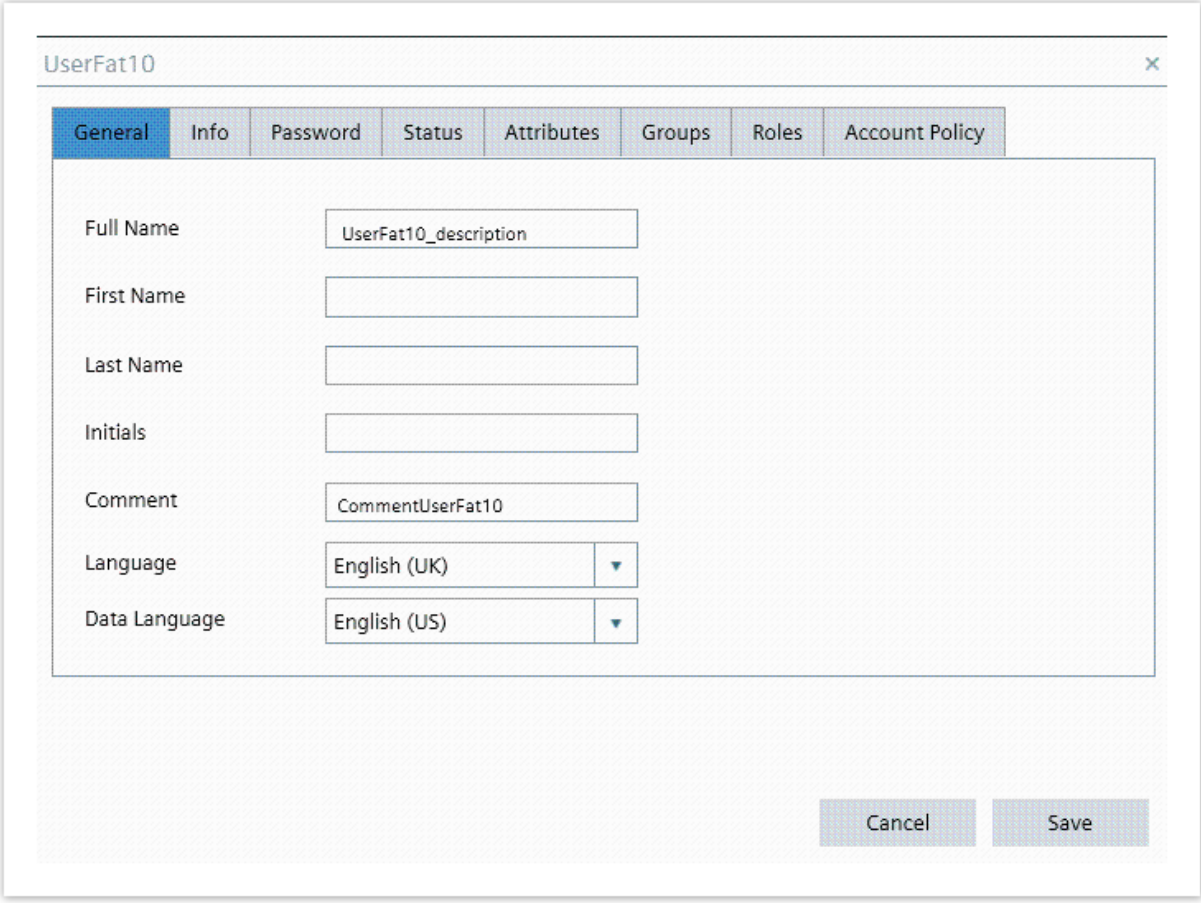
4.2 Updating a User

Important:

Imported AD and Windows Local users have editing restrictions, see Active Directory Users and Windows Users for more details.

Editing User Details

1. From the **Users** page, select a row and click **Edit** to edit the user main information directly in the grid.
2. If you want to insert or edit additional user details, select a row and click **Details** in the upper left-hand corner of the grid. Note that the password specified when editing a user is not bound to password policies, unless the password policy check is enabled. The following dialog box is displayed:



Available Operations

Each tab groups the user details that you can edit in that tab. Only specific properties whose editing needs additional explanations are described. In the following tabs you can:

- Edit User Attributes (**Attributes** tab).

- Display the group membership of the user (**Groups** tab). To add a user to a group, see How to Manage Groups.
- Associate Roles with Users (**Roles** tab).
- Edit User Account Policies (**Account Policy** tab).
- Change user status (**Status** tab) allows you to: Enable or disable a user, unlock a user, re-activate an expired user, or specify if they can or must change thier password.

Important:

In the current version of UMC, no field validators have been implemented.

Active Directory User Update

Imported fields are not editable. Only the following fields, which are not imported, can be modified:

- Tab **General**: **Language** and **Data Language**.
- Tab **Info**: **Email2** and **Email3**.
- Tab **Status**: **Enabled**.
- Tab **Attributes**: UMC custom attributes can be created, modified and deleted.
- Tab **Groups**: for all the users this tab displays only the user group membership; to add a user to a group see How to Manage Groups.
- Tab **Roles**: roles can be modified.
- Tab **Account Policy**: **User expiration date**, the alert fields and the **Password expiration days** field are not applicable. Only the **PKI Alias** and the **Authentication alias** can be modified.

All the other fields are imported from AD and cannot be modified via Web UI. They have to be modified in AD and they are automatically synchronized by UMC.

Windows Local User Update

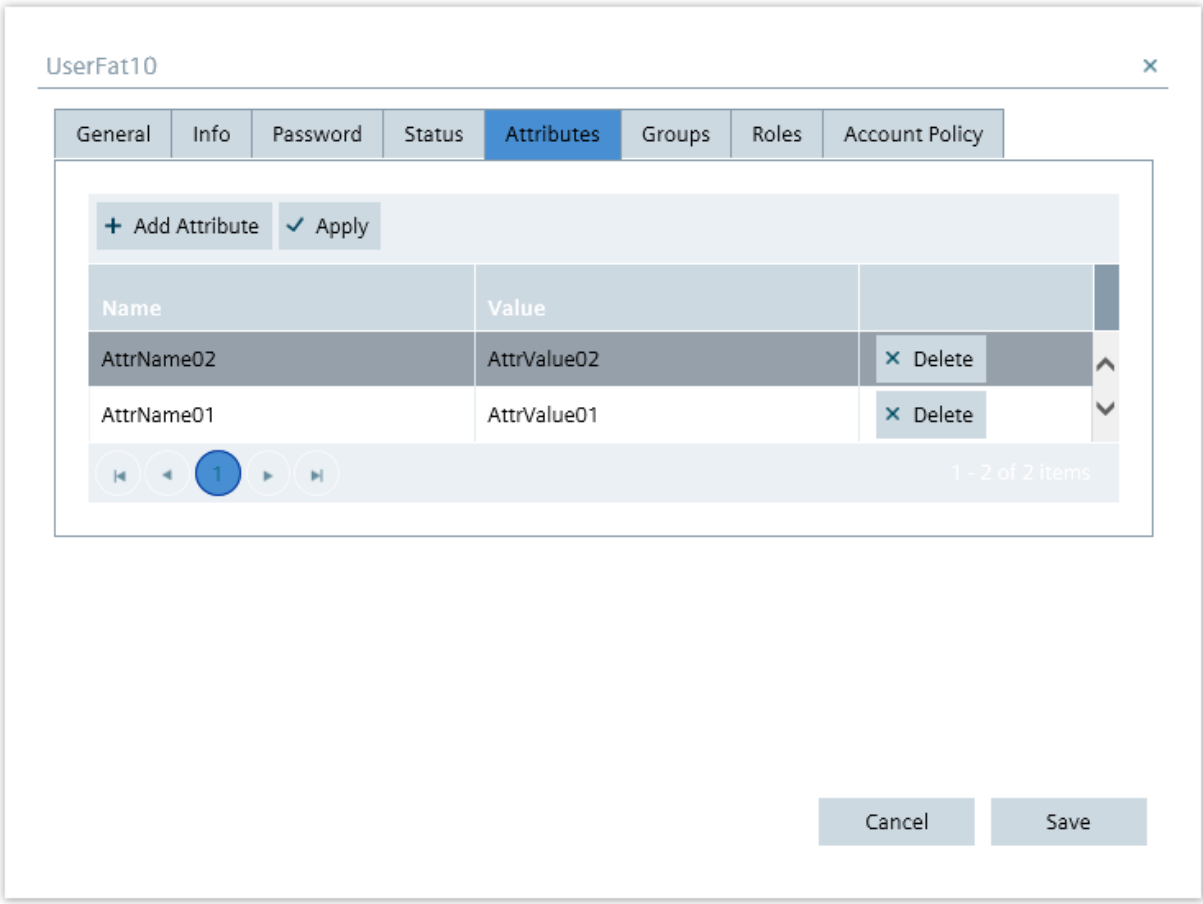
Imported fields are not editable. Only the following fields, which are not imported, can be modified:

- Tab **General**: **First Name, Full Name, Last Name, Initials, Language** and **Data Language**.
- Tab **Info**: **Mobile, Phone,Email1, Email2** and **Email3**.
- Tab **Status**: **Enabled**.
- Tab **Attributes**: UMC custom attributes can be created, modified and deleted.
- Tab **Groups**: for all the users this tab displays only the user group membership; to add a user to a group see How to Manage Groups.
- Tab **Roles**: roles can be modified.
- Tab **Account Policy**: **User expiration date**, the alert fields and the **Password expiration days** field are not applicable. Only the **PKI Alias** and the **Authentication alias** can be modified.

All the other fields are imported from Windows and cannot be modified via Web UI.

4.2.1 Editing User Attributes

In the **Attributes** tab you can edit the user attributes.



Procedure

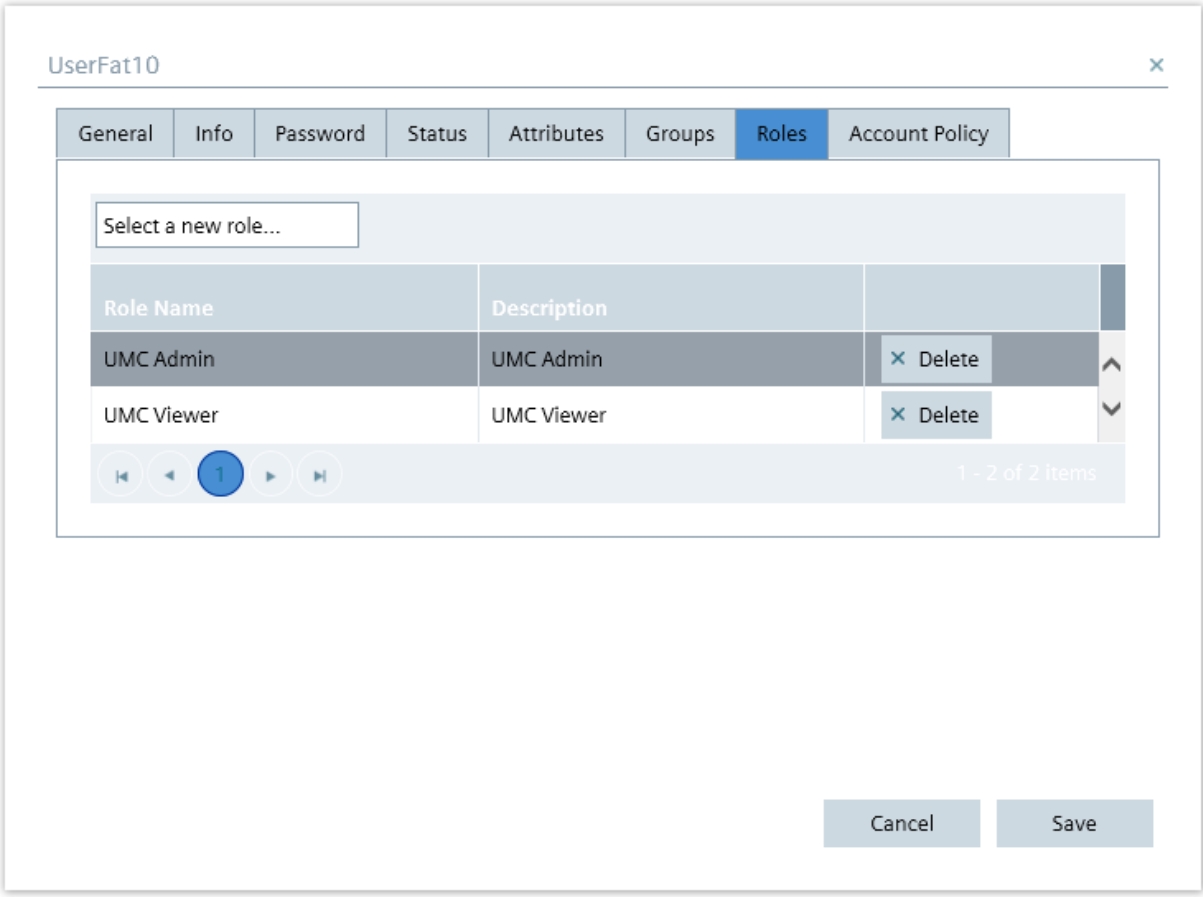
1. Perform one the following operations:

Operation	Actions
Add a new attribute	Click on the **Add Attribute** button. Add the attribute details in the new blank box that appears on top of the grid.
Delete an attribute	Select the row of the attribute you want to delete. Click on the **Delete** button.
Edit the attribute name or value	Click on the attribute you want to modify. Insert the required modifications in the text box.

2. To make the attribute modifications (add/delete/edit) effective, click the **Apply** button.
3. Click **Save**.

4.2.2 Associating a Role with a User

The **Roles** tab allows you to associate roles with users. A number of predefined roles are provided by UMC.



Procedure

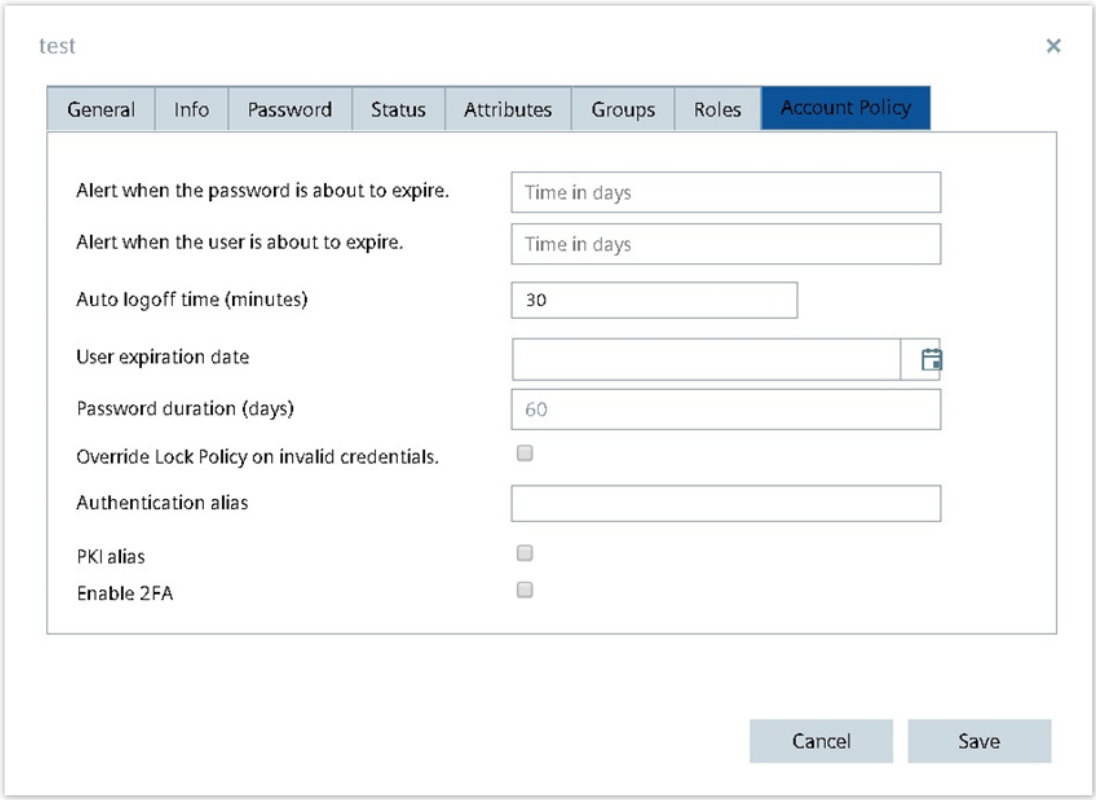
1. Type the role name in the box at the top of the grid. This box provides the autocomplete functionality so that only the first letters can be typed.
2. Select the required role and click **Save**.

Important:

- You can create new roles using the **umx** command. See the *UMX User Manual* for more details.
- The **Administrator** role cannot be associated with groups.

4.2.3 Editing User Account Policies

The **Account Policy** tab allows you to edit the user account policies.



Procedure

Fill the available fields. In particular, remember that:

- In the **Autologoff** box, you can enter a duration (in minutes) for the desktop session associated to the selected user.
- If you select the **Override Lock Policy on invalid credentials** checkbox. In this case, even though the user attempts to login with a wrong password a number of times that exceeds the global account policy **Maximum numbers of errors during login**, it is not locked. This field can be set only for users that are created from scratch within UMC, not for imported users;
- The maximum duration of a user password is 1827 days.
- in the field **Authentication alias** you can define the alias that is used to authenticate the user in the following ways:
  - via smart card authentication: in this case the **PKI alias** checkbox has to be selected and smart card authentication has to be configured;
  - via plugin authentication: in this case the **PKI alias** checkbox must not be selected and plugin authentication has to be configured.
- If you select the **Enable 2FA** checkbox to enable 2 factor authentication you must enable 2FA as an authentication method from authentication options and SADS in the global Account Policies.

For more information on the configuration of the different types of authentication see *User Management Component Installation Manual*.

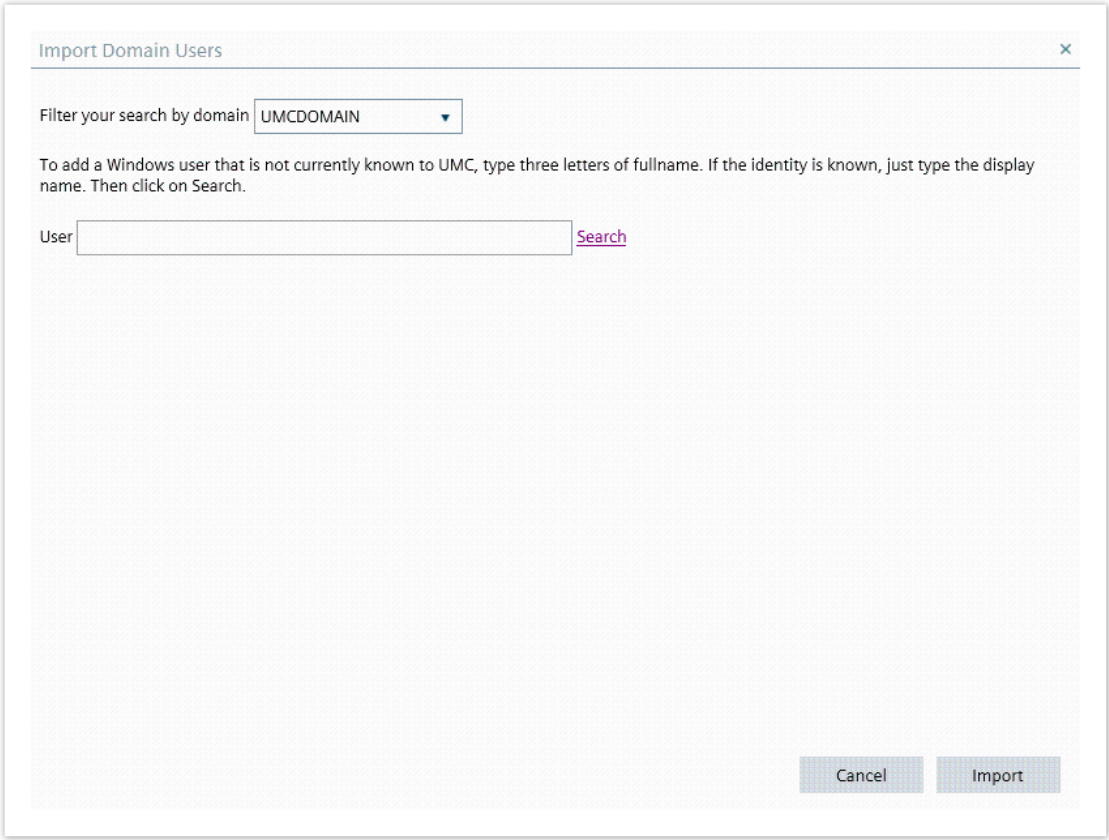
4.3 Importing a User from Active Directory

General Recommendations

- Windows local users can be imported only using the **umx** command. See the *UMX User Manual* for more details.
- Imported AD users and Windows Local users have editing restrictions, see updating a user.
- The import of users implies a search on Active Directory that can take a considerable amount of time and can return zero results when exceeding AD administration limits. It is strongly suggested that you perform restricted searches. To bulk import users, import them via the import of an AD group.

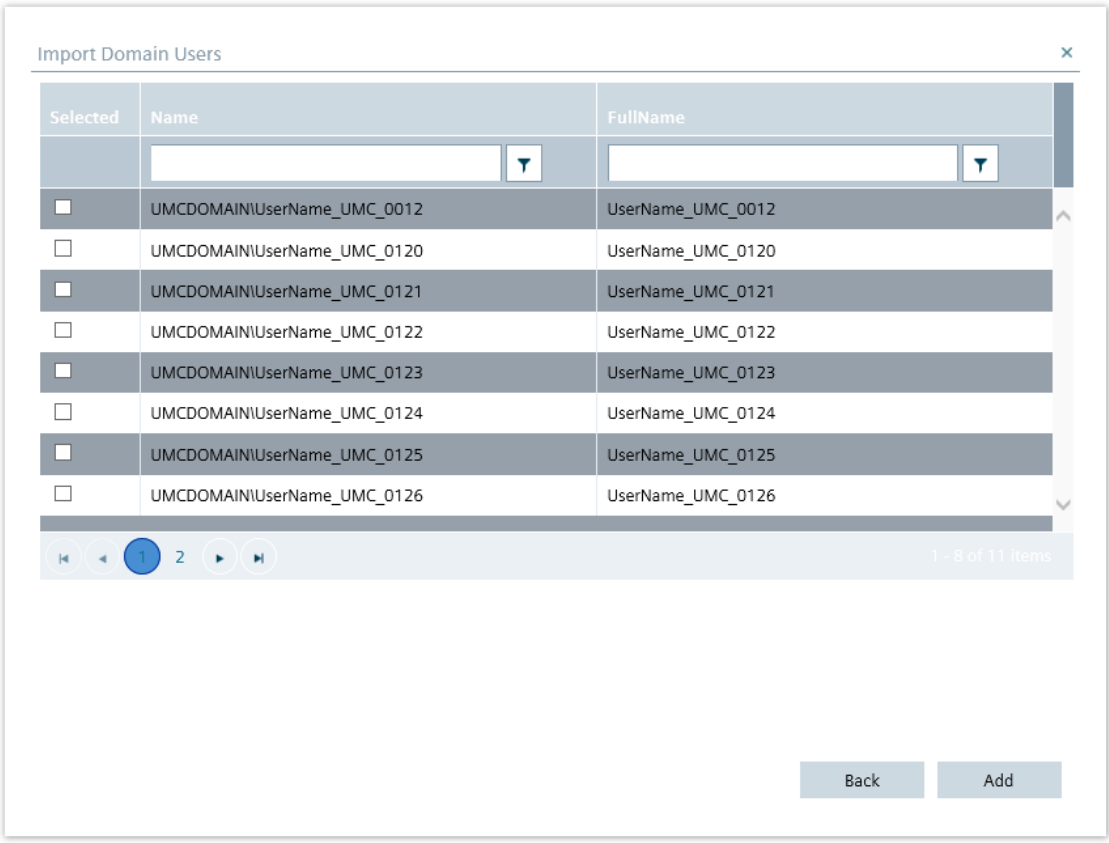
Procedure

1. In the **Users** page, click **Import Users**: the following dialog box appears.

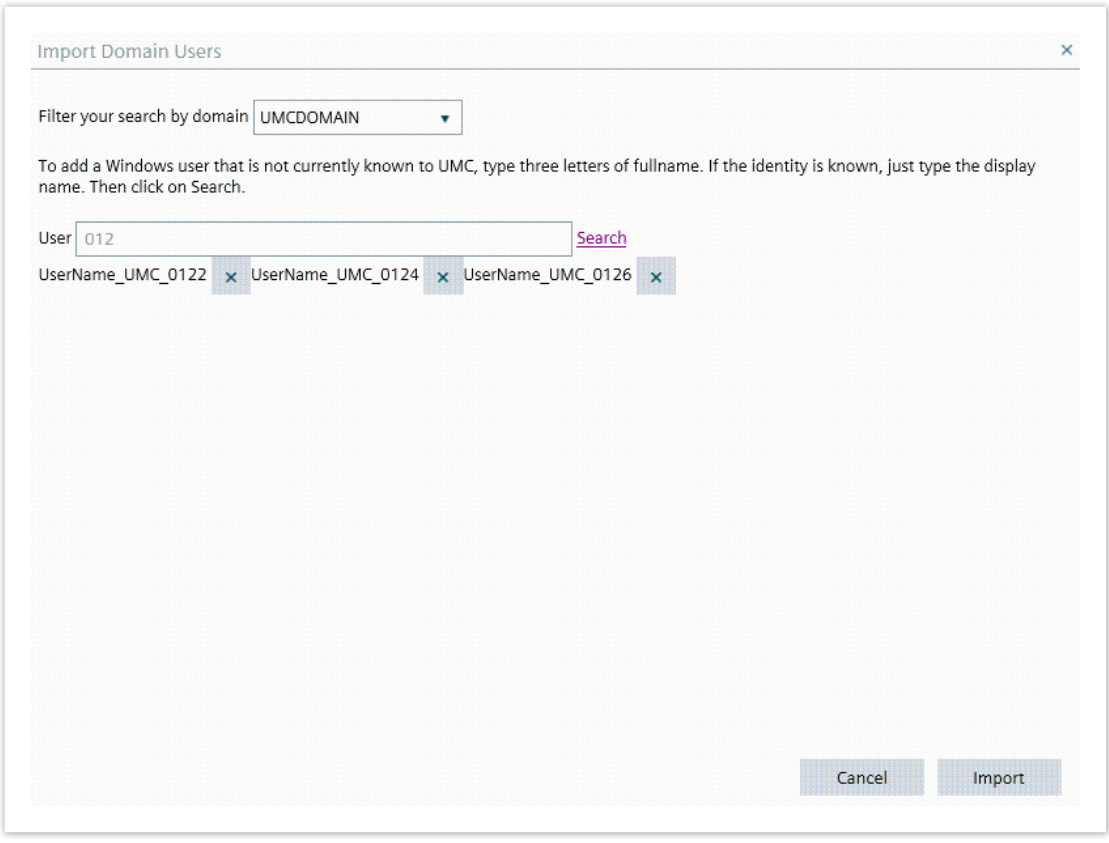


2. Enter the search criteria and click **Search**. The search criteria must contain at least the three initial characters of the user name. If you want to search by inserting other characters contained in the name, insert an * before the string. The search is perfomed in the following Active Directory fields: user name (sAMAccountName), user full name (displayName), and

common name (cn). The following dialog box appears:



3. Select the users you want to import and click **Add**. The selected users are displayed as in the following example:



4. Click **Import** to import the selected Active Directory users into the UMC database. Windows groups associated with these users are not imported into UMC database. For imported users, the user authentication is performed against the Windows System.

4.4 Unlocking a User

Important:

You cannot explicitly lock a user. To lock a user you have to insert a wrong password a number of times which depends on the global account policies **SL_ENABLE_LOCK_AFTER_NATTEMPTS** and **SL_MAX_LOGIN_ERRORS**. See the *UMX User Manual* for more information on how to list and modify the account policies.

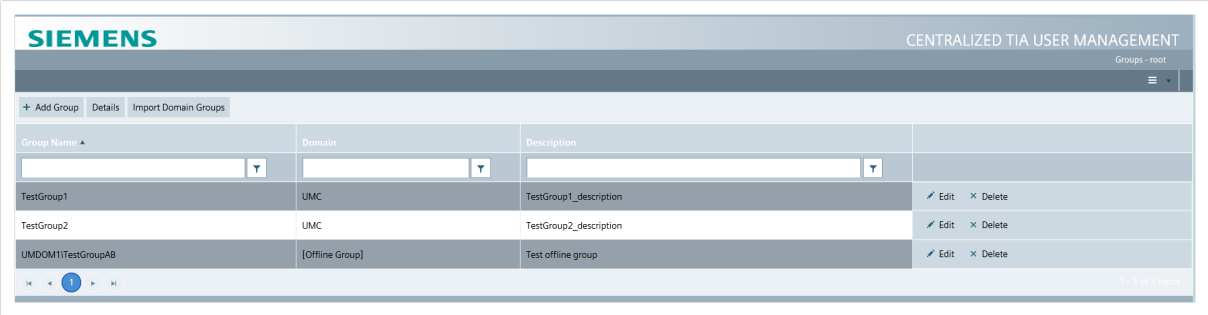
Procedure

1. To unlock a previously-locked user, select the row of the user to be unlocked.
2. Click **Unlock User**. The **Status** tab of the user details dialog box displays if the user is locked or not and can be used to unlock the user.

5 How to Manage Groups

Accessing the Page

From the menu on the upper right-hand corner of **UMC Home page**, select **Groups**. The **Groups** page is displayed.



Available Operations

Below each column name, a filter box allows you to filter the content of the selected column. In this page you can perform the following operations:

- create a group;
- update a group;
- import a group from Active Directory;
- delete a group.

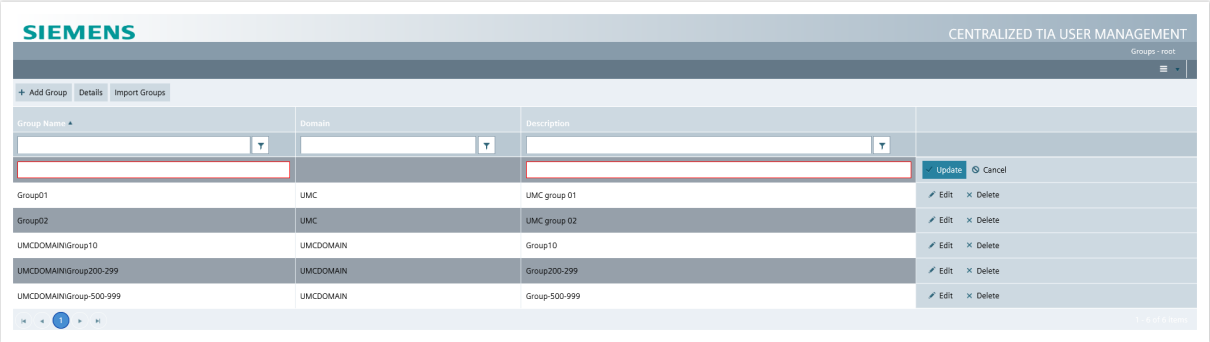
When you manage groups, refer to the corresponding **umx** commands for field constraints (see *UMX User Manual*).

5.1 Creating a Group

You can create one or more groups by following this procedure:

Procedure

1. Click **Add Group.**
2. In the new blank boxes that are displayed at the top of the columns, add the group details.
3. (Optional) You can flag the group as offline in the **Domain** column;
4. Perform either of the following actions:
   – click **Update** to confirm the creation;
   – click **Cancel** to cancel the insertion.



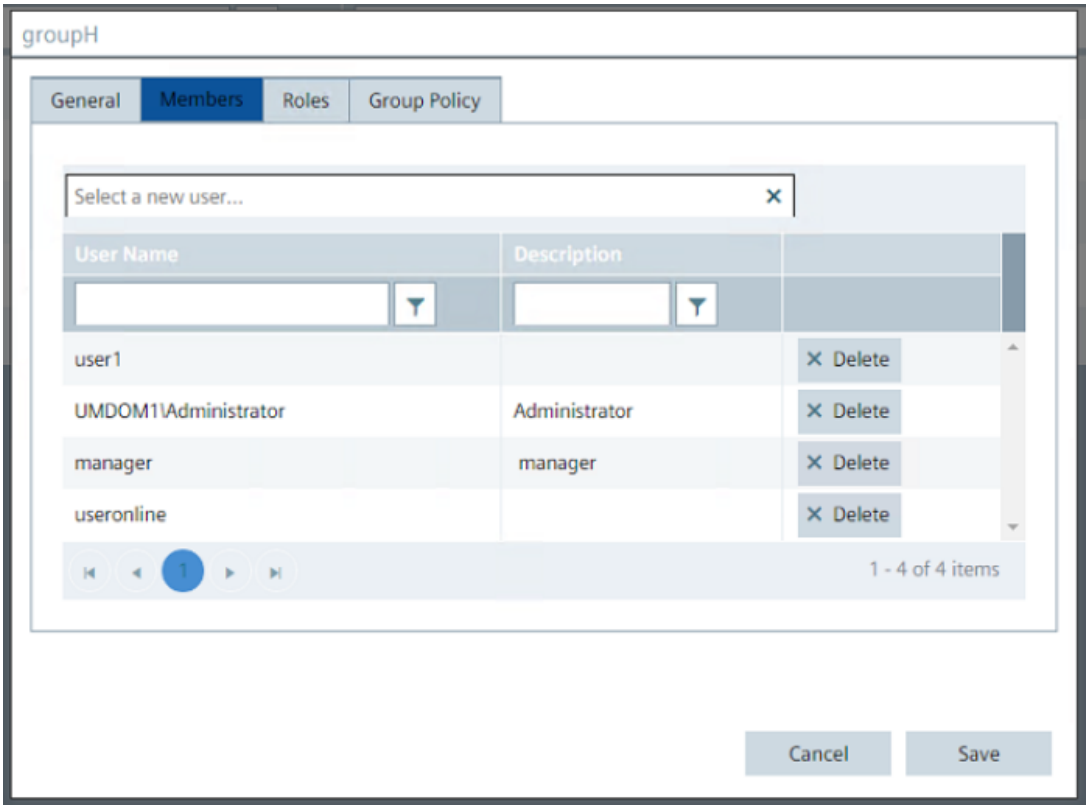
Offline Groups

If the group is created offline the description can contain an ldap query to be used by the UMC provisioning service to find the Active Directory group and populate the UMC group with its users. See User Manager Group for details about offline groups and the format of the description field to be used to configure the import.

5.2 Updating a Group

Editing Group Details

1. From the **Groups** page, select a row and click **Edit** to edit the group main information directly in the grid.
2. If you want to insert or edit additional group details, select a row and click **Details** in the upper left-hand corner of the grid. The following dialog box is displayed:



Available Operations

Each tab contains the group details that you can edit in that tab. Only specific properties whose editing needs additional explanations are described. In the following tabs you can:

- Associate Users with Groups (**Members** tab).
- Associate Roles with Groups (**Roles** tab). For more details, see Associating a Role with a User.
- Configure the Secure Application Data Support offline behavior for the Group (**Group Policy** tab).

Associating a User with a Group

1. Type the user name in the box at the top of the grid. This box provides the autocomplete functionality so that only the first letters of the name can be typed.
2. Select the required user and click **Save**.

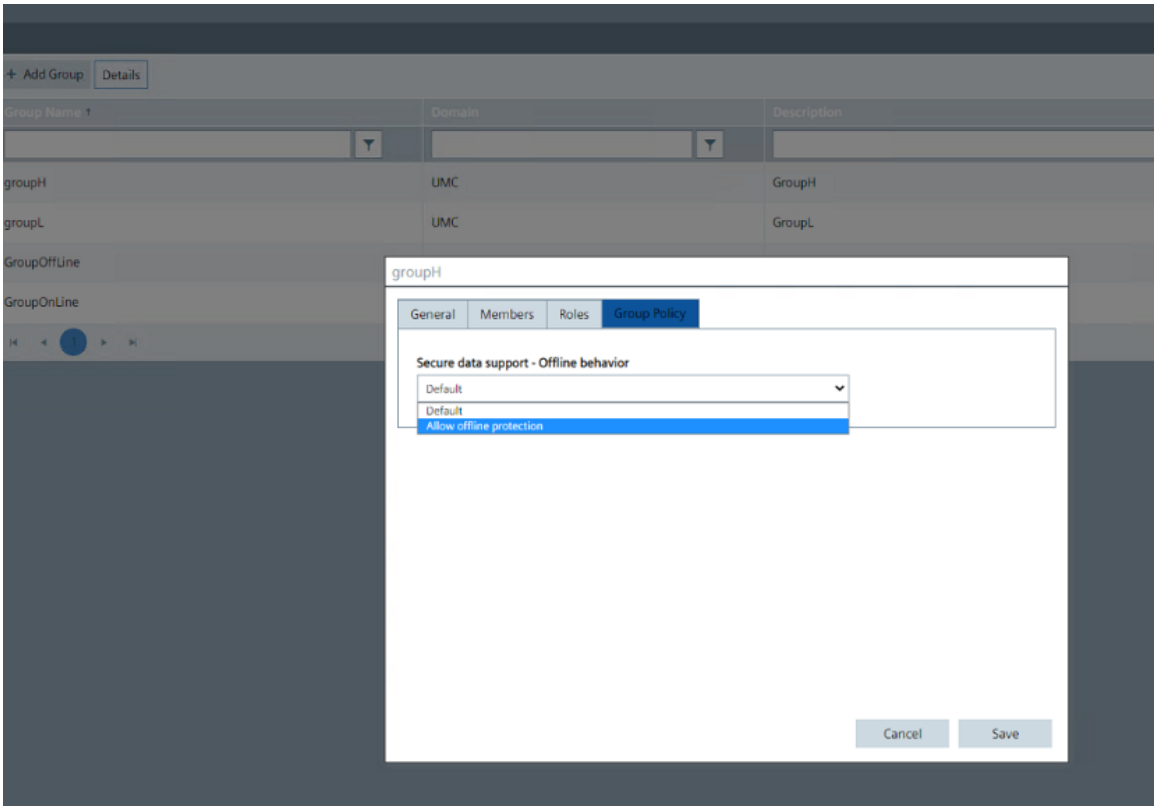
Configuring the Secure Application Data Support offline behavior

On a UMC server, the Secure Application Data Support is available when the server is connected to the UMC ring server. When offline, Secure Application Data Support is not available.

It is possible to configure on a Group that the Users belonging to that Group are allowed to use Secure Application Data Support also when the UM server is disconnected from the UMC ring.

In order to configure it:

1. In the drop-down list "Secure Application Data Support - Offline behavior" select "Allow offline protection"
2. Click **Save.**



The "Default" value, shown by default in the drop-down list, means that Secure Application Data Support is not allowed on a UM server when offline.

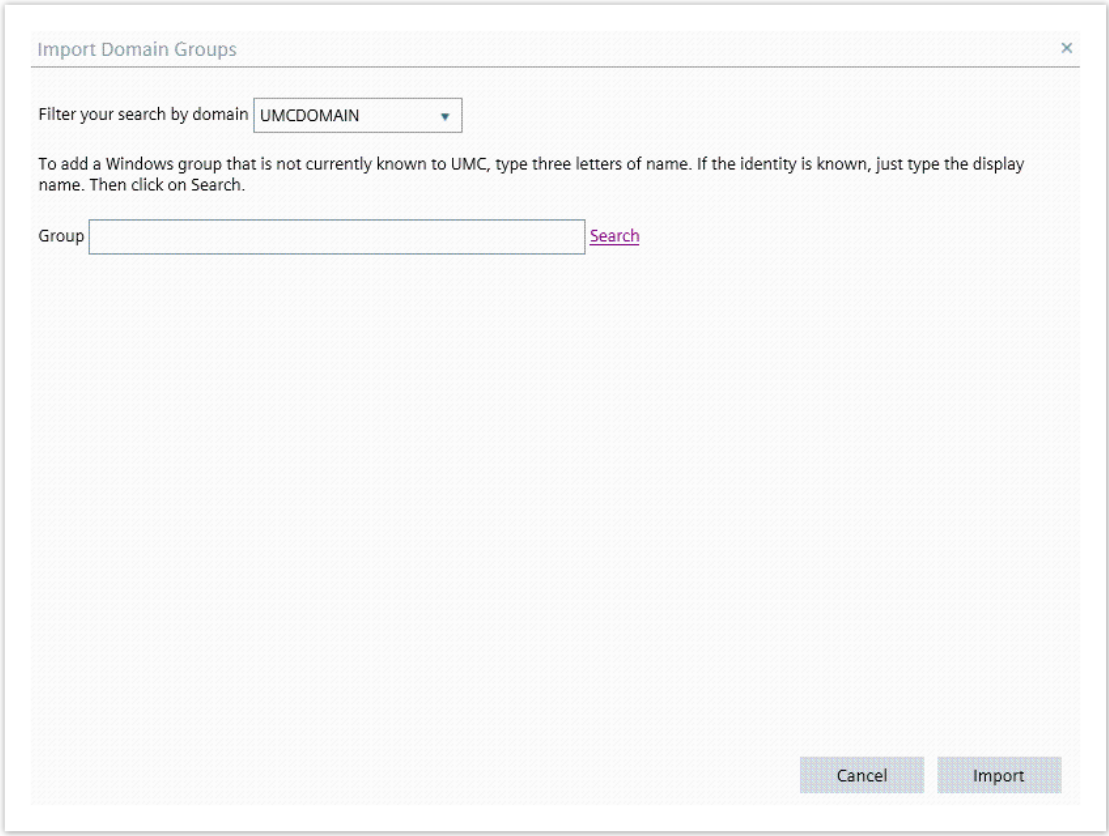
5.3 Importing a Group from Active Directory

The import of groups implies a search on Active Directory that can take a considerable amount of time and can return zero results when exceeding AD administration limits. It is strongly suggested that you perform restricted searches.

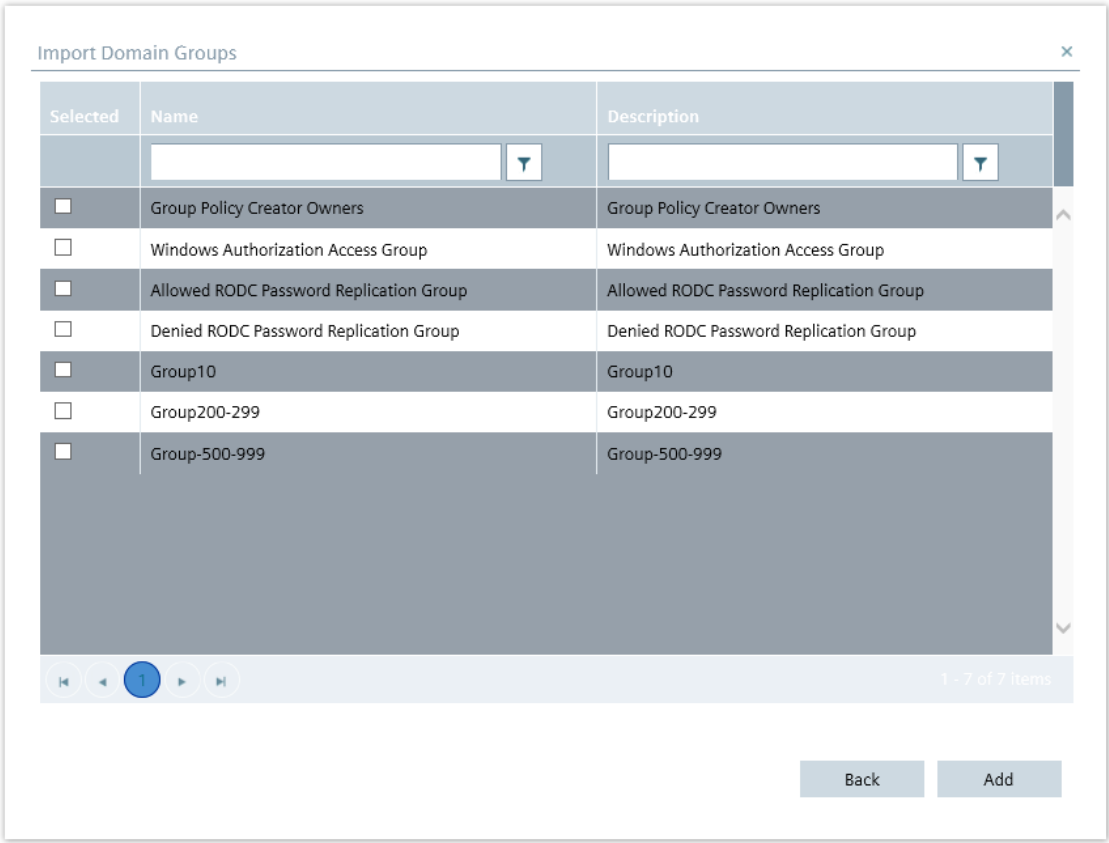
Procedure

1. In the **Groups** page, click **Import Domain Groups**: the following dialog box appears.
   Permalink: https://momwiki01.industrysoftware.automation.siemens.com/display/UMC/

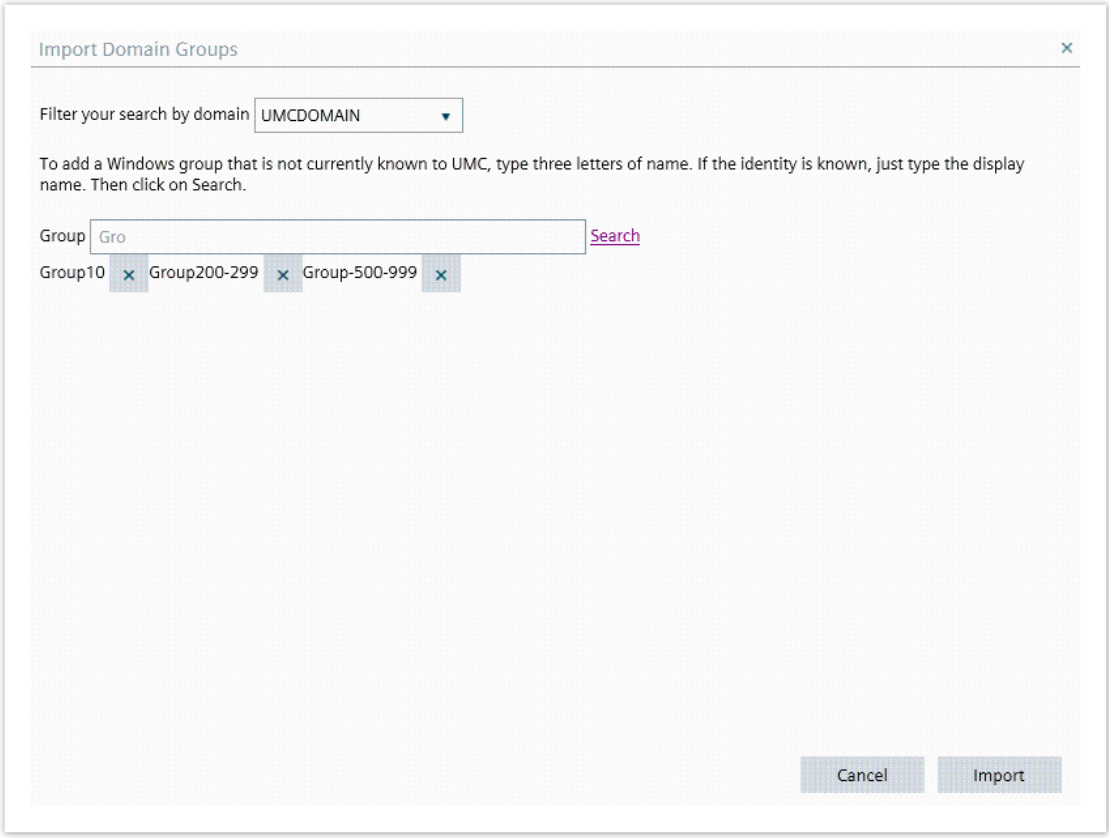
Importing+a+Group+from+Active+Directory



2. Enter the search criteria and click **Search**. The search field is the group name (cn Common-Name). The following dialog box appears.



3. Select the group you want to import and click **Add.** The selected groups are displayed as in the following example:



4. Click **Import** to import the selected Active Directory groups and the associated Active Directory users into the UMC database.

Active Directory Group Update

By default AD recursive groups are not supported. Only direct members are imported into UMC. For these users, the authentication is performed against the Windows System and the imported fields are not editable. As a result, the following rules are applied:

- Tab **General**: no fields can be modified.
- Tab **Members**: group members cannot be modified, users cannot be added to nor deleted from the group; as a consequence, users imported via an AD group cannot be deleted.
- Tab **Roles**: roles can be modified.

Additional configurations

- It is possible to enable the import of users belonging to nested groups. As a result, the users of nested groups are imported and bound to the parent group; the nested group itself is not imported. See UMC installation Manual, Appendix, Additional Provisioning Configurations for how to enable it.
- In case it is required to import an Active Directory group not by its Common Name (CN), the group must be created offline and the description can be used for configuring the import criteria. See User Manager Group for details.

Important:

The import of all the Active Directory users belonging to a group may take a considerable amount of time (usually in the order of minutes), depending on the number of members. During the user import, the Web UI can be used to perform other operations.

5.4 Deleting a Group

CAUTION:

- If a group is created from scratch in the UMC database and has associated users, all the associations are deleted. Users are not deleted.
- If a group is imported from Active Directory in the UMC database and has associated users, all the users which do not belong to other groups are deleted.

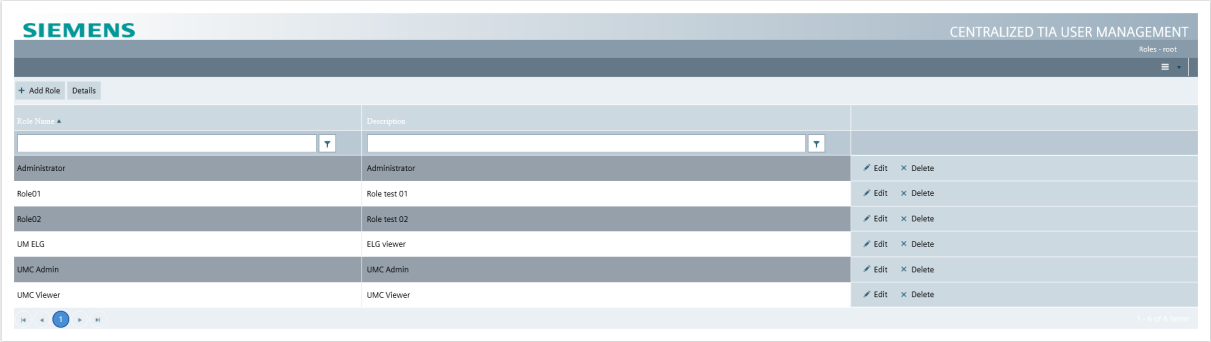
Procedure

1. Select the group row.
2. Click **Delete**.

6 How to Manage Roles

Accessing the page

From the menu on the upper right-hand corner of **UMC Home page**, select **Roles**. The **Roles** page is displayed.



Available Operations

Below each column name, a filter box allows you to filter the content of the selected column. In this page you can perform the following operations:

- create a role;
- update a role;
- delete a role.

When you manage roles, refer to the corresponding **umx** commands for field constraints (see *UMX User Manual*).

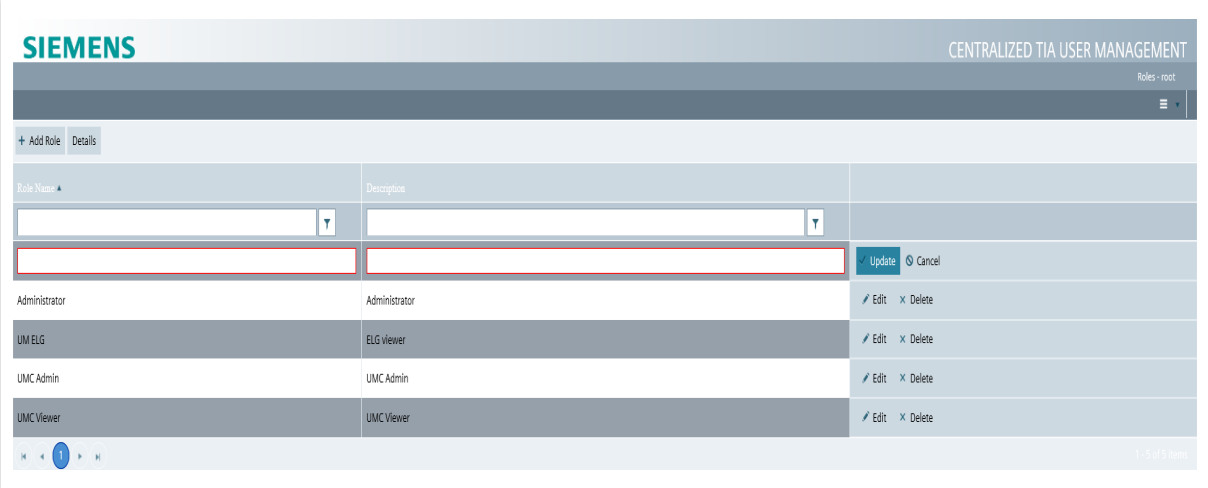
6.1 Creating a Role

You can create one or more roles by following this procedure. A number of roles are automatically created by the system during UMC configuration.

Procedure

1. Click **Add Role**.
2. In the new blank boxes that are displayed on top of the columns, add the role details. The number of roles present in the system cannot exceed 200.
3. Perform either of the following actions:
   – click **Update** to confirm the creation;
   – click **Cancel** to cancel the insertion.

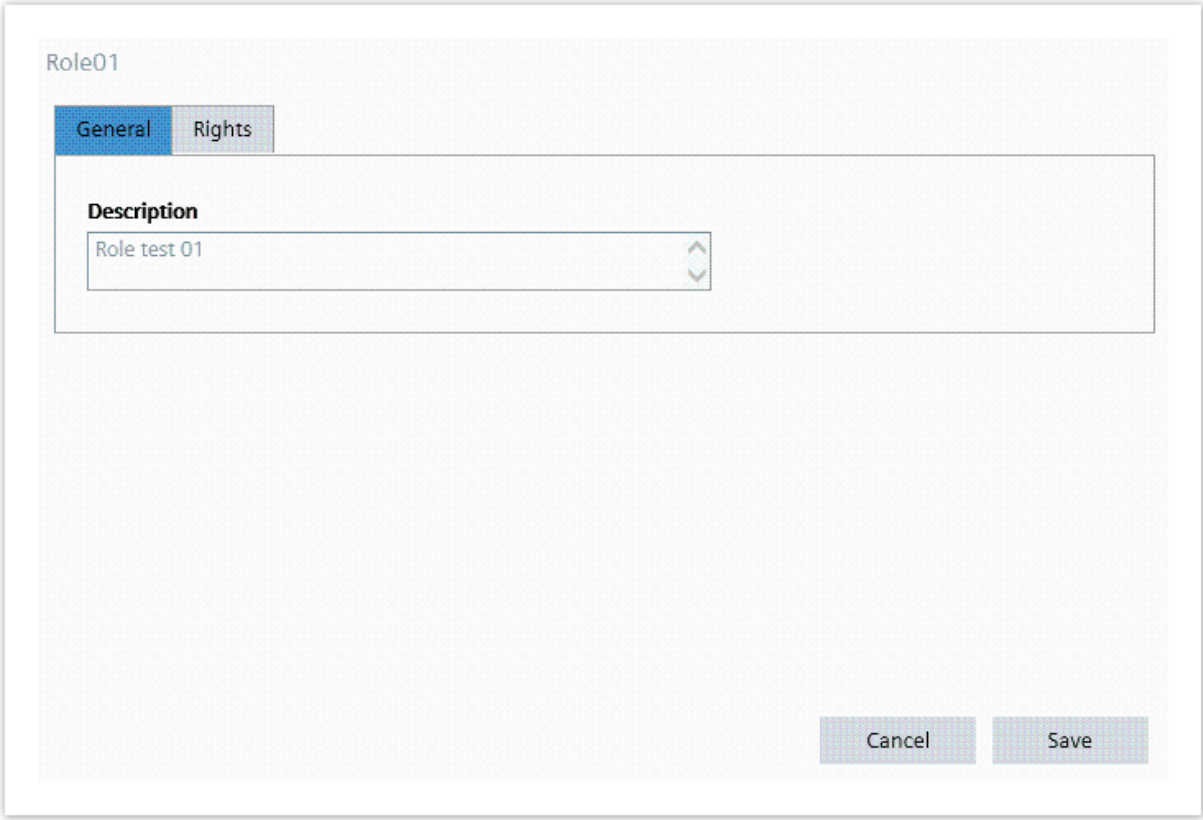
Note: Due to a database constraint on the role identifiers, you may get an error message saying that no more role identifiers are available. In that case, if you want to create new roles, you must purge the existing role first using the corresponding **umconf** command. See the *User Management Component UMCONF User Manual* for more details.



6.2 Updating a Role

Editing Role Details

1. From the **Roles** page, select a row and click **Edit** to edit the role main information directly in the grid.
2. If you want to insert or edit additional role details, select a row and click **Details** on the upper left-hand corner of the grid. The following dialog box is displayed.



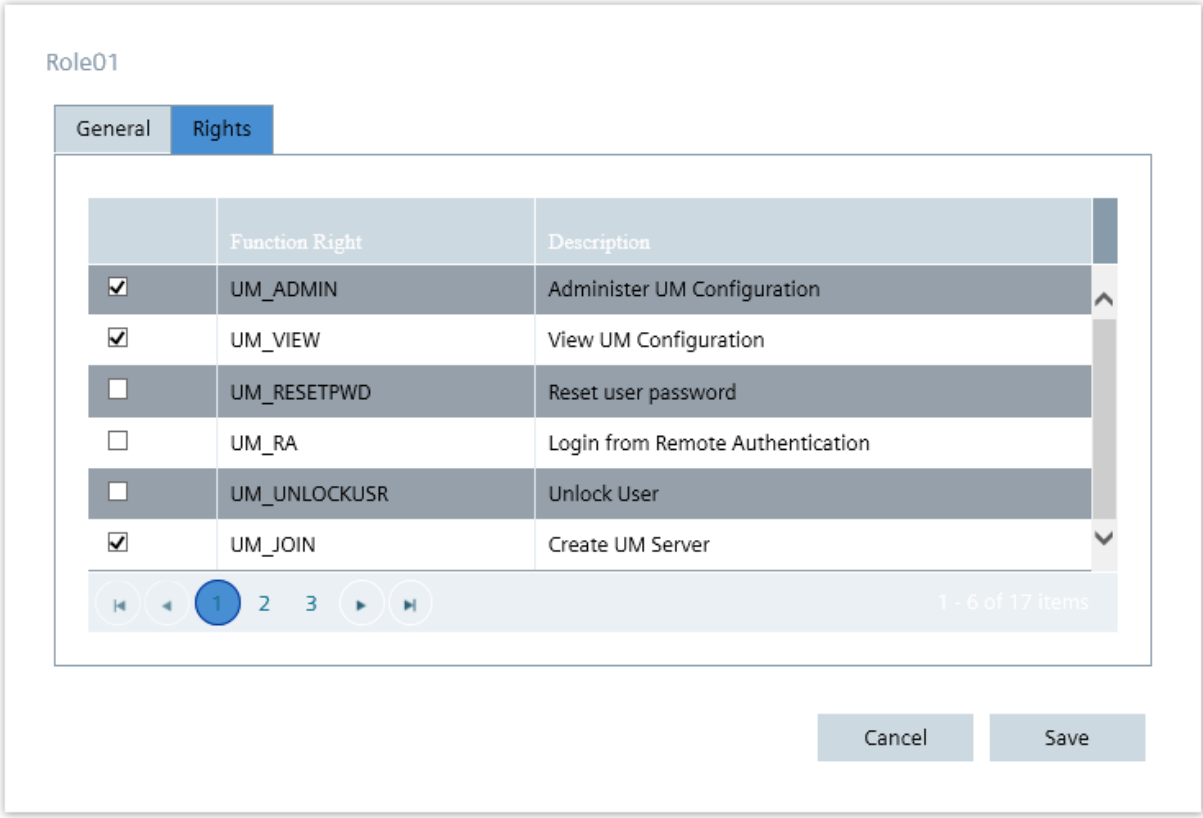
Available Operations

Each tab groups the role details that you can edit in that tab. In the following tab you can:

- Associate function rights with roles (**Rights** tab).

Associating a Function Right with a Role

1. Select the **Function Right** check box to associate the corresponding function right with the role.
2. Click on the **Save** button to save the modifications.


Role01
General
Rights
Function Right
Description
UM_ADMIN
Administer UM Configuration
UM_VIEW
View UM Configuration
UM_RESETPWD
Reset user password
UM_RA
Login from Remote Authentication
UM_UNLOCKUSR
Unlock User
UM_JOIN
Create UM Server
1
2
3
1 - 6 of 17 items
Cancel
Save

7 How to Manage Account Policies

Account policies are used to implement the policies on authentication (like the automatic lock of the user after wrong login attempts) and on password validation. They are divided into two main groups:

- **user account policies** that are defined at user level so that each user can have its own rules on authentication;
- **global account policies** that are defined at system level and are the same for all the users.

User account policies can also be managed in the **Users** page.

When you manage account policies, refer to the corresponding **umx** command for additional field constraints (see *UMX User Manual*).

Note: The maximum duration for the password expiration is 1827 days (approximately 5 years).

Accessing the page

From the menu on the upper right-hand corner of **UMC Home page**, select **Account Policies**. The **Account Policies** page is displayed.

Available Operations

In this page you can perform the following operations. Only specific fields whose editing needs additional explanations are described.

- Define password structure.
- Define password duration, lock and reuse settings.
- Perform advanced configurations.

Defining the Password Structure

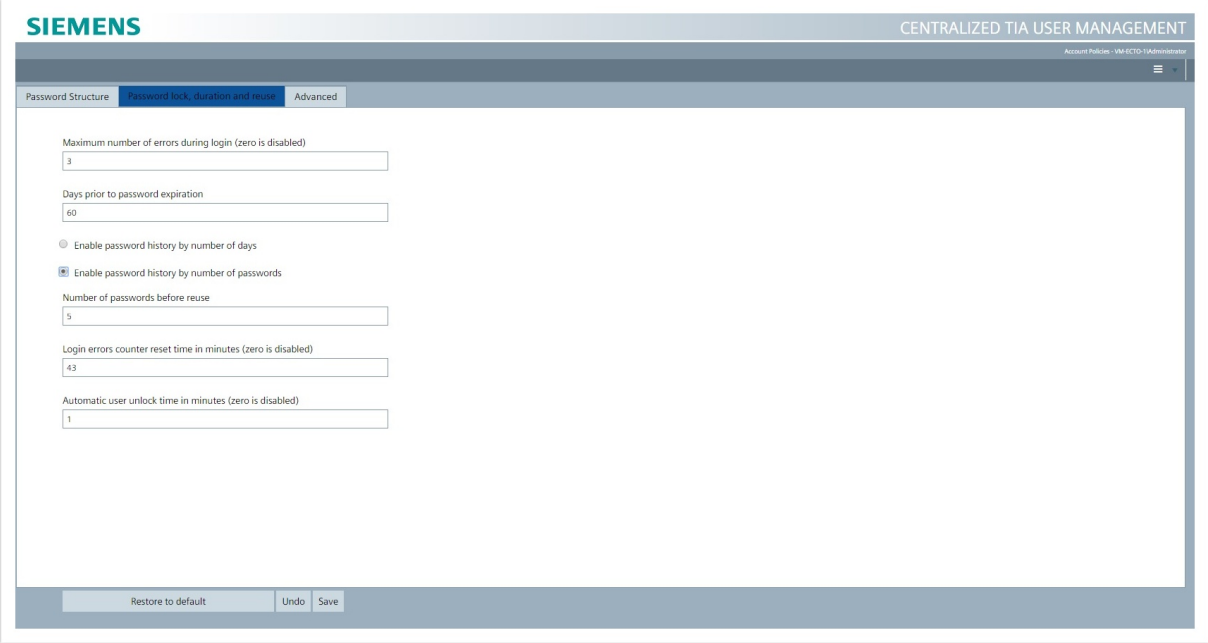
In the **Password Structure** tab, fill the available fields with the values you want to set for your passwords. You can also enable the administrative password policy check, so that administrative users can only set passwords which meet the policy which have been set, this does not apply to password reuse policies.

If the value in the **Password Minimum Length** and **Password Maximum Length** fields are set to 0, the check is disabled. Empty passwords are not allowed.

Defining password duration, lock and reuse settings

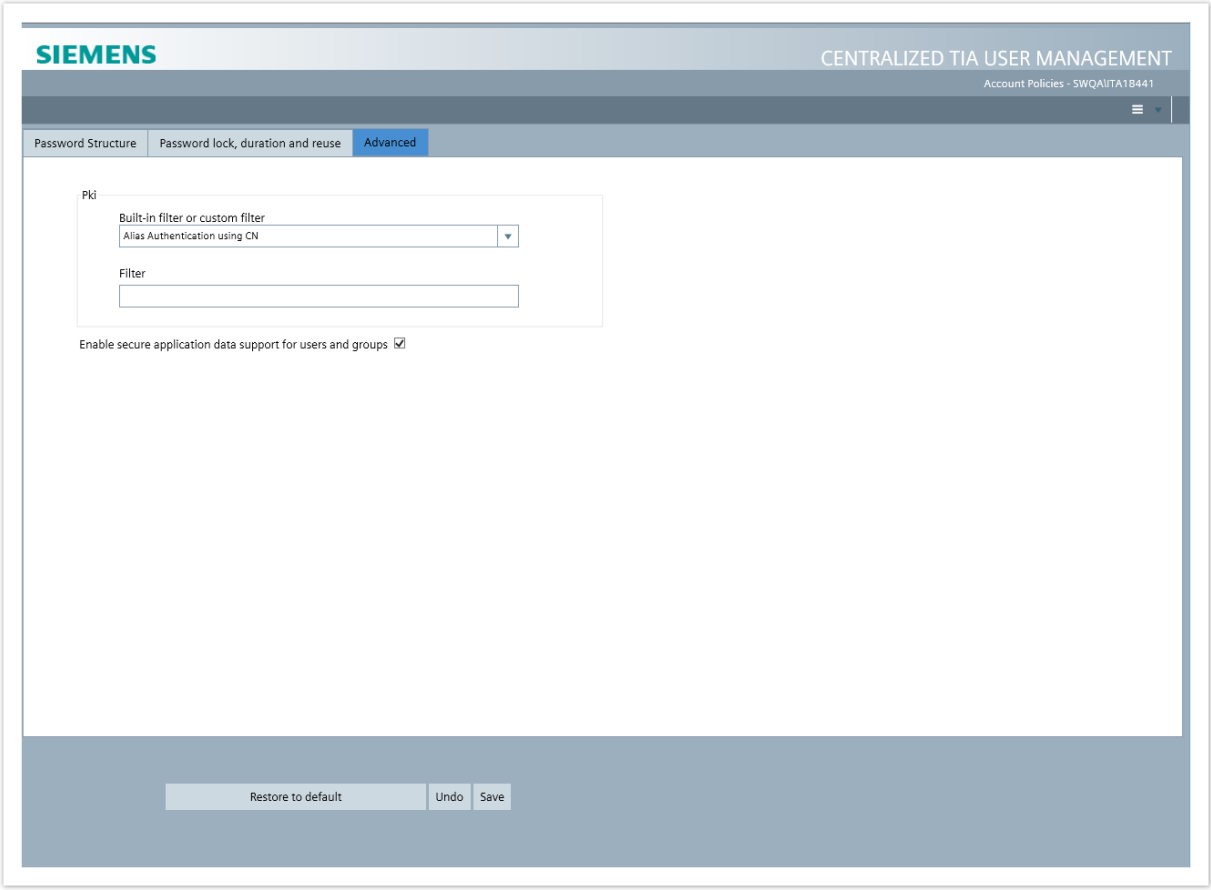
In the **Define password duration, lock and reuse settings** tab:

1. Set the maximum number of errors that can occur during the login before the user is locked. If the value is set to 0, the lock is disabled.
2. Set the number of days prior to password expiration.
3. Select one of the following:
   – **Enable password history by number of days** and then set the minimum days to wait before reusing a password.
   – **Enable password history by number of passwords** and then s et the number of passwords before use .
4. Set the time (in minutes) between two login operations to reset the Login error counter. If the value is set to 0, the reset of the Login error counter is disabled.
5. Set the time (in minutes) for the automatic user unlock. If the value is set to 0, the automatic unlock of the user is disabled.



Performing Advanced Settings

1. In the **Advanced** tab, in the **Pki** area, from the **Built-in filter or custom filter** drop-down menu, select the field to be used for user authentication via smart card; the following options are available:
   – **Authenticate using CN**
   – **Alias Authentication using CN**
   – **Authentication using filter on Subject**
   – **Alias Authentication using filter on Subject**
   – **Authentication using filter on Alternate Subject**
   – **Alias Authentication using filter on Alternate Subject**
2. Select the **Enable secure application data support for users and groups** check box to enable the SADS functionality. SADS capabilities at application level can be enabled via **umx** or Web UI by modifying an account policy. For what concerns the subject level, this can only be done via **umx**. For more details, see *UMX User Manual*.
3. Click **Restore to default** to restore the global account policy default values or click **Save**.


SIEMENS
CENTRALIZED TIA USER MANAGEMENT
Account Policies - SWQA\TA18441
Password Structure
Password lock, duration and reuse
Advanced
Pki
Built-in filter or custom filter
Alias Authentication using CN
Filter
Enable secure application data support for users and groups
Restore to default
Undo
Save

8 How to Manage IdP Configurations

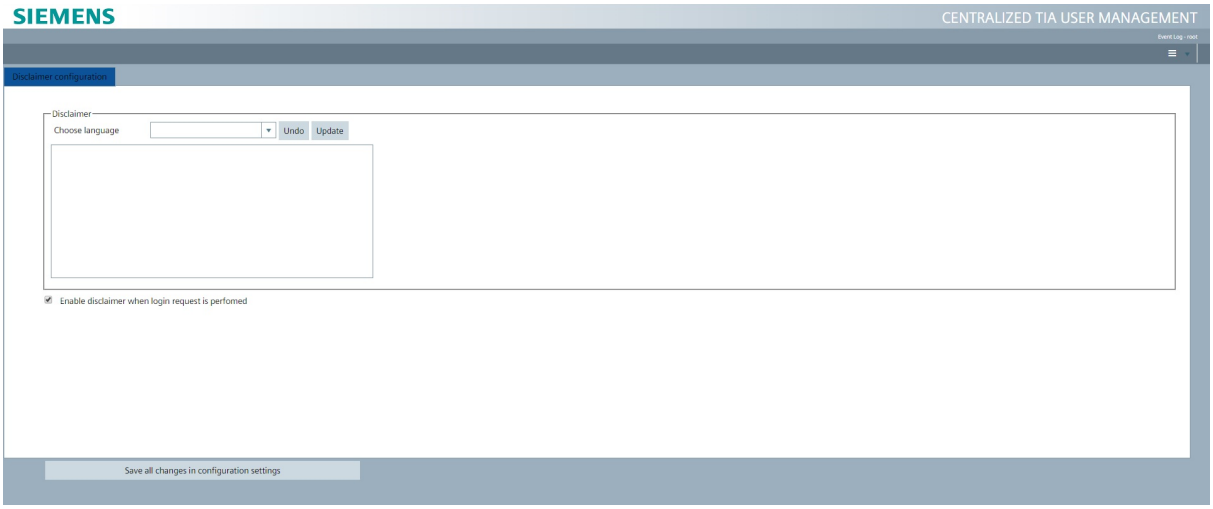
This page along with its tabs allow you to:

- Manage disclaimers and to customize the content of the disclaimer in: English, French, Spanish, German, Italian and Chinese.
- Manage authentication options, for example enable specific types of authentication and set their security level.
- Manage languages, enable or disable built-in languages and add custom languages not provided by UMC.

Note: Enabling or modifying the disclaimer sets a centralized configuration if one is not already present. If you performed specific configuration on the local file they may need to be applied to the central configuration or overridden.

Accessing the Page

From the menu on the upper right-hand corner of **UMC Home Page**, select **IDP Configuration**. The **IDP Configuration** page is displayed.



8.1 Configuring Disclaimers

UMC offers the possibility to display or hide disclaimers and to customize the content of the disclaimer in: English, French, Spanish, German, Italian and Chinese.

Note: Enabling or modifying the disclaimer sets a centralized configuration if one is not already present. If you performed specific configuration on the local file they may need to be applied to the central configuration or overridden.

Enabling Disclaimers

To enable the visualization of disclaimers select the **Disclaimer Configuration** tab and select the **Enable disclaimer when login request is performed** checkbox.

Customizing Disclaimers

Disclaimers can be customized for each of the six standard languages.

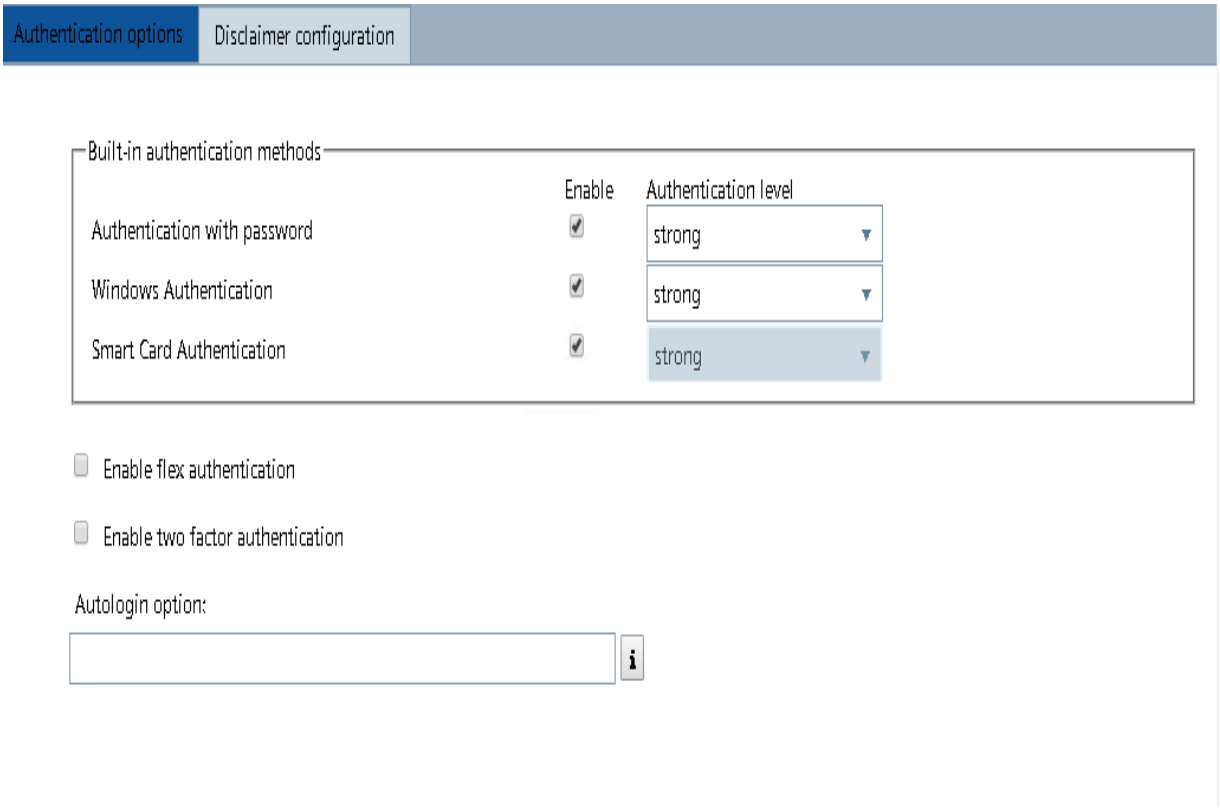
Procedure

1. select the **Disclaimer Configuration** tab.
2. Select the language from the drop down menu.
3. Modify the disclaimer as required and click **Update**.
4. Click **Save all changes to configuration settings**.

Note: Only the html tags br (break) and b (bold) can be used in the disclaimer.

8.2 Configuring Authentications Options

The **Authentication options** tab allows you to enable and disable authentication methods and specify their security level.



CAUTION:

The configuration which can be specified on this page can result in no longer being able to login into the web UI even with the root user. Verify that at least one authentication level is strong or that two factor authentication is configured and enabled, see *UMC Installation Manual* for more information.

Enabling/disabling Built-in Authentication Methods

The enable checkboxes for built-in authentication methods enable the authentication methods and set the value on the centralized configuration file. See *UMC Installation Manual* for more information.

Procedure

1. Click the **Authentication Options** tab.
2. Select the check box relative to the required type of authentication.
3. If required, select a security level from the drop down menu.
4. Click **Save all changes to configuration settings**.

Enabling/disabling Additional Authentication Methods

The enable checkboxes for additional authentication methods enable the authentication methods and set the value on the centralized configuration file. See *UMC Installation Manual* for more information.

Procedure

1. Click the **Authentication Options** tab.
2. Select the check box relative to the required type of authentication: Enable two factor authentication (for 2FA by time-based one-time password) or Flex Authentication.
3. Click **Save all changes to configuration settings**.

Setting the Security Level for Built-in Authentication Methods

The security level can be specified for the built-in authentication methods, except for smart card authentication, to specify how securely information is passed in the IdP claim so that the third party application can determine the authentication security level. In UMC Web UI, it can only be used if the authentication is **standard** or **strong**. The possible values are:

- **weak**
- **standard**
- **strong**

Procedure

1. Click the **Authentication Options** tab.
2. Select a security level from the drop down menu next to the authentication method.
3. Click **Save all changes to configuration settings**.

Configuring Auto Login Methods

Autologin is a feature that allows to define one or more authentication methods with which the identity provider tries to login automatically just after the loading of the authentication page.

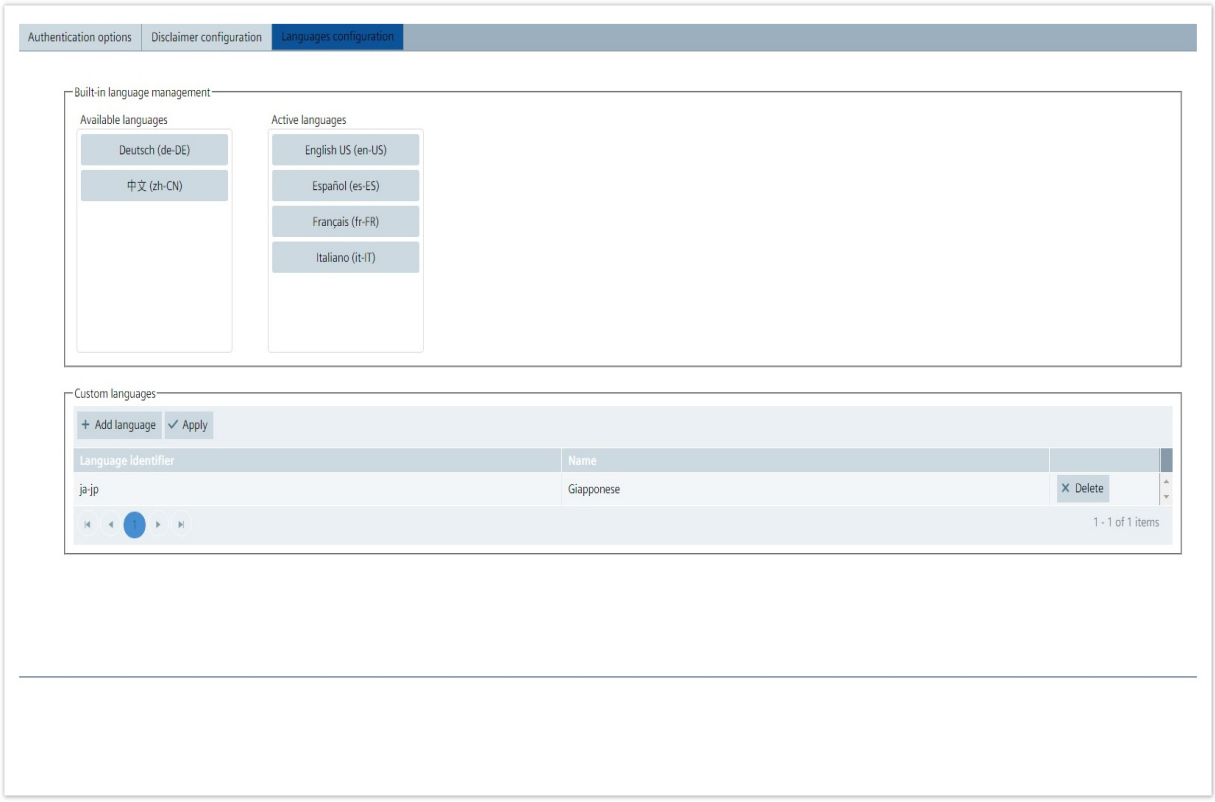
Procedure

1. Click the **Authentication Options** tab.
2. Specify the authentication method/s to use for automatic login, using the syntax: <iwa|pki|pluginname>
   – Windows authentication: "iwa"
   – Smart Card authentication: "pki"
   – Desktop plugin, Web plugin or Flex authentication: "pluginname", the plugin name is the name used for plugin registration.

   It is possible to define multiple authentication methods by dividing each method with "|". The identity provider will get the list of methods and use the first one available in the list. Example of syntax to use for autologin: "iwa|pki|32bitStateless|WebAdapter".
3. Click **Save all changes to configuration settings**.

8.3 Configuring Languages

The **Languages configuration** tab allows you to choose which languages to use from those provided by UMC and give you the possibility to add custom languages.



Enabling/disabling built-in languages

In the **Built-in languages management** area you can enable or disable the built-in languages installed by UMC (English, French, Spanish, German, Italian and Chinese).

The list on the left displays the built-in disabled languages and the list on the right displays the enabled languages. To enable or disable a built-in language, drag and drop a language from one list to the other.

Adding custom languages

1. In the area **Custom languages,** click **Add language**.
2. Insert a language identifier and a name with which the language will be displayed in the system. The language identifier must be compliant with RFC 5645.
3. Click **Apply**.
4. Click **Save all changes**.

Creating and providing resources file with translations

After configuring a new language, you have to install in the system the resources files that contain the translations for the new languages.

It is necessary to provide two different resource files, one for the UMC webUI application and one for the login page of the Identity provider. They must be copied in the following paths:

- **C:\Program Files\Siemens\UserManagement\WEB\Umc\js\common\language_files** for the UMC webUI application.
- **C:\Program Files\Siemens\UserManagement\WEB\IPSimatic-Logon\IDPAuthSite\locales** for the login page of the Identity Provider application.

In these two paths you can find resource files for existing languages and use them as template to create the new resource files for the custom language.

CAUTION:

- Each new resource file must be named like the resource files already present in the paths, by including the language identifier inserted during the configuration. In the example above, the file must be named **umc.ja-jp.json**.
- In the new resource file the value of the property **language** must match the value of the **Language identifier** inserted in the **Custom languages** tab. See the example below.

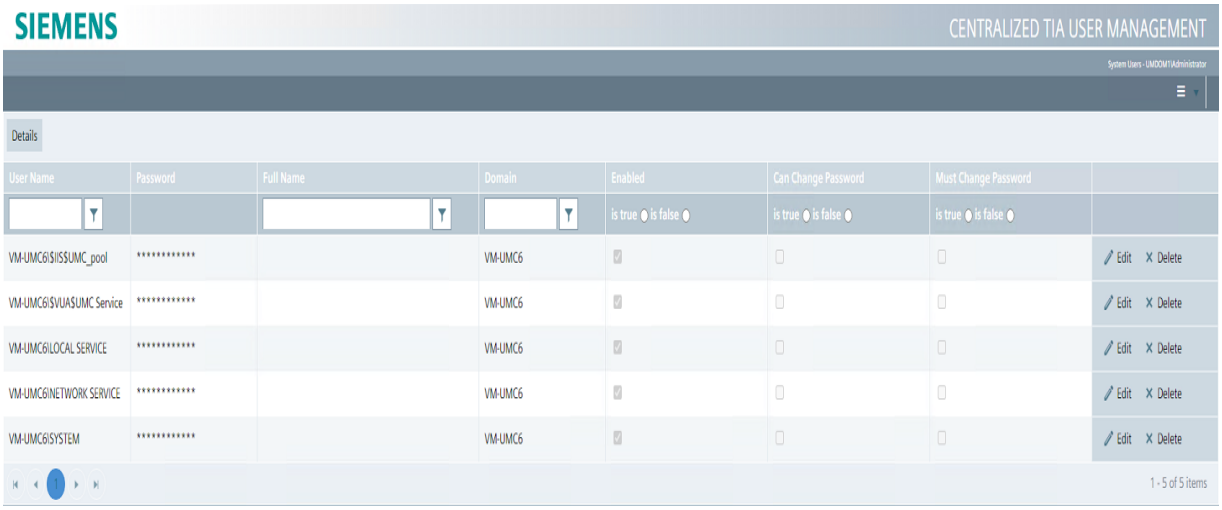
Example

```
"language": "ja-jp",
  "keys": {
    "sessionExpiredLabel": "Session Expired",
```

9 How to Manage System Users

Accessing the page

From the menu on the upper right-hand corner of **UMC Home page**, select **System Users**. The **System Users** page is displayed.



Available Operations

In this page you can view all the System Users that have been imported into UMC (via umx): Windows local Users, Virtual service Accounts, IIS App Pool Identities . Those System Users are not listed in the Users page.

Below each column name, a filter box allows you to filter the content of the selected column. In this page you can perform the following operations:

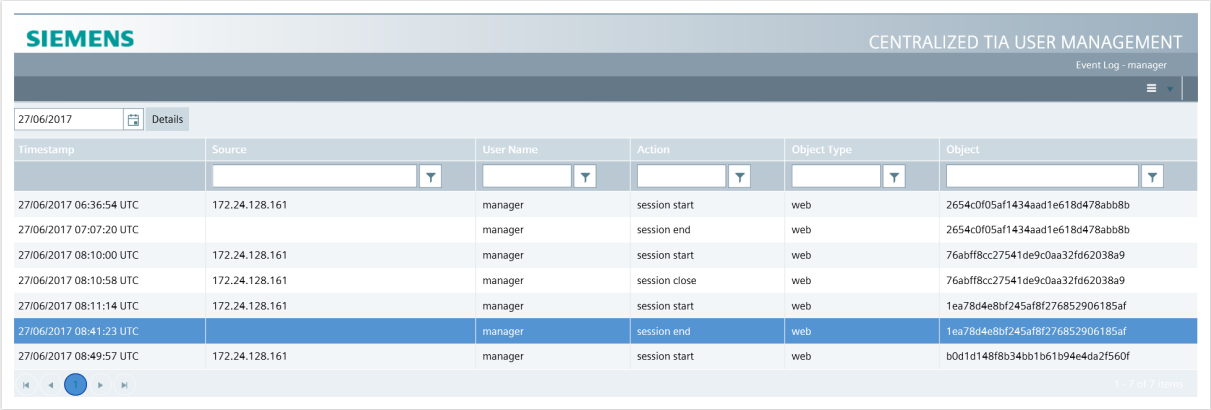
- update a user;
- delete a user.

When you manage users, refer to the corresponding **umx** commands for field constraints (see *UMX User Manual*).

10 How to Display the Event Log

Accessing the page

From the menu on the upper right-hand corner of **UMC Home page**, select **Event Log**. The **Event Log** page is displayed.

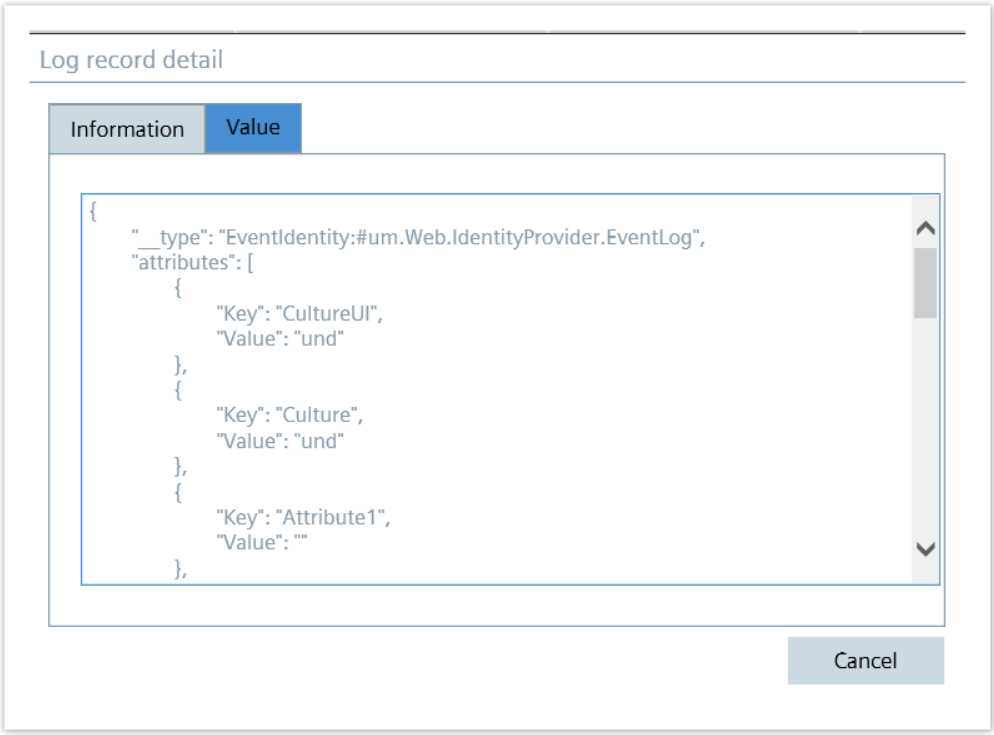


Prerequisites

Users must have either the function rights **UM_VIEW** and **UM_VIEWELG or UM_Admin** to access the **Event Log** page.

Procedure

1. Select a row and click **Details** to display the event log record details.
2. In the **Log record detail** dialog box, the **Value** tab displays the value in JSON format.


Log record detail
Information
Value
{
"__type": "EventIdentity:#um.Web.IdentityProvider.EventLog",
"attributes": [
{
"Key": "CultureUI",
"Value": "und"
},
{
"Key": "Culture",
"Value": "und"
},
{
"Key": "Attribute1",
"Value": ""
},
Cancel

11 Error Codes

In case of errors, the Web UI returns either a text error message or the last error code (hexadecimal format) returned by the UMC APIs invoked during the operation execution. See UMC APIs Error Codes for more details.

11.1 UMC APIs Error Codes

All the UMC APIs return a boolean value or an object handle. If the API is successful, the returned boolean value is true or the object handle is well formed; otherwise the returned boolean value is false, or null is returned instead of the object handle. If the API fails an error code can be retrieved calling the **SL_GetLastError** method. **SL_RESULT** defines the type of error. In what follows we list the possible error codes.

Generic Errors

Name	Hexadecimal Value	Decimal Value	Description
SL_SUCCESS	0X00	0	No errors have occurred.
SL_GENERROR	0X01	1	Generic error.
SL_BAD_HANDLE	0x114	276	Internal error for invalid handle.
SL_NOSESSION	0X30	48	The Web session is expired.

Authentication Errors

Name	Hexadecimal Value	Decimal Value	Description
SL_USERLOCKED	0X02	2	The user for whom you want to perform the authentication is locked.
SL_USERDISABLED	0X03	3	The user for whom you want to perform the authentication is disabled.
SL_WRONGUSERNAMEPASSWORD	0X04	4	During the authentication phase, the user name or password are incorrect.

Name	Hexadecimal Value	Decimal Value	Description
SL_PASSWORDPOLICYVIOLATION	0X05	5	Password policy violation (determined by UMC account policies). For a detailed list of Account Policies, see *User Management Component API SDK Developer Manual*.
SL_USERMUSTCHANGEPASSWORD	0X06	6	The user password must be changed.
SL_PASSWORDEXPIRED	0X07	7	The user password is expired.
SL_FAILED	0X0A	10	Generic operation failed.
SL_ALREADYLOCKED	0X0B	11	The UMC object is already locked.
SL_COMMERR	0X0C	12	Transmission/Communication error.
SL_NOTIMPL	0X10	16	Returned if a not implemented method is invoked.
SL_CHANGEPSWDISABLE	0X19	25	The user cannot change the password.
SL_USERUNKNOWN	0X20	32	The user is not present in the system.
SL_USERNEVEREXPIRE	0X21	33	The user never expires.
SL_TICKETEXPIRED	0X22	34	The authentication ticket is expired.
SL_USER_EXPIRED	0x27	39	The user is expired.
SL_PSWMINLEN_ERR	0x120	288	The account policy related to the minimal password length has been violated.
SL_PSW_CHANGE_FAIL	0X154	340	Password change failure.
SL_INVALID_NONCE	0x166	358	Login failed: invalid token. This event may occur if you try to access the login page directly from the URL or if you leave the login page open.
SL_WEAK_AUTH	0x167	359	Login failed: access not allowed using weak authentication method.

CRUD Operation Errors

Name	Hexadecimal Value	Decimal Value	Description
SL_ALREADYEXIST	0x0D	13	The UMC object already exists.
SL_LOCK_NEEDED	0x23	35	A lock is needed to complete the operation.
SL_NOT_LOCKED	0x24	36	The UMC object is not locked so you cannot unlock it.
SL_OBJVERMISMATCH	0X31	49	A UMC object has been simultaneously modified by two Web UI instances and an object version mismatch has been detected.
SL_INVALID_OPERATION	0x103	259	The operation cannot be performed on the selected object.
SL_OBJ_DOES_NOT_EXIST	0x111	273	The UMC object does not exist or has not yet been saved into the UMC database.
SL_OBJECT_LOCKED_IN_DATABASE	0X153	339	The UMC object is already locked.
SL_FAIL_NOTAMASTER	0x160	352	An attempt has been made to modify the UMC database on a machine that is not a master.
SL_FAIL_BINDING_ADMIN_ROLE	0x161	353	An attempt has been made to assign the Administrator role to a group or the user who performed the association, either a UMX user or a Web UI user, does not have the Administrator role.
SL_OBJ_OFFLINE	0x0F	15	The user/group for which you want to perform an operation is offline and the operation is not allowed for offline objects.
SL_INVALID_NAME_FOR_OFFLINE_OBJ	0x165	357	The offline user/group that you are creating does not follow the pattern *<domainName>\<objName>*.

Name	Hexadecimal Value	Decimal Value	Description
SL_INVALID_SID	0x5C	92	Invalid User Security Identifier (SID). See Microsoft Documentation on Security Identifiers for more details.

Provider Operation Errors

Name	Hexadecimal Value	Decimal Value	Description
SL_INVALID_PROVIDER	0x100	256	Operation not provided by this provider.
SL_INVALID_HANDLE	0x101	257	An invalid handle was passed as parameter.
SL_ERROR_LOADING_PROVIDER	0x102	258	An error occurred when loading the provider.

Internal or Parameter Errors

Name	Hexadecimal Value	Decimal Value	Description
SL_INVALID_PARAMETERS	0x104	261	The method has an incorrect parameter.
SL_MEMORY_ERROR	0x105	262	Memory allocation error.
SL_INITIALIZATION_ERROR	0x106	263	Initialization error.
SL_INVALID_LOCK_OPTION	0x108	264	The lock option has not been defined.
SL_INVALID_PROPERTY	0x109	265	The property has not been defined for the object.
SL_INVALID_CULTURE	0x17B	379	Invalid language

File Errors

Name	Hexadecimal Value	Decimal Value	Description
SL_ACCESS_FILE_ERROR	0x112	274	Access file error.
SL_UNKNOWN_FILE_FORMAT	0x113	275	Unknown file format.
SL_FILE_NOT_FOUND	0x50	80	File not found.
SL_PATH_NOT_FOUND	0x51	81	Path not found.

Name	Hexadecimal Value	Decimal Value	Description
SL_FILE_CREATION_FAIL	0x52	82	Error during file creation.
SL_PATH_CREATION_FAIL	0x53	83	Error during path creation.
SL_INVALID_PATH	0x54	84	Invalid path.

Function Rights Errors

Name	Hexadecimal Value	Decimal Value	Description
SL_RESOURCE_NOT_FOUND	0x150	336	The user does not have the correct function right to perform the requested operation. This error has the same meaning as the SL_MISSING_FUNCTION_RIGHT error.
SL_INVALID_RESOURCE	0x151	337	The function right does not exist.
SL_MISSING_FUNCTION_RIGHT	0x152	338	The user does not have the correct function right to perform the requested operation. This error has the same meaning as the SL_RESOURCE_NOT_FOUND error.

Service Layer Errors

Name	Hexadecimal Value	Decimal Value	Description
SL_CLAIM_EXPIRED	0X155	341	The claim is expired.
SL_CLAIM_INVALID	0X156	342	The claim is invalid.
SL_JSON_ERROR	0X157	343	The .json file is not well formed.
SL_MKTKT_FAILURE	0X158	344	The "make ticket" operation failed.
SL_ABORTED	0x159	345	Operation aborted.

Package Errors

Name	Hexadecimal Value	Decimal Value	Description
SL_PACKAGE_CREATION_FAIL	0x55	85	Package creation failed.

Name	Hexadecimal Value	Decimal Value	Description
SL_PACKAGE_COMPRESSION_FAIL	0x56	86	Package compression failed.
SL_PACKAGE_UNCOMPRESSION_FAIL	0x57	87	Package decompression failed.
SL_PACKAGE_ENCRYPTION_FAIL	0x58	88	Package encryption failed.
SL_PACKAGE_DECRYPTION_FAIL	0x59	89	Package decryption failed.
SL_PACKAGE_RESTORE_FAIL	0x5A	90	Package restore failed.
SL_PACKAGE_WRONG_PASSWORD	0x5B	91	Wrong password for the package.

Database Errors

Name	Hexadecimal Value	Decimal Value	Description
SL_DBFILE_ACCESS_DENIED	0X32	50	The user cannot access a UMC database file.
SL_DBFILE_ERROR	0X33	51	Generic UMC database file error.
SL_DBFILE_OUT_OF_SPACE	0X34	52	A UMC database file is full.
SL_TOO_MANY_GROUPS	0X36	102	Too many groups assigned to a user.
SL_TOO_MANY_ROLES	0X37	103	Too many roles assigned to a user or group.
SL_TOO_MANY_USERS	0X38	104	Too many users assigned to a group.
SL_ROLEIDS_OUT_OF_SPACE	0X35	53	No more role IDs are available in the role database file. A purge of the roles is needed.

User Alias Errors

Name	Hexadecimal Value	Decimal Value	Description
SL_INVALID_USER_ALIAS	0x5E	94	Invalid user alias name.
SL_USER_ALIAS_ALREADY_EXIST	0x5F	95	User alias already exists.
SL_BAD_PKI_FILTER_NAME	0x115	277	Invalid filter name or filter name not present when authmode = SL_PKI_FILTER_MASK.

Secure Application Data Support (SADS) Errors

Name	Hexadecimal Value	Decimal Value	Description
SL_INVALID_DOMAIN_NAME	0x60	96	Invalid domain name.
SL_NOT_CURRENT_DOMAIN	0x61	97	Input domain name is not the current domain.
SL_INVALID_KEY	0x70	112	Invalid key.
SL_KEY_GENERATION_FAIL	0x71	113	Error during key generation.
SL_KEY_ENCRYPTION_FAIL	0x72	114	Error during key encryption.
SL_KEY_DECRYPTION_FAIL	0x73	115	Error during key decryption.
SL_KEY_NOT_FOUND	0x74	116	Key not found.
SL_KEY_ENCRYPTION_NOT_ENABLED	0x75	117	Application key protection (global policies) not enabled.
SL_MAX_NUM_KEY	0x76	118	The maximum number of allowed keys has been reached.
SL_KEY_DECRYPTION_NO_ID_FOUND	0x77	119	No SUID of the identity has been found in EAK array.
SL_SADS_VERSION_ERROR	0x78	120	Wrong SADS version.
SL_WRONG_IDENTITY	0x79	121	Ticket authentication error while decrypting a key.
SL_EAK_BAD_FORMAT	0x80	128	Bad format of the encryption application object.
SL_SUBJECT_NOT_ENABLED	0x81	129	Encryption not enabled for the specified subject.
SL_SUBJECT_KEY_OBSOLETE	0x82	130	The decryption has been executed using an obsolete key.

12 Field Sizes

The following table lists the sizes for the main UMC database fields.

API Property Name	API Object	Web UI Display Name	UMX Parameter	Size in Chars
SL_USER_NAME	SLOBJ_USER	User Name	*name*	100
SL_USER_PASSWORD	SLOBJ_USER	Password	*password*	120
SL_USER_FULLNAME	SLOBJ_USER	Full Name	*fullName*	250
SL_GROUP_NAME	SLOBJ_GROUP	Group Name	*name*	100
SL_GROUP_DESCRIPTION	SLOBJ_GROUP	Description	*description*	260
SL_ROLE_NAME	SLOBJ_ROLE	Role Name	*name*	255
SL_ROLE_DESCRIPTION	SLOBJ_ROLE	Description	*description*	40
SL_ATTRIBUTE_NAME	SLOBJ_ATTRIBUTE	Attribute Name	*attribute name*	80