SIEMENS

User Management Component 2.7

UMCONF User Manual

05/2019
A5E47537974-AA

Contents

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 http://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 http://www.siemens.com/industrialsecurity.

Siemens AG
Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E47537974-AA
20190531_40676

Contents

1 UMCONF Overview

The **umconf** utility can be used to perform the basic configuration of the User Management Component (UMC). basic configuration steps can be performed using the guided interactive mode (recommended) or by using a range of switches and parameters. Additionally, depending on the options selected (switches) and the related parameters, the utility allows you to execute various configuration commands. Note that the execution of the **umconf** utility with no switches is identical to the execution of the utility in interactive mode (**umconf -i**).

This utility, which is distributed with UMC, is installed in the subdirectory \BIN (for example C:\Program Files\Siemens\UserManagement\BIN) and must be executed from a command prompt within this directory or in the C:\Program Files\Siemens\UserManagement\WOW\BIN folder. The execution of **umconf** is allowed by a Windows user with Administrative rights (elevated user if User Account Control (UAC) is enabled) or any users belonging to the um_config group.

CAUTION:

- The **umconf** utility must be used with care. Incorrect usage can cause system unavailability.
- Stop all of the applications that use UMC before launching umconf and making changes to the machine configuration.

UMC Basic Configuration

The basic configuration consists of:

- Creating the User Manager Domain;
- Creating the User Manager user with administrator role;
- Specifying the Windows user that is associated with the User Manager core service; this user must be either in the UM Service Accounts group or have Administrative rights.
- the Windows user with Active Directory access rights that is associated with the provisioning service - mandatory if you need Active Directory Provisioning. This option is not enabled if you create a Standalone Domain.

After the first installation it is necessary to perform the configuration steps above to run UMC on a machine that, once configured, will be promoted to UM ring server.

Important:

We strongly suggest using the command **umconf -i** to perform all the configuration steps.

Configuration Options

The following options are supported:

- fresh configuration: it is the first time that you are configuring UMC;
- overwrite an existing configuration: you have already configured UMC and you want to modify the configuration;

- upgrade an existing configuration from a previous version: you have already configured UMC, you have installed a newer version of UMC and you have to upgrade the configuration.

The different options are offered when running umconf interactively.

2 Concepts You Need to Know About

The following concepts are the basics you need to know before you start configuring UMC:

- User Manager Domain
- User Manager User
- Built-in User Roles
- Claim Key
- User Manager Function Rights

2.1 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.

UMC Computer Roles

In a typical UMC scenario there are three computer roles:

- **UM ring server**: the owner of the UM configuration, which is responsible for managing the domain, and provides full implementation of authentication and user management features. The *priority* ring server is the one which is configured first, running the **umconf** utility. If more than one ring server is available, if you unjoin the priority ring server, the system dynamically elects a new priority ring server.
- **UM server**: provides full implementation of authentication features, the UM server is in *degraded mode* if it is not connected to any UM ring server.
- **UM agent**: works as a client of the UM server/UM ring server to which it is attached, which can be used to run an application developed using the UMC API. See the *User Management Component API SDK Developer Manual* for more details. In order to import Windows Local Users, see **Importing a Windows Local User on an Agent** in the *UMC Installation Manual*.

Important:

Engineering operations are not allowed on the UM Agent except for encryption enablement.

CAUTION:

If you want to manage Active Directory users, the UM ring server and the UM server machines have to be joined to the AD Windows domain.

2.2 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

2.3 Built-in User Roles

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.

2.4 Claim Key

A claim is a statement that one subject, such as a person or organization, makes about itself or another subject. The subject making the claim or claims is the provider. We use this mechanism to provide web authentication. When the user authenticates himself against the identity provider, it receives a claim. This claim is signed using the private claim key. Once a relying party needs to verify the claim, it uses the corresponding public claim key (previously installed on the relying party). It is up to the relying party how this public claim key is installed.

2.5 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.*
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.

Name	Description
UM_REGCLIENT	The user can register UMC station clients.

3 Commands for Listing a Summary of UMCONF Commands

The following command can be used to display a summary of UMCONF commands:

- Help

3.1 Help

This command displays a brief summary of the different commands with their parameters and switches.

Syntax

```
umconf -h
```

4 Commands for Creating UM Entities

The following commands can be used to create UMC entities:

- Create Domain
- Create UM Administrator User
- Create Claim Key

4.1 Create Domain

This command creates a UM Domain named as the input parameter if no domain exists. If a domain has already been defined, use the -f switch to overwrite the existing domain. If you are working with a distributed scenario with an active firewall, the inbound and outbound connections through the 4002 port must be allowed. The command creates also the private claim key, which is necessary for correct system functioning.

CAUTION:

Overwriting an existing domain can cause possible data loss.

Syntax

```
umconf -c -d name [-f]
```

Parameters

- *name* is the string representing the UM Domain name, only alphanumeric characters are allowed.

Switches

Switch	Description
-f	Forces the creation of a new UM Domain. If a domain with the same name is present it is overwritten.

Example #1

umconf -c -d mydomain

4.2 Create UM Administrator User

This command creates the UM Administrator user. This user can be created only once.

CAUTION:

Using umconf you can create only one UM user with Administrator role and neither the user nor the password can be changed. The password can be changed via **umx** command or via Web UI.

General Recommendations

It is strongly recommend that you comply with the password policies of your organization in order to grant password strength for the UM Administrator user. For example, a password policy may impose that your password meets the following requirements:

- be at least 8 characters long;
- contain characters from three of the following four categories:
  – uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);
  – lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters);
  – base 10 digits (0 through 9);
  – nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

When creating the UM Administrator User, if you are using the command via script, add a warning that suggests to insert a password that complies with the password policies of your organization.

Syntax

```
umconf -c -u name -p password
```

Parameters

- *name* is the string representing the user name, only alphanumeric characters are allowed.
- *password* is the password associated to the user. An empty password is not accepted.

Example #1

umconf -c –u administrator -p 123

4.3 Create Claim Key

This command creates a new private claim key and generates the corresponding public key. The new private claim key becomes the current one used by the Identity Provider to sign the claims provided to the relying parties.It can be run only on a ring server that is master. This command cannot be run on a master ring server machine that is running in safe mode (writing is not enabled).

The public key of the claim can be found in %programdata%\Siemens\UserManagement\CERT\CLAIM and the filename is **key.pub**. The key can be exported. During the create domain operation a claim key is created, this new claim key overwrites the existing one. If needed the relying party applications should be updated with the new claim key.

CAUTION:

In case of a distributed scenario, once you have created a new claim key on a UM master ring server/UM server, to align the keys, the **UMCService** of the other UM ring server/UM server machine has to be manually restarted.

Syntax

```
umconf -c -k
```

5 Commands for the Management of UM Services

The following commands can be used to associate users to UM Services:

- Associate Active Directory Windows User with Provisioning Service
- Associate User with UM Service

5.1 Associate Active Directory Windows User with Provisioning Service

This command associates the Windows user identified by the parameter *name* with the UM service **UPService.exe**. In order to associate the Windows user with the service, the password must be inserted as input parameter.

This Windows user must have the following rights:

- Active Directory access rights;
- write access on the UMC folder C:\ProgramData\Siemens\UserManagement\CONF or alternatively he must belong to the Windows group **UM Service Accounts**.

This command also creates the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\User Management\WebUI\Settings\domains_support and sets it to "yes", which enables the Web UI import user and group functionalities.

Important:

In order to disable the Active Directory provisioning, you have to set to "no" the value of the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\User Management\WebUI\Settings\domains_support and stop the UM service **UPService.exe**.

Syntax

```
umconf -P -u name -p password [-f]
```

Parameters

- *name* is the string representing the user name preceded by the domain.
- *password* is the password associated with the user.

Switches

Switch	Description

-f	If the Provisioning Service is running and has been already configured, this switch allows you to overwrite the existing configuration.

5.2 Associate User with UM Service

This command associates the Windows user identified by the parameter *name* with the UM service **UMCService.exe**. In order to associate the Windows user with the service, the password must be given as input parameter. This user must be either in the UM Service Accounts group or have Administrative rights. In case you want to associate a built-in Windows local user, you have to use the Windows Services configuration tool.

CAUTION:

The user associated to UM service must only be changed via UMConf.

Syntax

```
umconf -s -u name -p password [-f]
```

Parameters

- *name* is the string representing the user name preceded by the domain. If the user is local, the name must be preceded by the string ".\" or *machinename*\. For Example: .\administrator, mydomain\myuser.
- *password* is the password associated with the user. If the virtual account NT SERVICE\UMC Service has been specified, the password will not be prompted.

Switches

Switch	Description
-f	If the services are running and have been already configured, this switch allows you to overwrite the existing configuration.

6 Commands for Binding/Unbinding

The following commands can be used to perform binding or unbinding actions:

- Attach Agent
- Join Server
- Unjoin Server
- Retrieve Fingerprint

6.1 Attach Agent

This command attaches a machine to a UM domain and promotes it to the UM agent role. All the parameters of the command are optional. If a parameter is not inserted when launching the command, you will be prompted to insert it. The *serviceUserName* and *servicePassword* parameters are an exception to this behavior: if not inserted the default is the built-in Windows user *Local System*.

The command installs the network and machine certificates on your machine. In presence of an active firewall, the inbound and outbound connections through the 4002 port must be allowed. In an agent machine you can run an application developed using the UMC API, see the *User Management Component API SDK Developer Manual* for more details.

Syntax

```
umconf -a [-f] [-c computerName] [-u userName] [-p password] [-s
serviceUserName servicePassword] [-v] [-fp fingerprint]
```

Parameters

- *computerName* is the name of one of the UM ring servers or UM servers of the domain you want to be attached to.
- *userName* is the name of a UM user having the **UM_ATTACH** function right or the **Administrator** role.
- *password* is the password of the UM user associated with the parameter *userName*.
- *serviceUserName* is the name of a Windows Local/domain user (who is either a member of the UM Service Accounts group or has Administrative rights) that you want to associate with the User Manager services.
- *servicePassword* is the password of the Windows user associated with the parameter *serviceUserName*.
- *fingerprint* is the fingerprint of the UMC domain.

Switches

Switch	Description
-f	If the machine has already been configured, the existing configuration is overwritten.
-v	If this switch is present, the installation of the certificates is not interactive. The -v switch is mandatory if the fingerprint is specified.

6.2 Join Server

This command promotes the machine to a UM server or UM ring server machine. If the machine is not yet attached to the UM domain, the command attaches it. All the parameters of the command are optional. If a parameter is not inserted when launching the command, you will be prompted to insert it. The *serviceUserName* and *servicePassword* parameters are an exception to this behavior: if not inserted the default is the built-in Windows user *Local System*.

The command installs:

- the network and machine certificates on your machine;
- the ticket and claim keys.

In presence of an active firewall, the inbound and outbound connections through the 4002 port must be allowed.

CAUTION:

Consider that if you have configured the AD provisioning on the priority ring server you must configure it also in the machine you are joining. See the -b switch below to exclude the AD provisioning configuration. If you want to use this command via script, the use of -b is mandatory and to configure the provisioning you have to use the umconf command to associate the Active Directory Windows user with the Provisioning Service.

Syntax

```
umconf -j [-f] [-m serverType] [-c computerName] [-u userName] [-p password]
[-s serviceUserName servicePassword] [-v][-b] [-fp fingerprint]
```

Parameters

- *serverType* determines the type of the server that will be joined to the ring:
  - 0 the machine will be a UM server, in this case the provisioning is not configured;
  - 1 the machine will be a UM ring server.
- *computerName* is the name of one of the UM ring servers of the domain you want to be joined to.

- *userName* is the name of a UM user having the **UM_RINGMNG** function right (to create a UM ring server) or **UM_JOIN** function right (to create a UM server) or having the **Administrator** role. For more details see User Manager Function Rights.
- *password* is the password of the UM user associated with the parameter *userName*.
- *serviceUserName* is the name of a Windows Local/domain user (who is either a member of the UM Service Accounts group or has Administrative rights) that you want to associate with the User Manager services.
- *servicePassword* is the password of the Windows user associated with the parameter *serviceUserName*.
- *fingerprint* is the fingerprint of the UMC domain.

Switches

Switch	Description
-f	Forces the services stop.
-m	This switch determines the type of server that will be joined to the ring: • 0 the machine will be a UM server; • 1 the machine will be a UM ring server.
-v	If this switch is present, the installation of the certificates is not interactive. The -v switch is mandatory if the fingerprint is specified.
-fp	If the switch -v and -fp are present the fingerprint specified is used for validation.
-b	The Active Directory provisioning configuration is not performed. This switch is relevant only for UM ring server configuration. In case of UM server the provisioning is never configured.

6.3 Unjoin Server

This command downgrades a machine having the UM ring server/UM server role to a UM agent role. The parameters *userName* and *password* of the command are optional. If the parameter is not inserted when launching the command, you will be prompted to insert it, whereas, if you do not insert the parameter *computerName,* by default the command is executed for the machine on which you are launching it. If you unjoin a priority ring server, the system dynamically elects a new priority ring server.

In presence of an active firewall, the inbound and outbound connections through the 4002 port must be allowed.

CAUTION:

If you perform the unjoin remotely (parameter *computerName* is present) of a machine that is disconnected from the network and the unjoined machine returns connected after a while, you have to delete the UMC configuration before joining it again.

Syntax

```
umconf -u [-u userName] [-p password] [-c computerName] [-f]
```

Parameters

- *userName* is the name of a UM user having the **UM_RESETJOIN** function right or having the **Administrator** role.
- *password* is the password of the UM user associated with the parameter *userName*.
- *computerName* is the name of the machine having the UM ring server/UM server role that you are unjoining. This parameter must be used only if the UMC services of the machine you are running the command cannot communicate with the UMC services of the machine you are unjoining. This happens for instance when the unjoining machine is no more available.

Switches

Switch	Description
-f	Forces the services stop.

6.4 Retrieve Fingerprint

This command retrieves the fingerprint (net id) of the UMC domain from the specified computer. To obtain the fingerprint from a configured machine for a machine which has not been configured, the [-c computerName] parameter can be used. If you do not specify the computer name, the fingerprint is retrieved locally.

Syntax

```
umconf -fingerprint [-c computerName]
```

Parameters

- *computerName* is the name of the machine from which you want to obtain the fingerprint.

7 Commands for Centralized Configuration Management

The following commands can be used to manage the UMC centralized configuration:

- Get Default Centralized Configuration
- Set Centralized Configuration
- Get Centralized Configuration

Set Initial central configuration

To set a centralized configuration you must:

1. Execute get default configuration.
2. Modify the file .json file as required for your centralized configuration, see the *User Manager Installation Manual*.
3. Set the centralized configuration.

Update Central Configuration

To update the current centralized configuration you must:

1. Execute get configuration in order to retrieve the current version of centralized configuration.
2. Modify the current configuration as required, see the *User Manager Installation Manual*.
3. Set the centralized configuration.

For information on the contents of the default, central and local configuration files see the Identity provider configuration section in the *User Manager Installation Manual.*

7.1 Get Default Centralized Configuration

This command retrieves the default configuration .json file. The file can be used as a template from which you can copy the keys for the values to set in the local or central configuration.

Syntax

```
umconf -getdefaultconfig -file fullpath
```

Parameters

- *fullpath* the path and the name of file in which the default configuration is to be saved.

7.2 Set Centralized Configuration

This command sets the file specified as the centralized configuration. The configuration file has a specific version, which is incremented every time a set operation is performed, you must perform a get before setting a configuration, in order to retrieve the latest version.

Syntax

```
umconf -setconfig -u username -p password -file fullpath [-label labelName]
```

Parameters

- *userName* is the name of a UM user who has the **UM_ADMIN** function right or the **Administrator** role.
- *password* is the password of the UM user associated with the parameter *userName*.
- *fullpath* is the complete path of the .json file which contains the UMC configuration that is to be set.
- *labelName* is the name that identifies the configuration.

Switch	Description
-label	(for future use only) Optional, allows you to specify a label in order to identify each specific configuration.

7.3 Get Centralized Configuration

This command retrieves the centralized configuration file which is currently set and saves it to the file and location specified.

Syntax

```
umconf -getconfig -file fullpath [-label labelName]
```

Parameters

- *full_path* the full path of the file which is to be retrieved.
- *labelName* is the name that identifies the configuration.

Switch	Description
-label	(for future use only) Optional, allows you to specify a label in order to identify each specific configuration.

8 Commands for Upgrading Entities

The following command can be used to upgrade a UM domain:

- Upgrade Domain

8.1 Upgrade Domain

This command upgrades an existing UM Domain. It can be used after installing UMC on a machine where a previous version was installed and configured.

CAUTION:

We strongly suggest to use the command **umconf -i** to perform all the upgrade steps that include this domain upgrade operation.

Syntax

```
umconf -U [-f]
```

Switches

Switch	Description
-f	Forces the services stop.

9 Commands for Deleting a UM Configuration

The following commands can be used to delete a UM configuration:

- Delete Configuration

9.1 Delete Configuration

This command deletes UMC configuration, restoring the system as if it was just installed. The command has to be run after the UMC services has been stopped or using the -f switch to stop them automatically. After executing the command, it is necessary to perform the **Recycle** of the following application pools in **IIS Manager**:

- Web UI pool (**umc_pool**, for configuration via script);
- Identity Provider pool (**SimaticLogonPool**, for configuration via script).

In case you want to remove a UM ring server/UM server from the UMC system you have also to perform the unjoin operation of the machine *before* executing this command.

CAUTION:

Performing the restart of a UMC service and/or the **Recycle** of the application pool can cause service interruption.

Syntax

```
umconf -D [-f]
```

Switches

Switch	Description
-f	Forces the UMC services to stop before deleting all data.

10 Commands for Importing Packages

The following commands can be used to import a UM package:

- Import Package - UMC Partially Configured

10.1 Import Package - UMC Partially Configured

This command imports a UMC configuration via an input UMC package on a machine where the UMC domain has been already created. To run this command the **only configuration step** that you must have performed on the system is the domain creation. If UMC is configured, to import a package you must use the corresponding umx command. For more details see the *UMX User Manual*.

UMC package is a UMC proprietary format, zipped and encrypted. If not inserted, you will be prompted to insert a password for the decryption that has to be the same as the one used in the export package umx command. For more details see the *UMX User Manual*.

The effects of this operation are:

- the creation of the UMC user with administrator role;
- the import of all the users, groups and roles that are part of the package.

For more information on the import/export/update package usage see the *Standalone Engineering Station Scenario* in the *User Management Component Installation Manual*.

Syntax

```
umconf -I [-f] -F file -p password
```

Parameters

- *file* is the path and name of the file to be imported, for instance C:\temp\myPackage;
- *password* is the archive password.

Switches

Switch	Description
-f	Forces the services to stop.

11 Commands for the Management of Whitelist Entries

The following commands can be used to manage Whitelist Entries:

- Create Whitelist Entry
- List Whitelist Entries
- Remove Whitelist Entry

11.1 Create Whitelist Entry

This command adds a host to the Identity Provider whitelist. Whitelisting allows you to maintain a list of hosts that are granted some privileges. If present in the list:

- the host can call the IdP (service validation);
- the host can create an iFrame embedding the IdP (iFrame validation).

If the host is not present in the list, the call is rejected. In case of service validation, we log a warning message on UMC event log and, if enabled, we log also a message on the Identity Provider log file.

After executing the command, for each machine where the Identity Provider is installed, it is necessary:

- to restart the **UMCService**;
- to perform the **Recycle** of the application pool of the Identity Provider (**SimaticLogonPool**, for configuration via script) in **IIS Manager**.

CAUTION:

Performing the restart of a UMC service and/or the **Recycle** of the application pool can cause service interruption.

Syntax

```
umconf -c -w -d name
```

Parameters

- *name* is the string that represents the host according to URL standard format, and must specify the exact path of the relying party. It can be:
  - localhost;
  - machine name (e.g. myMachine);
  - internet domain name (e.g. www.myDomain.net);
  - IP address (e.g. 172.23.1.48).

– or to whitelist the service layer:
- computername/UMC/slwapi/service
- computername/UMC/slwapi/service and computername.userdnsdomain/UMC/slwapi/service.

Remember to recycle the application pool of the Identity Provider to apply all pending modifications.

11.2 List Whitelist Entries

This command lists the hosts of the Identity Provider whitelist. The only default value present in the whitelist is the hostname of the machine; this value is added to the whitelist when the UMC domain is created.

Syntax

```
umconf -l -w
```

Example

```
umconf -l -w
```

Example output:

whitelist contains the following domains:

localhost

myMachine

170.23.1.48

11.3 Remove Whitelist Entry

This command removes a host from the Identity Provider whitelist.

After executing the command, for each machine where the Identity Provider is installed, it is necessary:

- to restart the **UMCService**;
- to perform the **Recycle** of the application pool of the Identity Provider (**SimaticLogonPool**, for configuration via script) in **IIS Manager**.

CAUTION:

Performing the restart of a UMC service and/or the **Recycle** of the application pool can cause service interruption.

Syntax

```
umconf -d -w -d name
```

Parameters

- *name* is the string representing the host according to URL standard format. It can be:
  – localhost;
  – machine name (e.g. myMachine);
  – domain name (e.g. www.myDomain.net);
  – IP address (e.g. 172.23.1.48).

Example

```
umconf -d -w -d 175.22.3.55
```

Output:

domain 175.22.3.55 successfully removed from whitelist.

Remember to restart UMC service to apply all pending modifications.

12 Commands for the Management of Plugins

The following commands can be used to manage UM plugins:

- Register Plugin
- Register Cookie Adapter
- List Registered Plugins
- Deregister Plugin

12.1 Register Custom Plugin

This command registers a custom plugin. It can only be executed on a master ring server.

After executing the command, for each machine where the Identity Provider is installed, it is necessary to perform the **Recycle** of the application pool of the Identity Provider (**SimaticLogonPool**, for configuration via script) in **IIS Manager**.

CAUTION:

Performing the **Recycle** of the application pool can cause service interruption.

Syntax

```
umconf -r -u username -p password -P plugin_path -d plugin_description -name
pluginname [-w web_plugin|-w2 hybrid_plugin [-cors response format]]
[-usealias][-pk public key file] [-sl security level] [-l language file]
```

Parameters

- *userName* is the name of a UM user who has the **UM_ADMIN** function right or the **Administrator** role.
- *password* is the password of the UM user associated with the parameter *userName*.
- *plugin_path* is the path and name of the dll plugin to be registered, for instance C:\temp\myPlugin.dll;
- *plugin_description* is the string that will appear in the drop-down menu on the right of the Idp login page on the client machine;
- *plugin_name* specifies the unique name of the plugin. Note that the following names are reserved: iwa, pki, desktop, web, web_cors, hybrid, hybrid_cors and ":".
- *response format* for future use.
- *securitylevel* defines the type of authentication. This information is passed in the IdP claim so that the third party application can determine the authentication security level; in UMC Web UI

can only be used if the authentication is **standard** or **strong**.The security level can only be specified for web and hybrid plugins. The possible values are:
  – **weak**
  – **standard**
  – **strong**

- *languagefile* not used.

Switch	Description
-w	For future use. Specifies that the plug in is a web plugin, if this switch is used you must use -pk, see below.
-pk	For future use. Specifies a public key associated to the plugin.
-w2	For future use.Specifies that the plug in is a hybrid plugin.
-usealias	Specifies that the alias of the user is to be used instead of the username.

12.2 Register Cookie Adapter

This command registers a cookie adapter. It can be executed only on a master ring server.

After executing the command, for each machine where the Identity Provider is installed, it is necessary to perform the **Recycle** of the application pool of the Identity Provider (**SimaticLogonPool**, for configuration via script) in **IIS Manager**.

CAUTION:

Performing the **Recycle** of the application pool can cause service interruption.

Syntax

```
umconf -r -u userName -p password -P url -d plugin_description -w -pk
public_key_path -sl securityLevel [-l languagefile]
```

Parameters

- *userName* is the name of a UM user having the **UM_ADMIN** function right or having the **Administrator** role.
- *password* is the password of the UM user associated with the parameter *userName*.
- *url* is the url of the cookie adapter to be registered;
- *plugin_description* is the string that will appear in the drop-down menu on the right of the Idp login page on the client machine;

- *public_key_path* is the public key generated at the setup of cookie-adapter
- *securityLevel* defines the type of authentication. This information is passed in the IdP claim so that the third party application can determine the authentication security level; in UMC Web UI authentication is performed in case of **standard** and **strong**. The possible values are:
  – **weak**
  – **standard**
  – **strong**
- *languagefile - not used*.

Switches

Switch	Description
-w	Specifies that you are registering a cookie adapter.
-pk	Specifies a public key associated to the plugin.

12.3 List Registered Plugins

This command can be be executed on any server and lists the plugins which are registered on the master ring server, along with their:

- **Plugin Uid**: the unique id of the plugin which is necessary to activate plugins on clients.
- **Path:** the path of the plugin.
- **Description:** the description of the plugin.
- **Class**: Specifies the type of plugin: desktop, web or hybrid.
- **Pub keyid:** the public key id.
- **Security Level:** Weak, Standard and Strong, see register custom plugin for more information.
- **Plugin Name:** the unique the name of the plugin, this field is empty in plugins which were created prior to UMC 1.9.1.

Syntax

```
umconf -l -P
```

Example

An example of the command output follows:

#1 Plugin Uid: 889f1341-0260-4f77-81fd-ceadf8f56c4fPath: C:\Users\Administrator\Desktop\Test_plugins\Bin\PluginTAF.dllDescription: Plugin Desktop Stateful Class: desktopPub keyid:Security level: weak Plugin name: my desktop plugin #2 Plugin Uid: 3c179694-e5ed-4225-b064-eb01b981251bPath: C:\Users\Administrator\Desktop\Test_plugins\Bin\PluginTAF2.dllDescription: Plugin Desktop Stateless Class: desktopPub keyid:Security level: weak Plugin name:my plugin

12.4 Deregister Plugin

This command deregisters a plugin on a master ring server.

After executing the command, for each machine where the Identity Provider is installed, it is necessary to perform the **Recycle** of the application pool of the Identity Provider (**SimaticLogonPool**, for configuration via script) in **IIS Manager**.

CAUTION:

Performing the **Recycle** of the application pool can cause service interruption.

Syntax

```
umconf -dP  -u userName -p password -name pluginname [-P pluginId]
```

Parameters

- *userName* is the name of a UM user having the **UM_ADMIN** function right or having the **Administrator** role.
- *password* is the password of the UM user associated with the parameter *userName*.
- *pluginname* is the name of the plugin alternatively you can use *pluginId.*
- *pluginId* is the position of the plugin in the list of registered plugins. See example below.

Example

If the command:

```
umconf -l -P
```

returns:#2 Plugin Uid: 5a25fc03-3bd1-479b-9b02-2dcb9f6f60f3Path: https://mymachine/tcss_webDescription: Teamcenter Web Class: webPub keyid: 88FACEFCD6ED416BC6D516D10E09ABBBDA85FDC6Security level: strongUse alias: enabledPlugin name: Teamcenter Web#3 Plugin Uid: 113dc9ec-ada6-4f61-b938-9bf2a50b1401Path: https://vm-chessa/tcss_hybridDescription: Teamcenter Hybrid Class: hybrid_corsPub keyid: 88FACEFCD6ED416BC6D516D10E09ABBBDA85FDC6Security level: strongUse alias: enabledPlugin name: Teamcenter Hybrid

```
pluginlist contains 2 plugins correctly registered.
```

the command:

```
umconf -dP -u myUser -p 098P@ssword! -name Teamcenter Hybrid
```

deregisters the Windows plugin.

13 Commands for the Management of Logs

The following commands can be used to manage logs:

- Archive logs
- Extract logs

13.1 Archive logs

This command archives the system log folder into a UMC package. UMC package is a UMC proprietary format, zipped and encrypted. The exported package is the input of the extract logs command.

Syntax

```
umconf -log -a -f file [-p password]
```

Parameters

- *file* is the path and name of the package file, for instance C:\temp\myLogs;
- *password* is the package password. If not provided, the user will be prompted to insert the password.

13.2 Extract logs

This command extracts the system logs previously archived into a UMC package. UMC package is a UMC proprietary format, zipped and encrypted. If the password is not inserted when launching the command, you will be prompted to insert it. The input password has to to be the same of the one used in the archive logs command.

Syntax

```
umconf -log -e -f file [-p password]
```

Parameters

- *file* is the path and name of the package file, for instance C:\temp\myLogs;
- *password* is the package password.

14 Commands for Renewing Certificates

The following commands allow to update machine certificates, which are created when a agent is attached or a server is joined. The machine certificate is x.509 certificate which allows SSL communications between UMC machines.

- Renew Certificate

14.1 Renew Certificate

This command updates the expiration date of the machine certificate of a UMC machine, the renewed certificate is valid for 2 years.

CAUTION:

When performing this operation from a machine which is not ring server, if the operation fails the machine will be detached and must be re-attached in order to attempt the operation again.

Syntax

```
 -rc [-f(orce)] [-c computername] [-u username] [-p password] [-v] [-fp
fingerprint]
```

Parameters

- *computerName* is the name of one of the UM server on which the certificate is located.
- *userName* is the name of a UM user who has the UM_ATTACH function right or the **Administrator** role. For more details see User Manager Function Rights.
- *password* is the password of the UM user associated with the parameter *userName*.
- *fingerprint* is the fingerprint of the UMC domain.

Switches

Switch	Description
-f	Forces the UMC services to stop before renewing the certificate.

-v	If this switch is present, the installation of the certificates is not interactive. The -v switch is mandatory if the fingerprint is specified.

15 Commands for Launching UMConf in Interactive Mode

The following command can be used to execute the umconf utility in interactive mode:

- Launch Interactive Mode

15.1 Launch Interactive Mode

This command executes the **umconf** utility in interactive mode. The following configuration steps are performed launching the interactive mode:

- the User Manager Domain;
- the User Manager user with administrator role, the password for this user should be at least 8 characters long and contain characters from three of the following four categories:
  - uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);
  - lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters);
  - base 10 digits (0 through 9);
  - nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/
- the Windows user that is associated with the **UMCService.exe** service; if the virtual account NT SERVICE\UMC Service has been specified, the password will not be prompted.
- the Windows user that is associated with the **UPService.exe** service - mandatory only if you need to import Active Directory users via the **umx** tool or via the Web UI;
- the private claim key.

The following options are supported:

- fresh configuration: it is the first time that you are configuring UMC;
- overwrite an existing configuration: you have already configured UMC and you want to modify the configuration;
- upgrade an existing configuration from a previous version: you have already configured UMC, you have installed a newer version of UMC and you have to upgrade the configuration.

Syntax

```
umconf -i
```

Or alternatively:

```
umconf
```

16 Commands for Purging Roles

The following command can be used to purge UM role IDs:

- Purge Role IDs

16.1 Purge Role IDs

This command purges the roles identifiers. Role identifiers are generated incrementally, until the maximum value of 32600 is reached. Once this value is reached it is no longer possible to insert any new role (regardless of the maximum roles number) until you make the purge of the roles previously deleted.

CAUTION:

This command stops the **UMCService** and restarts it after the execution. The stop can cause service interruption.

Syntax

```
umconf -purge -roles
```

17 Commands for Displaying Lists

The following commands can be used to display the list of servers:

- Display Server List

17.1 Display Server List

This command displays the list of the servers with their machine role. The command can be executed only on a server or ring server machine.

Syntax

```
umconf -t
```

Example

```
umconf -t
```

Output

The server list contains:

servername: myname1 ring server
servername: myname2 ring server
servername: myname3 server

18 Commands for dSSO functionality

The following commands can be used to enable or disable dSSO functionality:

- Enable or disable dSSO

18.1 Enable or disable dSSO

This command enables or disables the dSSO functionality.

Syntax

```
umconf -dsso [enable|disable] [-f(orce)]
```

Switches

Switch	Description
-f	Forces the UMC Secure Communication to restart.

Examples

```
umconf -dsso enable
```

Output

dSSO functionality successfully enabled.
UMC Secure Communication Service need to be restarted manually.

```
umconf -dsso disable -f
```

Output

dSSO functionality successfully disabled.
UMC Secure Communication Service has been restarted.

19 Error Codes

Value	Description
0	Success.
1	The user launching the command does not have the proper administrative rights.
10	Initialization error, for instance a registry key is missing.
50	Command syntax error.
100	Command execution error.