SIEMENS

Contents

Main Functionalities	1
What's New	2
Compatibility Issues	3
Functional Limitations	4
Fixed Technical Issues	5
Release Test Tools	6
Appendix	7

User Management Component 2.7

User Management Component Release Notes

07/2019

-

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.

Contents

1 Main Functionalities 4
1.1 UMC 1.1 4
1.2 UMC 1.2 5
1.3 UMC 1.3 7
1.4 UMC 1.4 8
1.5 UMC 1.5 9
1.6 UMC 1.6 10
1.7 UMC 1.7 11
1.8 UMC 1.8 11
1.9 UMC 1.9 12
1.10 UMC 1.9.1 13
1.11 UMC 2.0 14
1.12 UMC 2.1 15
1.13 UMC 2.2 16
1.14 UMC 2.3 16
1.15 UMC 2.4 17
1.16 UMC 2.5 18
1.17 UMC 2.6 18
1.18 UMC 2.7 19

2 What's New 20

3 Compatibility Issues 23

4 Functional Limitations 24
4.1 User Management Component Web UI 26
4.2 Active Directory Provisioning 27

5 Fixed Technical Issues 30

6 Release Test Tools 31

7 Appendix 32
7.1 Health Check Service 32

1 Main Functionalities

The User Management component implements a centralized user management functionality for MOM/ TIA products. UMC provides the following types of authentication:

- authentication against internal or Windows accounts using the Web Single Sign On (WSSO) or integrated in any product;
- smart card authentication;
- custom plugin authentication;
- cookie adapter authentication;
- authentication via an external IAM;
- Teamcenter integration.

Provisioning of users and groups is available in different ways: automatically from text files or Active Directory, using scripts or manually using the UMC Web UI. Based on the authentication provided by UMC any product can implement authorization business logic. Web Single Sign On allows any user to login only once for all the Siemens Web applications integrated with UMC.

For details on the functionalities released in each version of UMC see UMC Functionality Timeline.

1.1 UMC 1.1

The main developments and improvements which were made in this version are listed below:

Machine Roles

The system is able to manage two machine roles out of the three that will be supported:

- UM ring server: is the owner of the UM configuration, that is domain management.
- UM agent: works as a local user manager server in order to perform authentication using the remote UM server or UM ring server.

The UM server machine role is not yet supported and the ring server redundancy (scenario with **up to two** ring server machines and agents) is only supported for testing purposes.

Identity Provider Improvements

- The following features have been implemented:
  – Integrated Windows Authentication on Identity Provider.
  – Authentication with Ticket - New Ticket format.
  – New **join** command for the **umconf** tool to promote a machine to be a UM ring server.

  - Active Directory (AD) provisioning of users and groups: once the users and groups have been imported from AD into the UMC database, they are automatically synchronized. A new service **UMCSyncService** has been added to manage AD provisioning synchronization.
  - Identity Provider: Possibility to disable the cancel button on the login page.

Web UI Improvements

- The following features have been implemented on the Web UI:
  - new **Unlock User** button available on **Users** page;
  - new page for role editing;
  - new column filter;
  - new page for global account policy management;
  - import of users and groups from AD;
- The script **IdP_WebUI_configurator.bat** allows you to configure the UMC Web components to work with the HTTPs protocol.

Installer and Configuration Management Improvements

- The **umconf** command to delete the configuration has been implemented.
- The uninstall procedure has been implemented.
- The upgrade procedure from 1.0 to 1.1 has been implemented.

1.2 UMC 1.2

The main developments and improvements which were made in this version are listed below:

Technological Improvements

The following general features have been implemented:

- New OpenSSL version: v1.0.1p;
- The synchronization service **UMCSyncService** has been removed and its behavior has been incorporated into the **UMCService**.
- UMC is now based on Microsoft Visual Studio 2015.

Redundancy

Ring server redundancy has been enabled, in particular:

- the redundant ring server does not accept modifications if a network failure occurs and the connection with the master ring server is lost (safe mode);
- safe mode can be disabled via umx command;
- the provisioning service is available in a redundant scenario;
- you can perform the unjoin of a machine remotely

Lock on Invalid Credentials

This feature was partially developed in UMC 1.1:

- now it is possible to specify that some users cannot be locked;
- the lock of a user based on the number of wrong passwords inserted has been changed: the counter is local to the specific UM Agent (host or TS Session in case of Terminal Server). No specific implementation is present for Web session scoping.

UMC Event Log

UMC event log has been implemented. UMC event log provides a mechanism to store the history of events that has been raised using the UMC component. Event data will be stored in one or more files. A new server **um.ELGSrv.exe** has been implemented to manage the event log.

In a redundant scenario, log files can potentially be generated from different servers. Mechanisms to manage reconciliation of data produced by different servers has been implemented.

We have developed internal APIs to write UMC events and to search UMC events related to a given date.

A UMC Web UI page (with limited reading capabilities) has been created to display event data and to search them according to an input date. The old value and the new value of UMC data related to the event are displayed.

The log forwarding will allow one to forward the log files to another application (e.g. UAF or SIMATIC IT Production Suite). It is based on an http(s) protocol in order to be platform independent.

In addition a new UMX command to list event log records has been implemented.

Security Improvements

- A specific UMC user can be assigned to the UMC provisioning service to harden the system security to comply with the lowest privileges principle.
- The IdP **service** field has been validated.
- Https is a prerequisite to have all UMC components running properly. This has implied modifications to UMC cookie management and a complete review of UMC installation and configuration documentation.

Machine Role Support

The system is able to manage three machines roles:

- UM ring server: is the owner of the UM configuration, that is domain management;
- UM agent: works as a local user manager server in order to perform authentication using the remote UM server or UM ring server.
- UM server: has been implemented, which offers the following:
  – The umconf command to join a server machine has been modified in order to join a UM ring server or a UM server.
  – Claim signature validation on UM server has been implemented.
  – Event log works also in degraded mode: logs are collected also when the UM server is not connected to the UM ring server and are forwarded when the connection is up again.
  – An agent can be attached both to a UM ring server or to a UM server.

We support the ring server redundancy, that is a scenario with **up to two** ring server machines.

1.3 UMC 1.3

The main developments and improvements which were made in this version are listed below:

General

- UMC Web UI has been modified to adhere to the guidelines common to all SCADA/MES products (fonts, colors, header, etc.).
- Windows 10 OS and Edge browser support has been added.
- The possibility to import via umx the following built-in users: Local System, Network System, Local Service.
- Whitelisting.
- Radius support.

UMC APIs

- Modifications to UMC APIs have been performed in order to support that the database lock is configuration provider based and not process based. Now, if a configuration provider locks the UMC configuration, all the others cannot modify the configuration. Account policy modifications are an exception and maintain the old behavior.
- UMC Service Layer APIs have been released.
- The original UMC APIs work in degraded mode, that is when the UM server is not connected to the UM ring server.
- New SL-API (ISLA/ISLEA) in order to authenticate a user using a WEBSSO Claim.

Security enhancement on Web UI and Identity Provider

Review of cookie usage, random number generation and path management inside the UMC Web UI and Identity Provider. WEB SSO session creation and deletion are logged in the Event Log.

1.4 UMC 1.4

The main developments and improvements which were made in this version are listed below:

User Management Functionalities

- Create offline users and groups via UMX command for engineering purposes.
- Import Active Directory users via UMX command by searching for user name and full name.
- Import Offline Active Directory Windows Users/Groups
- Export UMC configuration data (user, groups/roles) to a package which is compressed and encrypted.
- Import Package. This functionality allow the UMC Administrator to import a package in a target UMC configuration.

Web UI

- Identity Provider Web pages have been updated in order to adhere to new usability standards.
- Multi-Language implementation in the Web UI has been finalized.

Technical Improvements

- OpenSSL version has been updated and recompiled.
- CORS calls which are not in the white list are not executed.

Scenarios

- The standalone engineering station scenario is now completed. The following operations are possible:
  – To export engineering data into an encrypted and zipped package.
  – Data can be imported into a target machine as follows:
    - the target machine is not configured: umconf import package command;
    - the target machine is already configured: umx import package command (the configuration of the engineering station and the target machine are merged);
  – Data can be used to overwrite the ones in the target machine: umx update via package command;
- SL-APIs have been developed to implement the previous operations.
- Migration procedure of distributed scenarios have been tested and documented.

Security

- A mechanism has been implemented to avoid the cross-site request forgery on the login and change password pages.
- Output encoding has been added for ctx parameter returned to relying party.
- iFrame option for IdP has been implemented.
- Service Layer APIs for role management have been implemented.
- Output encoding has been added for ctx parameter returned to relying party (continued from previous sprint).
- Service Layer APIs for group and user management have been implemented.
- Service Layer APIs for managing assignment of role to users/groups.
- Disclaimer on session closure has been added to the Identity Provider.
- A "logout" page has been implemented: when a user logs out from Web UI is redirected to the logout page instead of generating a new login request
- Additional security disclaimers have been added to the IdP and to the pdf documents. Disclaimers have been localized.
  - The display of the security disclaimer can be disabled modifying the value to **false** in the key <add key="UseDisclaimerMessage" value="true" /> in the Identity Provider **web.config** file (e.g. C:\Program Files\Siemens\UserManagement\WEB\IPSimatic-Logon\Web.config).
- Disable deletion for users imported via groups have been implemented.
- "Logout" page has been removed.

1.5 UMC 1.5

The main developments and improvements which were made in this version are listed below:

General Improvements

- Error format of CORS requests is correctly managed.
- Role identifier mechanism has been completely revised.
- iSSO Service has been implemented.
- Integration of the logon station information in the IdP claim.
- IdP health state information has been improved and NLB has been integrated with health state service.
- Reset password API has been developed.
- Local Identity Service functionalities are available in https.
- Local Identity Service functionalities are available (in http) on UMC machines (ring servers, servers and agents) and can be configured on client machines after a UMC basic setup installation.
- New command in Local Identity Service in order to retrieve PC identity name.

Scenario Support and Machine Roles

- Change password can be performed on a UM server in degraded mode.
- UMC station client (previously mentioned as UMC basic setup) has been released and registration procedure has been finalized.

SWAC Component Improvements

- IdP SWAC component provides the following functionalities:
  – Change password
  – Integrated Windows Authentication
- Cancel button in SWAC login component can be configured (visible/not visible). The login protocol regulates the visibility of the Cancel button. See the SPH UMC Specification for more details.

Security Improvements

A Disclaimer on UMC administration password has been added to the UMC documentation.

1.6 UMC 1.6

The main developments and improvements which were made in this version are listed below:

Technical Updates

- New Open SSL version (1.0.2._).
- Support of IE compatibility view on Login page.
- UMC set up uses the new version (V5) of the SEPA framework.
- Windows Server 2016 is now supported.

User Management Updates

- Users can be identified via custom aliases, the related umx commands have been implemented.
- User names have been extended to 120 chars length.
- Synchronization of AD deletions via UMC provisioning service has been implemented.
- Specific function right to register UMC Station Client has been created.

Security Improvements

- A signed ticket (via IdP certificate) has been implemented for authentication via smart card.
- UMC daily build integrates the new version (V5) of the SEPA framework.
- Authentication using Smart Card via Custom alias has been implemented.

Usability Improvements

- UMC Station Client usability has been improved.
- Smart Card authentication usability has been reviewed.
- Web UI usability has been reviewed for user names long to 120 chars.

Documentation Improvements

A Troubleshooting section has been added to the UMC Installation Manual.

1.7 UMC 1.7

The main developments and improvements which were made in this version are listed below:

SWAC Improvements

- SWAC login page usability has been reviewed according to latest standards.
- SWAC components have been developed for each UMC Web UI page.
- UMC Web UI SWAC components have been documented.
- UMC SWAC documentation has been reviewed.

General Improvements

- Refactoring on low level software.
- Plugin authentication implementation has been finalized and documented.
- Upgraded to a later version OpenSSL.
- Localization has been finalized.

1.8 UMC 1.8

The main developments and improvements which were made in this version are listed below:

Secure Application Data Support (SADS)

Applications can be accessed according to function rights contained in roles assigned to users or groups. Application data should therefore be stored so that only authorized users can read or change it. This can be achieved by storing encrypted and signed data and to decrypt it according to the user's access control configuration. As a result, only the users configured to access the application can sign, verify, decrypt and encrypt the application data required to perform the necessary operations.

Important:

The SADS functionality is disabled and will be available starting from the next version.

Custom Plug-in Authentication

UMC provides a way to fully customize authentication developing your own authentication plug-in. The authentication in this case is weak, which means that the authenticated user does not have associated access rights on UMC.

Authentication via Cookie Adapter

UMC provides a way to configure authentication based on cookies. A cookie adapter is released with UMC application which allows an external authentication system to integrate with UMC authentication mechanism via cookies. This functionality has been designed to use a third-party IAM together with UMC Web SSO.

Autologin Option on Identity Provider

This functionality allows you to enable the automatic login with Windows Authentication, via Smart Card or via Cookie Adapter depending on the value assigned to a specific key ("AutoLoginMode").

1.9 UMC 1.9

The main developments and improvements which were made in this version are listed below:

Authentication

- Windows authentication is available on an agent (only for domain accounts).
- Smart card authentication: login disclaimer has been improved on ssl session.

Engineering Operations new features and improvements

- UMC engineering operations have been disabled on agent machines.

- Healthcheck functionality has been integrated into UMX command.

Secure Application Data Support (SADS)

Applications can be accessed according to function rights contained in roles assigned to users or groups. Application data should therefore be stored so that only authorized users can read or change it. This can be achieved by storing encrypted and signed data and to decrypt it according to the user's access control configuration. As a result, only the users configured to access the application can sign, verify, decrypt and encrypt the application data required to perform the necessary operations.

SADS actions are now traced in UMC ELG.

Machine Role and Scenario Support

- UMC station client registration can be performed via script
- new agent role
- Long term mixed UMC versions scenarios are supported as of UMC 1.9

Installer Improvements

SIWA allows you to install and/or to unzip the UMC setup.

Documentation improvements

- A new dedicated Security concept document.
- UMC installation documentation can be reached from the setup folder and from the setup wizard.

1.10 UMC 1.9.1

The main developments and improvements which were made in this version are listed below:

Plug-ins

- A new Stateless plug-in which does not store the identity and provides its value using events.
- Autologin with plugins.

Authentication

- Team Center Authentication which allows you to use Teamcenter Manufacturing users to authenticate on UMC.
- Implementation of Windows Authentication on a machine with the agent role.
- Authentication via user name has been added to custom plugins, meaning it is now possible to skip the creation of a user alias and use simply use the username instead.

Installer Improvements

SIWA and .Net ODK are now automatically signed.

Service Layer

Domain Name information has been added to the UMC Service Layer.

1.11 UMC 2.0

The main developments and improvements which were made in this version are listed below:

Identity Provider

- A new Identity provider has been developed, with improved speed and scalability.
- New Login UI has been provided.
- A centralized configuration system is available, which allows you to specify some of the IdP configurations for all servers and override these configurations to meet your needs.

Security

- All UMC Servers have been ported to 64 bit.
- You can now enable a password policy check to ensure that administrators can only specify passwords that meet the constraints specified by the global account policies.
- A Security Review has been performed.
- It is now possible to login from an Agent when UMC is not available.

Federation Interface

A UMC Federation Interface has been implemented to allow integration with an external IAM system.

Log Forwarding

New ‘C’ SDK is available for forwarding ELG logging to an external logging system.

1.12 UMC 2.1

The main developments and improvements which were made in this version are listed below:

Security

- Security Disclaimer can now be configured in UMC WEB UI (relevant for IEC 62443-3-3 conformity, System use notification).
- Memory cache management of IdP has been improved (relevant for IEC 62443-3-3 conformity, Concurrent session control).

Electronic Signature

A new Electronic Signature functionality is provided, to be used when a user is required to sign a specific document or transaction. In particular the following topics are available:

- New SignatureRequest API in Identity Provider
- New dedicated parameters (Description, Comment, Comment is required)
- Language and CanCancel parameters (optional)
- New Signature Request form
- New method in SWAC Login component

Second User Authentication

- The possibility to authenticate a second user without creating a new login session is provided, to be used for “right elevation” in order to perform specific actions, when the logged in user does not have the required rights.
- Authentication with smart card is also supported.

User Management

- New global account policy in WEB UI for enabling Password policy check.
- Expired Users do not depend on the System Date anymore.

1.13 UMC 2.2

The main developments and improvements which were made in this version are listed below:

Identity Provider

- New parameters are managed in the Login request:
  – Language
  – Authentication method
  – Security level
- Login UI usability has been reviewed
- Signature Request UI usability has been reviewed

Security

A session invalidation mechanism has been provided, so that after the user performs a logout the authentication cookie can no longer be used (relevant for IEC 62443-3-3 conformity, Session integrity).

Performance Improvements

An increased number of users can now be managed. In particular:

- The login perfomances were optimized in order to reach the possibility to login 500 concurrent sessions
- Group retrieving optimizations have been performed
- New limits to the binding between users and groups are available
- Tests have been performed with a scenario up to 10000 users configured.

Federation Interface

The new manual, *UMC Federation Adapter Developer Manual* has been released.

1.14 UMC 2.3

The main developments and improvements which were made in this version are listed below:

Identity Provider

- The security level of built-in authentication methods (username and password, Windows authentication) can be configured.
- New Login UI style compliant with new guideline for DF FA and PL.

Two Factor Authentication

- Second Factor Authentication by using TOTP (Time Based One-Time Password) is provided.
- Enabling and configuration in UMC Web UI
- New user profile page for managing user secret

1.15 UMC 2.4

Diagnostics

- Siemens Tracing tool is integrated for diagnostic purposes. It replaces the usage of proprietary UmTracer tool.
- Tracing tool is not distributed, it is a prerequisite. If installed, traces are written under UMC SubSystem category.
- Proprietary tracing tool is available as troubleshooting tool, to be used on demand under customer support supervision.

Desktop Single Sign-on

- A Desktop Single Sign-on functionality is provided, by which a logged in user gets access to any application running on a specific user session.
- Applications can register to be notified about any Desktop Single Sign-on session change.

CAUTION:
The Desktop Single Sign-on functionality is disabled and will be available starting from the next version.

1.16 UMC 2.5

User Management

- It is possible to export/import users in a json format text file.

Desktop Single Sign-on

- A Desktop Single Sign-on functionality is provided, by which a logged in user gets access to any application running on a specific user session.
- Applications can register to be notified about any Desktop Single Sign-on session change.

Windows Virtual Service Account support

The virtual account NT SERVICE\UMC Service can be associated to UM Service if a least privilege principle must be satisfied.

1.17 UMC 2.6

Identity Provider

It is possible to add custom languages to the Login UI Language list. Related translations must be provided.

Security

Event Logging system has been improved, in order to protect against excessive log activity.

User Management

It is possible to export/import users, groups, roles and global policies in a json format text file.

1.18 UMC 2.7

Windows Virtual Service Account support

- It is possible to import in UMC a Windows Virtual Service Account and to assign it to a UMC group.
- It is possible to authenticate an imported Windows Virtual service account.

Local User Management

A "Local" User Management functionality is provided on Windows, like the one provided for panels on Linux by the UMC for Linux component:

- It is possible to import the UMC system configuration from a json file.
- local users/groups/roles/account policies are imported from the same json file.

UMC WEB UI is customized in order to show a limited set of entities.

The functionality is reserved for specific adopters.

2 What's New

Identity Provider

- A new Identity provider has been developed, with improved speed and scalability.
- New Login UI has been provided.
- A centralized configuration system is available, which allows you to specify some of the IdP configurations for all servers and override these configurations to meet your needs.
- New parameters are managed in the Login request:
  - Language
  - Authentication method
  - Security level
- The security level of built-in authentication methods (username and password, Windows authentication) can be configured.
- It is possible to add custom languages to the Login UI Language list. Related translations must be provided.

Security

- All UMC Servers have been ported to 64 bit.
- You can now enable a password policy check to ensure that administrators can only specify passwords that meet the constraints specified by the global account policies.
- A Security Review has been performed.
- It is now possible to login from an Agent when UMC is not available.
- Security Disclaimer can now be configured in UMC WEB UI (relevant for IEC 62443-3-3 conformity, System use notification).
- Memory cache management of IdP has been improved (relevant for IEC 62443-3-3 conformity, Concurrent session control).
- A session invalidation mechanism has been provided, so that after the user performs a logout, the authentication cookie can no longer be used (relevant for IEC 62443-3-3 conformity, Session integrity).
- Event Logging system has been improved, in order to protect against excessive log activity.

Federation Interface

- A UMC Federation Interface has been implemented to allow integration with an external IAM system.
- The new manual, *UMC Federation Adapter Developer Manual,* has been released.

Log Forwarding

A new ‘C’ SDK is available for forwarding ELG logging to an external logging system.

Electronic Signature

A new Electronic Signature functionality is provided, to be used when a user is required to sign a specific document or transaction. In particular the following topics are available:

- New SignatureRequest API in Identity Provider
- New dedicated parameters (Description, Comment, Comment is required)
- Language and CanCancel parameters (optional)
- New Signature Request form
- New method in SWAC Login component

Second User Authentication

- The possibility to authenticate a second user without creating a new login session is provided, to be used for “right elevation” in order to perform specific actions, when the logged in user does not have the required rights.
- Authentication with smart card is also supported.

User Management

- New global account policy in WEB UI for enabling Password policy check.
- Expired Users are not depending on the System Date anymore.
- It is possible to export/import users, groups, roles and global policies in a json format text file.

Performance Improvements

An increased number of users can now be managed. In particular:

- The login performances were optimized in order to reach the possibility to login 500 concurrent sessions.
- Group retrieving optimizations have been performed.
- New limits to the binding between users and groups are available.
- Tests have been performed with a scenario up to 10000 users configured.

Two Factor Authentication

- Second Factor Authentication by using TOTP (Time Based One-Time Password) is provided.

- Enabling and configuration in UMC Web UI.
- New user profile page for managing user secret.

Diagnostics

- Siemens Tracing tool has been integrated for diagnostic purposes. It replaces the usage of proprietary UmTracer tool.
- Tracing tool is not distributed, it is a prerequisite. If installed, traces are written under UMC SubSystem category.
- Proprietary tracing tool is available as troubleshooting tool, to be used on demand under customer support supervision.

Desktop Single Sign-on

- A Desktop Single Sign-on functionality is provided, by which a logged in user gets access to any application running on a specific user session.
- Applications can register to be notified about any Desktop Single Sign-on session change.

Windows Virtual Service Account support

- The virtual account NT SERVICE\UMC Service can be associated to Um Service if a least privilege principle must be satisfied.
- It is possible to import in UMC a Windows Virtual Service Account and to assign it to a UMC group.
- It is possible to authenticate an imported Windows Virtual service account.

Local User Management

A "Local" User Management functionality is provided on Windows, like the one provided for panels on Linux by the UMC for Linux component:

- It is possible to import the UMC system configuration from a json file.
- local users/groups/roles/account policies are imported from the same json file.

UMC WEB UI is customized in order to show a limited set of entities.

The functionality is reserved for specific adopters.

3 Compatibility Issues

This page contains the final list of compatibility issues between this release and previous versions.

- As of UMC 2.0 the Identity Provider has undergone substantial changes which means that some of the IdP configurations have changed, see *UMC Installation Manual* for information relative to upgrading from previous version of UMC.
- UMX command umx -i(nfo) -r (rolename or roleId) -v(erbose) : the verbose option has been deprecated. Users and groups bound to a role are no more listed.
- As of UMC 2.5, UMC user database is changed due to security reasons. As a consequence:
  – A UMC server of version V<2.5, connected to a UMC ring server of version V2.5, behaves as an Agent (authenticates remotely to the ring server).
  – It is not possible to connect a new UMC server of version V<2.5 to a UMC ring server of version V2.5. The machine can be connected as an Agent.

4 Functional Limitations

General Functional Limitations are listed below whereas the functional limitations related to Active Directory Provisioning and UMC Web UI are listed in dedicated sections:

- UMC Web UI Functional Limitations
- Active Directory Provisioning Functional Limitations

Disabled Users Able to Log in via Plug-ins or Cookie Adapter Authentication

Users which have been disabled via UMC can still log in using custom plug-ins, Teamcenter Manufacturing plug-in and cookie adapter authentication.

Using UM Service Accounts Group to run UMC Services

To use a user who is a member of the UM Service Accounts Windows group to run UMC Services, you must manually grant the group full control on the CONF folder: programdata\Siemens\UserManagement\CONF, and all its sub-folders.

Setup

UMC Station Client setup: before uninstalling the UMC station client you must manually run the configuration script **slsso_configuration.bat** in C:\Program Files\Siemens\UserManagement\BIN with parameter **uninstall**.

Windows Authentication Issue with HTTP/2 (Chrome 57.0.2987.110)

The authentication issue described in the following article causes an issue with Windows Authentication: https://bugs.chromium.org/p/chromium/issues/detail?id=713851

For example:

To disable HTTP/2 on Windows 10 HTTP.SYS, set the following registry value on the Windows 10 desktop in HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters

- EnableHttp2Tls REG_DWORD 0
- EnableHttp2Cleartext REG_DWORD 0

Secure Application Data Support (SADS)

- When the agent machine is disconnected from the ring server, SADS capabilities are not available.
- Key history and key revocation:

– No SK revocation is currently supported.
– No SK history list is currently supported.
– One SK pair is supported for a Subject (group or user).
– The subject must be deleted and created again, if a SK must be revoked.

UMCONF

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

Multi-Language

- Authentication procedure may fail if the user name and/or password contain both latin and non latin characters.
- Authentication procedure may fail if the user name contains upper case characters whose conversion in lower case is not unique. Examples are ΠΣ and Ö.

Windows Integrated Authentication

- Windows Integrated Authentication does not work in an http scenario.
- In Windows 10 and Windows Server 2016, due to a Chrome mulfunction, the first time that you open the browser the Windows Integrated Authentication does not work with one click. A second click is necessary to log in.

Web Components

- The UMC Web Components (Identity Provider, Web UI, Remote Authentication) have not been tested on a 32 bit machine.
- If the Identity Provider is configured in https, all the relying parties (i.e. the Web UI) have to be configured to work in https. Using a relying party in http, while it is configured in https, does not guarantee the correct application behavior.

Concurrent Modifications via Web UI

Lock mechanism has to be improved: the lock on an object is currently performed only during the write operation.

Redundancy

The single message "unlock" is not implemented.

Plugin Management

After registering/deregistering a plugin, for each machine where the Identity Provider is installed, the plugin registration is loaded by Identity Provider with a delay of about 1 minute. In the case an immediate change is needed, it is necessary to restart the **UMCService**.

4.1 User Management Component Web UI

Usability

- Error messages have to be improved.
- Web UI pages do not support notifications. In some cases you need to refresh the page to display the last updates.

Multi-Language

The descriptions of Function rights are not localized.

Importing Users/Groups

- For imported users, the value of the columns **Can Change Password** and **Must Change Password** in the grid are not coherent with the corresponding values on Active Directory.
- When importing users/groups, in case you need to execute queries retrieving a large number of items, you may need to modify the Active Directory administration limit **MaxPageSize**. For more details, see for instance the following links:
  - https://support.microsoft.com/en-us/kb/315071
  - https://technet.microsoft.com/en-us/library/aa998536%28v=exchg.80%29.aspx.
- When importing a group having a high number of associated users, you may need to modify the Active Directory administration limit **MaxValRange**. For more details, see for instance the following links:
  - https://support.microsoft.com/en-us/kb/315071
  - https://technet.microsoft.com/en-us/library/aa998536%28v=exchg.80%29.aspx.
- Importing users/groups having names shorter than 3 characters is not possible using the Web UI. You have to use the **umx** command.

Inline Editing for Imported Users/Groups

The **Edit** button is present in the grid for imported groups, but no fields can be edited inline.

4.2 Active Directory Provisioning

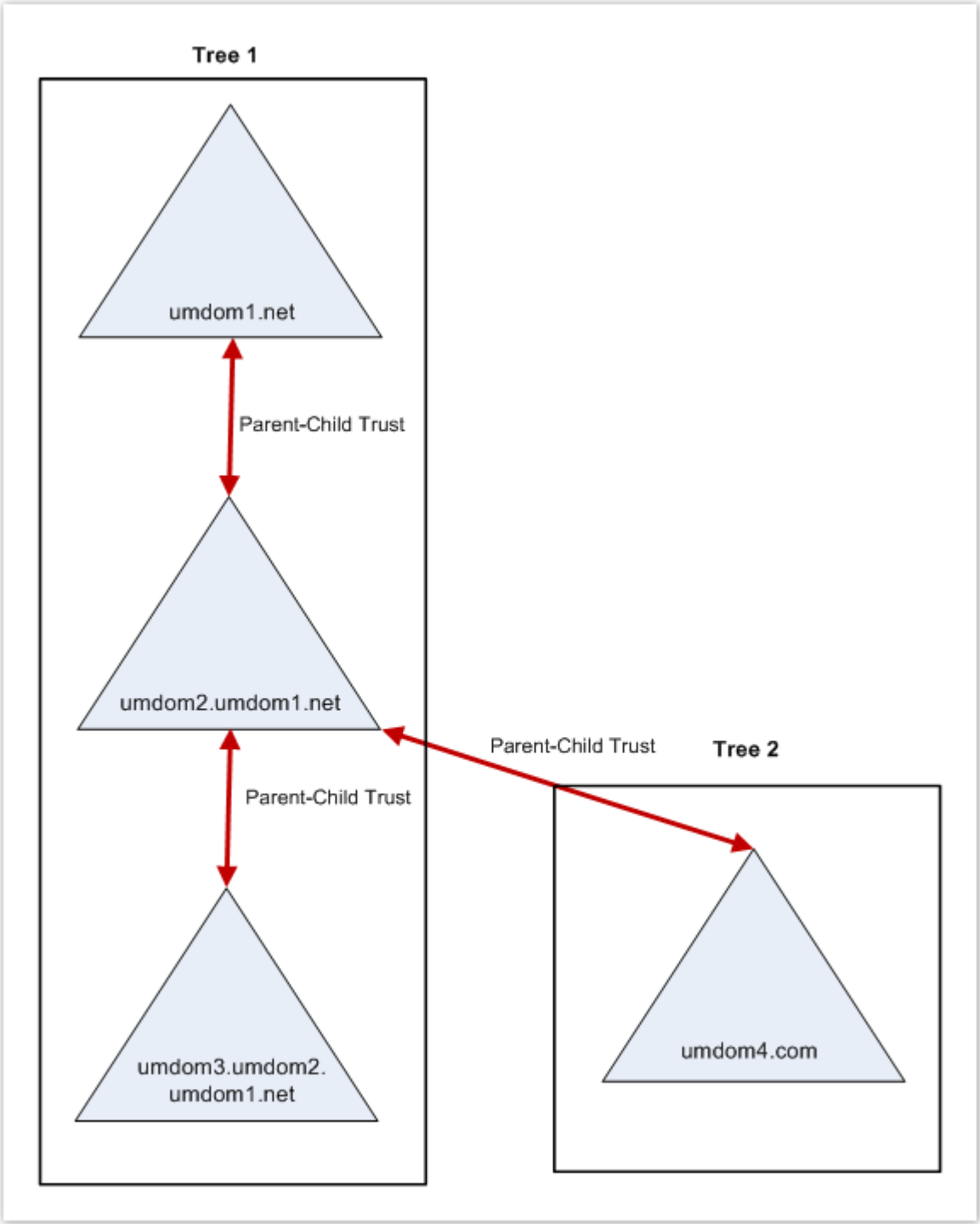
List Windows Domains

Both **umx** and Web UI do not allow you to list Windows domains trusted to one of the domains belonging to the hierarchy of the domain of the machine where you are running the command.

Import AD Users

Web UI allows you to import AD users from a trusted domain to one of the domains belonging to the hierarchy of the domain of the machine on which the Web UI is installed.

Example
Consider the following domain trees where your ring server machine is joined to the Windows domain **umdom1.net** (or one of the children domains). Using **umx**, you cant list and import the users in the domain **umdom4.com**. You can also list and import the users and groups belonging to **umdom4.com** using via Web UI, but to do so all the domains must be specified in the **piisrv_config.json.**



Import Users from Domains with the same Label

Both **umx** and Web UI do not allow the import of users belonging to domains having the same name label. For example, users cannot be imported from the trusted domains **dom1.net** and **dom1.com**.

Initials and Mobile AD fields

The AD fields **Initials** and **Mobile** are not imported.

Supported Groups

Only groups having the **Group scope** equal to **Universal** are supported.

Delete an imported user

Deleting an imported user (directly not via group) in AD is not synchronized. The user has to be manually deleted in UMC.

AD Recursive Groups

We do not support AD recursive groups. Only direct members of an AD group are imported into UMC.

Group Import

The import of groups implies a search on Active Directory that can take a considerable amount of time. If you import a group, via **umx** or Web UI, and immediately after you delete it, the UMC database can be temporarily misaligned. The synchronization service will perform the alignment at the next synchronization round.

Slow Data Alignment after AD Modifications

If you perform AD modifications (such as the update of an AD user field) and you have many users (more than 500), it can happen that UMC data are aligned slowly.

UMC Web UI on Windows 7 Machine

If UMC Web UI is installed on a Windows 7 machine, you have to install https://support.microsoft.com/en-us/kb/932552 to perform AD import.

5 Fixed Technical Issues

This page contains the final list of fixed issues for the version.

ID	Title
1986141	Password policy check during user update.
2438929	Password length can be entered as type float.
2614821	Wrong error message when an attach is tried on a user that does't have the "UM_ATTACH" function right.
2619838	In the Server, both Ring master and Authentication server are pointing to PRS machine after SRS came down.
2657863	UMAC : Adding a user with filter box enabled creates empty users.
2706998	PRS_Account Policy_Change a Set of Account Policies.
2712059	UMAC: Minimum Password Length is not working.
2772452	In UMC > Event Log, data in the **Source** column is not consistent and differs according the user action.
2825965	Sporadic behavior: Able to delete the Administrator Role in UMC.
3141205	Sporadic crash of W3WP Process while starting the product and logging in.
3032285	If the UMC user requires a password change at the first login in UMAC or UMC, it accepts the original password as new password.
3110276	SL_GenerateTicket does not work with SL_AuthenticateFromClaim.
3260657	Unable to perform engineering operations (SL_NOT_MASTER).
3281435	Active directory and UMC integration are not able to configure the polling time.
3281437	AD users update cannot be removed automatically.
3727910	Active directory group wrong update tentative in UMC.
3783022	[piisrv] Unexpected end of process for provisioning piisrv.

Some security improvements have been also applied.

6 Release Test Tools

The following tools/test pages are included in the current delivery for testing or diagnostic purposes and may be removed in the final delivery when the final functionality will be completed.

Important:

In case of a request that requires modifications in a tool, the opportunity of a fix will be evaluated case by case.

7 Appendix

In this section you can find the following information:

- Health Check Service
- Additional provisioning configurations

7.1 Health Check Service

CAUTION:

The JSON structure is under construction and subject to change.

UMC Health Check is an HTTPS service whose data exchange is based on JSON format.

Example URL

```
https://localhost:16/healthcheck
```

Allowed ports are also 32 and 2259.

Response JSON Example


```
{
   "server_status":
  [{"is_running":1,"server":"Electronic Log"},
   {"is_running":1,"server":"Resource Authenticator"},
   {"is_running":1,"server":"Resource DB Manager"},
   {"is_running":1,"server":"UM Authenticator"},
   {"is_running":1,"server":"UM File Server"},
   {"is_running":1,"server":"UM Join Server"},
   {"is_running":1,"server":"UM Key Server"},
   {"is_running":1,"server":"UM Remote IPC Service"},
   {"is_running":1,"server":"UM Ring Server"},
   {"is_running":1,"server":"UM Secure Communication Service"}],
   "machine_status":
  [{"connected_to_authentication_server":"vm-vdip22-03",
    "connected_to_ring_master":"vm-vdip22-03",
    "discovery_status":"connected",
    "machine_role":"ring",
    "safemode":0,
```

```
     "version":"105.0.201.10",
     "workstation_status":"master"}],
    "claim_key":1,
    "ticket_key":1,
    "um_database":1,
    "health": 1
}
```


Response JSON Description

server status property Array

Each server status object has the following properties:

Property	Type	Description
isrunning	integer	It is equal to 1 if the server is running, 0 otherwise.
server	string	A generic server description according to the following correspondence: **Process name** / **Health check description** um.ELGSrv.exe — Electronic Log um.RACRMSRV.exe — Resource Authenticator um.RACSERV.exe — Resource DB Manager um.server.exe — UM Authenticator um.ffsyssrv.exe — UM File Server um.jei.exe — UM Join Server um.kei.exe — UM Key Server um.Ris.exe — UM Remote IPC Service um.ring.exe — UM Ring Server IPCSecCom.exe — UM Secure Communication Service See the *UMC Installation Manual* for more details.

machine status property Array

The machine status object has the following properties. If the **health** property is equal to 0, that means the health check did not pass, the **machine status** property is not returned.

Property	Type	Description
connected_to_authentication_server	string	The machine name (UM ring server or UM server) to which authentication requests can be sent.
connected_to_ring_master	string	The ring master machine.
discovery_status	string	The discovery status. Possible values are: **connected**, **standalone** (not used), **no_configuration_found**, **not_initialized**, **generic_error**.
machine_role	string	The machine role. Possible values are: **ring**, **server**, **agent**.
safemode	integer	It is equal to 1 if the machine is a UM ring server in safe mode, 0 otherwise.
version	string	Installed UMC version.
workstation_status	string	Possible values are: • **master**, the machine is a master UM ring server; • **online**, the machine is a UM ring server, not master, or a UM server; • **remote_master_is_in_safe_mode**, the machine is a UM server connected to a master in safe mode; • **initializing**, the machine is an initialization phase; • **degraded**, the machine is a UM server not connected to any UM ring server; • **unconnected**, not connected; • **segregated**, the machine is a segregated server; • **error**, generic error.

Additional properties

Property	Type	Description
claim_key	integer	It is equal to 1 if the UMC system can generate a claim key, 0 otherwise.
ticket_key	integer	It is equal to 1 if the UMC system can generate a ticket key, 0 otherwise.
um_database	integer	It is equal to 1 if all the needed UMC databases are present, , 0 otherwise.
health	integer	It is equal to 1 if all the health checks are passed, 0 otherwise. If the **health** property is equal to 0, that means the health check did not pass, the **machine status** property is not returned.