SIEMENS

User Management Component 2.9.2

UMC Installation Manual

Contents

09/2020
A5E50361197-AA

Guidelines

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

Important:

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

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

Trademarks

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

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

Disclaimer of Liability

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

Security information

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

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

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

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

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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E50361197-AA
20200910_42680

Contents

1 Concepts You Need to Know About

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

- User Manager Domain
- User Manager User
- User Manager Group
- Machine Roles
- Deployment Scenarios
- Built-in User Roles

1.1 User Manager Domain

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

Important:

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

1.2 User Manager User

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

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

UM User Types

You can distinguish three types of UM users:

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

UM User Passwords

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

Offline Users

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

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

Important:

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

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

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

User Limits

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

1.3 User Manager Group

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

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

UM Group Types

There are two types of UM groups:

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

Offline Groups

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

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

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

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

{{Q=<ldap query>

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

Group Limits

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

1.4 Machine Roles

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.

The main differences between the three aforementioned machine roles are listed in the table below.

The ring server to which the other ring servers send the request to write on the UMC database (the candidate for writing) is called *master ring server*. Both the priority and secondary ring server can be master.
If the priority server is master, writing is enabled and the machine can write on the UMC database.

In case of failure, the secondary ring server becomes a master ring server with no writing enabled (*safe mode on*). If the safe mode is switched off using the appropriate umx command, the secondary ring server becomes a master with writing enabled. Consider that some operations on the UMC system configuration are not allowed in this case, e. g. modifying the whitelist (see *UMCONF User Manual* for more details).

UMC Station Client

A machine role orthogonal to the previous ones is *UMC station client*. A UMC station client is a machine where UMC station client software has been installed and that has been registered to be a trusted machine. A UMC station client provides a claim in which certified logon station information is included. These details can be used to associate authorization rights with a machine, which must not be a ring server, server or agent, using the client product.

UMC installation includes the UMC station client installation, thus, UM ring servers, UM servers and UM agents need only to register to become UMC station clients, whereas a machine that is not part of the UMC domain has to install the UMC station client software first and then has to register to become a UMC station client.

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.

Machine Role Functionalities

The table below provides the functionality mapping against the machine roles. For each functionality:

 denotes that the functionality has been fully implemented;

⊖ denotes that the functionality is not available.

⚠ only available when the system is connected to the UM Server

	UM Server	UM Ring Server	UM Agent
Perform TIA User authentication	⊕	⊕	⚠
Local single modifications	⊖	⊕	⊖
Change password	⊕	⊕	⚠
Authentication against Active Directory	⊕	⊕	⊕
Manage Domain attach/join	⊕ (acts as proxy for agents)	⊕	⊖
Potential Master	⊖	⊕	⊖
Can sign authentication object	⊕	⊕	⊖
Propagate UM configuration	⊖	⊕	⊖
Can host Identity Provider /Remote Authentication or UMC Web UI	⊕	⊕	⊖
Number of instances	max 4	1-2	max 25
Off Line Authentication/Read-Only on the configuration	⊕	⊕	⊖
Ring Failover - recovery	⊕	⊕ (merge missing)	⊖
Electronic Log Store&Forward	⊕	⊕	⊖
Log Forwarding	⊖	⊕	⊖
Import Windows Local Users	⊕	⊕	⊕
Import AD Users/Group	⊕	⊕	⊖

Propagation of UM configuration

The UM configuration is distributed from the master ring server to the UM servers, in order to allow a faster local authentication. Any configuration change is performed on the primary master ring server and then propagated to the connected UM servers. The synchronization of the configuration starts when at least 30 seconds from the last modification are passed. This “stabilization” time is required for avoiding too many alignments in case many close changes are performed. After that time the propagation of the configuration starts, which means that some other time (typically from few seconds to few minutes) is required before the configuration alignment is completed on all the UM servers.

Offline availability

As the UM configuration is distributed from the master ring server to the UM servers, the authentication of UMC users is performed locally. Therefore, authentication of UMC users is available on UM servers also when the UM server is disconnected from the ring server, provided that the configuration has been propagated before the disconnection occurs.

Authentication of AD users is performed by Windows, therefore the alignment of UM configuration is not sufficient for providing an offline authentication. In this case, authentication must occur at least once to allow a user to authenticate when offline, through the usage of a temporary cache.

The configuration of Secure Application Data Support is not aligned by default on UM servers. As a consequence, Secure Application Data Support is not available when the UM server is disconnected from the ring server. It is possible to configure on a Group that the users of this group are allowed to use Secure Application Data Support also when offline. For the configured group the needed Secure Application Data Support configuration is propagated from the ring server to the UM servers, therefore allowing a local usage.

1.5 Deployment Scenarios

We support the following deployment scenarios:

- **standalone scenario**: one ring server where UMC and all its Web components are installed and configured. A quick configuration guide is available for this scenario.
- **redundant scenario**:
  – 2 UM ring server machines, one ring server is configured first and is called *priority ring server*, the secondary one is added to the ring using the join command;
  – up to 4 UM servers
- **distributed scenario**:
  – 1 or 2 UM ring server machines, one ring server is configured first and is called *priority ring server*, the secondary one is added to the ring using the join command;
  – up to 4 UM servers
  – up to 25 UM agents.

Each UMC Web component can be installed and configured on any UM ring server and/or on any UM server. If you install the UMC Web UI on a UM server, you cannot import AD users via UMC Web UI.

NLB redundancy is supported only for Identity Provider.

Standalone engineering station

UMC allows you to prepare configuration data (users, groups and so on) in a standalone engineering station, export this data in a UMC configuration package which can then be imported into a production target system. The two commands involved are the umx export and import package commands. If you want to overwrite the configuration of the target production system with that of the source engineering machine the update command can be used instead of the import command. For more information on these command and how they impact the target machine, see the *UMX User Manual*.

If the target system is not configured, you can import a package using the umconf import package command. For more information see the *UMCONF User Manual*.

1.6 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 Supported Browsers

The following browsers are supported either by the Identity Provider and by the Web UI.

General Recommendations

- For security reasons, we suggest that you set the browser cookie policy management so that cookies are not maintained after the browser is closed. In this way you can disable the possibility that a user reopens a browser and is logged in without providing the credentials again.
- The browser used to display the UMC Web UI must allow the pop-up display.
- While using the UMC Web UI do not select the option **Prevent this page from creating additional dialogs**. The selection of this option causes Web UI malfunctions.
- Disable the **Autocomplete** option in your browser settings.
- Disable the password saving option in your browser settings.

Identity Provider

- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11
- Chrome 32.0.1700.107 m or higher
- Firefox 31.0 or higher
- Microsoft Edge 25.10586.0.0 or higher
- Microsoft Edge 83.0.478.58 (Chromium based)

UMC Web UI

The Web UI is based on HTML5. For this reason it is supported only on:

- Internet Explorer 11
- Chrome 32.0.1700.107 m or higher
- Firefox 31.0 or higher
- Microsoft Edge 25.10586.0.0 or higher
- Microsoft Edge 83.0.478.58 (Chromium based)

Important:

The following resolutions are supported:

- 1280x800
- 1920x1200

3 Prerequisites

The following lists the prerequisites for UMC divided by:

- General Recommendations
- Supported Operating Systems
- Microsoft Visual C++ Packages
- Identity Provider Prerequisites
- IIS Configuration
- If you wish to use HTTPS instead of HTTP you must configure IIS for HTTPS

General Recommendations

- **Operating Systems:** The operating system must be updated to the latest security patches in order to improve system reliability and security,
  The Windows Security Patch KB2532445 must be installed on the following OS:
  – Windows Server 2008 R2 SP1(Professional, Enterprise, Datacenter Edition)
  – Windows 7 SP1 (x86, x64)
- **Computer Naming Conventions:** The computer name of the machines on which you will install UMC must only contain alphanumeric characters and not exceed 15 characters. See host name limitations in Microsoft Support Documentation for more information.

Note: If the configuration of Windows is such that the temp files are deleted when the system is restarted, the installation will fail if the system is restarted by the setup. Should this occur you must launch the setup again.

Supported Operating Systems

UMC can be installed on the following Operating Systems:

- Windows Server 2019 (Standard)
- Windows Server 2016 (Standard)
- Windows Server 2012 R2 (Standard, Datacenter Edition)
- Windows Server 2008 R2 SP1 (Standard, Enterprise, Datacenter Edition)
- Windows 8.1 (x86, x64)
- Windows 7 SP1 (x86, x64)
- Windows 10 Version 1511 (OS Build 10586.0) or subsequent (x86, x64)

The following table lists the UMC components which can run on 32 or 64 bit machines.

Component	32 bit	64 bit
UMCONF	✓	✓
UMX	✓	✓
Identity Provider	✗	✓
Web UI	✗	✓
Remote Authentication	✗	✓
Integrated Windows Authentication	✗	✓
Service Layer API	✗	✓
API SDK	✓	✓

Microsoft Visual C++

In order to install UMC, the following redistributable packages have to be installed on Windows server 2008 R2, Windows 7, Windows 8.1, Windows server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 10:

- Microsoft Visual C++ 2015 Redistributable - x86 14.0.23026.00
- Microsoft Visual C++ 2015 Redistributable - x64 14.0.23026.00

Important:

- For 32-bit operating system versions only the 32-bit redistributable packages have to be installed, whereas for 64-bit operating system versions all the redistributable packages have to be installed.
- In the BUNDLE and SIWA installers the redistributable packages are automatically installed.

Identity Provider Prerequisites

- The machine has to be a 64 bit machine.
- Microsoft Framework:
  - Microsoft .NET Framework 4 Client Profile
  - Microsoft .NET Framework 4 Extended
- Microsoft Internet Information Services:
  - Internet Information Services 7.5, 8, 8.5, or 10. Note that in the case of IIS 7.5 you must add .json to the MIME types.
- IIS extension: Application Request Routing 3.0 and its prerequisites have been downloaded and installed (you can download and install web platform from here: http://www.microsoft.com/web/

downloads/platform.aspx, launch it on the machine and search for Application Request Routing 3.0).

CAUTION:

UMC Web services use cookies to guarantee the correct functioning. We do not display any warning related to cookie usage, as our application must not be used as an open Web service, available, for instance, on the Internet.

3.1 IIS Prerequisites

IIS configuration verification steps vary depending on the version of Windows on which it is being performed. The following verification procedures are based on: Windows Server 2016 and Windows 10

In order to harden your system it is recommended you install the minimum set of IIS features possible, see *UMC Security Concept* for more information on system hardening.

Windows Server 2016

Verify the following features and roles are installed for Windows Server 2016.

1. On the start page click **Server Manager.**
2. Click **Dashboard** on the left pane.
3. Click **2 Add Roles and Features.**
4. Click **Role-based or feature-based installation** and click **Next**.
5. Select a server from the list and click **Next**.
6. Verify the following **Roles** are selected under **Web Server (12 of 34):**
   – **Common HTTP Features (4 of 6)**
      - **Default Document**
      - **Directory Browsing**
      - **HTTP Errors**
      - **Static Content**
   – **Health and Diagnostics (1 of 6)**
      - **HTTP Logging**
   – **Performance (1 of 2)**
      - **Static Content Compression**
   – **Security (2 of 9)**
      - **Request Filtering**
      - **Windows Authentication**
   – **Application Development (4 of 11)**
      - **.Net Extensibility 4.6**
      - **ASP.NET 4.6**
      - **ISAPI Extensions**

- **ISAPI Filters**

7. Verify the following **Roles** are selected under **Management Tools (3 of 7):**
   – **IIS Management Console**
   – **IIS Management Scripts and Tools**
   – **Management Service**
8. Click **Next.**
9. Verify the following **Features** are selected:
   – **.Net Framework 3.5 Features (1 of 3)**
      - **.Net Framework 3.5 (includes .net 2.0 and 3.0)**
   – **.Net Framework 4.6 Features (3 of 7)**
      - **.NET Framework 4.6**
      - **ASP.NET 4.6**
      - **WCF Services (1 of 5)**
         - **TCP Port Sharing**
   – **Windows Defender Features and WoW64 Support**
      - **Windows Defender**
      - **GUI for windows Defender**
   – **Windows PowerShell (3 of 5)**
      - **Windows PowerShell 5.1**
      - **Windows PowerShell 2.0 Engine**
      - **Windows PowerShell ISE**
10. Close **Windows Server Manager**.

Windows 10

Verify the following features and roles are installed for Windows 10.

1. Type "*Turn Windows Features on and off*" in the **Search Windows** search box.
2. Click **Turn Windows Features on and off** in the result pane, a windows is displayed.
3. Verify the following are installed under **Internet Information Services**:
   – **Web Management Tools:**
      - **IIS Management Console**
      - **IIS Management Scripts and Tools**
      - **IIS Services**
   – **World Wide Web Services:**
      - **Application Development Features**
         - **.Net Extensiblity 4.6**
         - **ASP.NET 4.6**
         - **ISAPI Extensions**
         - **ISAPI Filters**
      - **Common HTTP Features**

- **Default Document**
- **Directory Browsing**
- **HTTP Errors**
- **Static Content**

- **Health and Diagnostics**
  - **HTTP Logging**

- **Performance Features**
  - **Static Content Compression**

- **Security**
  - **Request Filtering**
  - **Windows Authentication**

– **.Net Framework 3.5 Features**

– **.Net Framework 4.6 Advanced Features**
  - **ASP.NET 4.6**
  - **WCF Services**
    - **TCP Port Sharing**

– **Windows PowerShell 2.0**
  - **Windows PowerShell 2.0 Engine**

4. Click **Cancel** to close the window.

3.2 Configuring Https Protocol in Microsoft IIS

This procedure allows you to configure IIS to work with HTTPS protocol and is only required if you wish to use HTTPS protocol, which is strongly recommended in plant environments.

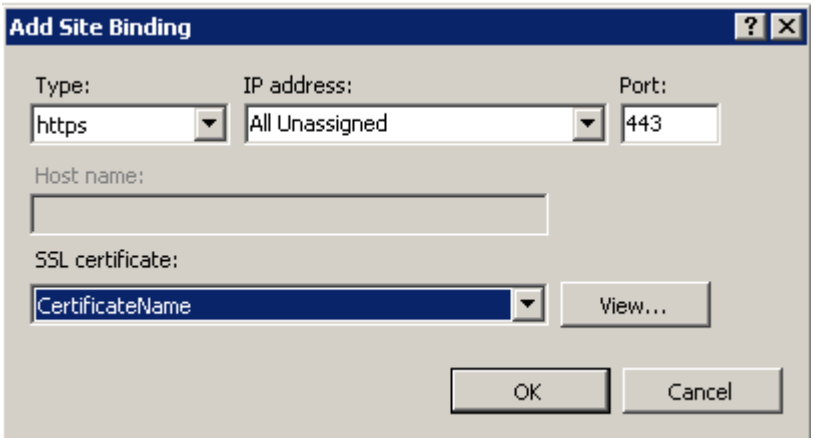
Prerequisites

A valid SSL certificate has been acquired from a Certification Authority or a self-signed SSL certificate has been created.

Procedure

1. Open **IIS Manager**.
2. In the tree on the left go to the node of the site which you have configured.
3. Right click on the node and select **Edit Bindings**.

4. Click **Add**: the following dialog box opens.



5. Insert the parameters as displayed in the previous image and click **OK**. The **SSL certificate** parameter has to be the acquired certificate name.
6. Click **OK** and then **Close**.

4 How to Configure UMC

The UMC can be configured in a:

- standalone scenario by configuring only a priority ring server,
- redundant scenario by adding a secondary ring server,
- distributed scenario with multiple servers, agents and station clients.

Depending on your scenario you can use one of the following workflows:

- For a simple standalone UMC installation on 64bit machine with HTTPS you can follow the Quick Configuration - Standalone UMC Scenario,
- For distributed and redundant scenarios or additional configurations, for example if you wish to install UMC on a 32 bit machine follow How to Configure a UMC Scenario.

HTTP Configuration

CAUTION:

We strongly suggest that you enable HTTPS in plant environments.

If HTTPS protocol has been configured HTTP cannot be used.

If IIS is not configured to work with https protocol, you can configure UMC both manually and via script, but secure protocol is not enabled. In this scenario:

- If UMC Web UI does not work, verify that the value of the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\User Management\WebUI\Settings\secure is set to 0.
- Smart card authentication does not work.

4.1 Quick Configuration - Standalone UMC Scenario

The following procedure describes the minimum steps required to configure a UMC standalone scenario, therefore a machine which has the role priority ring server. The procedure does not endeavor to document all the possible configuration options, however some additional configurations which can be applied to this scenario are listed in additional configurations, for more complex configurations and scenarios, see How to Configure a UMC Scenario.

Prerequisites

- Full UMC installation has been installed.
- IIS has been configured to work with the HTTPS protocol.
- The operating system is 64 bit.

- (only required to manage Active Directory users) the Windows user specified at step 2 (managing Active directory users) must have:
  – Active Directory access rights;
  – Write access on the UMC program data subfolder \CONF(for example C:\ProgramData\Siemens\UserManagement\CONF) or alternatively belong to the Windows group **UM Service Account;**

Procedure

1. Right-click **UMConf,** which can be found in the subdirectory in Bin or Wow\bin, for example; C:\Program Files\Siemens\UserManagement\Wow\Bin, and select **Run As Administrator.**
2. Following the guided configuration in UMConf Interactive mode:
   – Create a User Management Domain, by specifying a name using only alphanumeric characters.
   – Create a User Management User with administrator role, by specifying the username using only alphanumeric characters, and a password which complies with your organization's password policy.
   – Associate a Windows user who is either a member of **UM Service Accounts** group or who has administrative rights to the **UMCService,** by inserting .\ *username* and the corresponding password.
   – (optional) To manage Active Directory users, specify a Windows user as described in prerequisites, by inserting *domain**username* and password.
3. Right-click **IdP_WebUI_configurator.bat,** which can be found in C:\Program Files\SIEMENS\UserManagement\BIN, if the default installation folder is selected, and select **Run as Administrator.**

Result

UMC and the identity provider web are configured.

Additional Configurations

- Configure Firefox for Integrated Windows Authentication, this procedure is not required for other browsers.
- Perform Additional Identity Provider Configuration.
- If SADS (Secure Application Data Support) is required, it must be enabled via the UMX utility, by running the command: umx -AP -setakp, for more information see the *UMX User Manual.*
- If SLRA support is required, see Configure SLRA support.
- If Desktop Single Sign on is required, see Configure Desktop Single Sign On.

4.2 How to Configure a UMC Scenario

Prerequisites

- 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.
- Check that the connectivity to TCP/4002 is enabled on all machines (or disable firewall on **um.Ris.exe**, the UM process responsible for UM machines communications).
- The firewall configuration on UMC Servers and Ring Servers must be configured to allow inbound access on either the port which is used for HTTP (by default 80) or, the port that is used for HTTPS (by default 443).

Workflow

1. Configure the machine you have elected as priority master.
2. Configure the machine you have elected as secondary master (only for redundant scenario).
3. (Optional) Configure one or more machines as UM servers, using the **UMConf.exe** program on the User Management, to join the server to the domain (**serverType** parameter equals to 0) . Refer to the *UMCONF User Manual* for more details.
4. (Optional) Configure one or more machines as agents, using the **UMConf.exe** program on the User Management, to attach the agent to the domain. Refer to the *UMCONF User Manual* for more details.
5. Configure the web components.
6. (Optional) Install and configure UMC station clients.
7. (Optional) Configure SLRA support.
8. (Optional) Configure Desktop Single Sign On.

Additional Operations

- The following optional step can be performed on one of the previous machines:
  Associate an administrative Role with a user, so that this user can run the **umx.exe** command or can log in to the Web UI to manage UM users and groups.

4.2.1 Configuring UM Priority Ring Server

Once UMC has been installed the configuration must be performed via UMConf**.** The steps are described using UMConf in interactive mode. **UMConf.exe** is distributed with UMC and installed in the subdirectory \BIN(64bit) or Wow\Bin (32bit). If you need to import an existing configuration import command must be executed via a **UMConf.exe**, for more information on UMconf see the *UMCONF User Manual.*

Prerequisites

- Full UMC installation has been installed.
- (only required to manage Active Directory users) the Windows user specified at step 2 (Managing Active directory users) must have:
  – Active Directory access rights;
  – Write access on the UMC folder C:\ProgramData\Siemens\UserManagement\CONF or alternatively they must belong to the Windows group **UM Service Account**.

Procedure

1. Right-click **UMConf,** which can be found in the sub-directory Wow\bin, for example; C:\Program Files\Siemens\UserManagement\Wow\Bin, and select **Run As Administrator.**
2. Following the guided configuration in UMConf Interactive mode:
   – Create a User Management Domain, by specifying a name using only alphanumeric characters.
   – Create a User Management User with administrator role, by specifying the username using only alphanumeric characters, and a password which complies with your organization's password policy see *UMC Security Concepts* for more information;
   – Associate a Windows user who is either a member of **UM Service Accounts** group or who has administrative rights to the **UMCService,** by inserting .\ *username* and the corresponding password.
   – (optional) To manage Active Directory users, specify a Windows user as described in prerequisites, by inserting *domain**username* and password.

Note:
- If SADS (secure application data support) is required see the *UMX User Manual*.
- the user which is assigned to the UMCService must only be modified via UMConf.

Additional Operations

Additional provisioning configurations can also be performed.

4.2.2 Configuring UM Secondary Ring Server

Prerequisites

- You must have created the main ring server machine.
- A full UMC Installation has been installed on the machine.
- If https is required you must configure https in IIS.

Procedure

To create another ring server machine:

1. Join the server using the **umconf.exe** program. See *UMCONF User Manual* for more details.
2. If you have configured the AD provisioning on the priority ring server, you have to configure it also in the secondary ring server.

Additional Operations

- Additional Provisioning Configuration can also be performed.
- In order to add the Service Layer to whitelisting login to the WEB UI using the Administrator user created during the initial configuration.

4.2.3 How to Configure UMC Web Components

Once UMC has been installed if required you can configure the web components as described below.

Prerequisites

- The machine is configured as a UMC ring server or server
- if the machine is not primary ring server you must add the service layer to white-listing by logging in to the Web UI with the Administrator user or via umconf on the primary ring server.
- The firewall configuration on UMC Servers and Ring Servers must be configured to allow inbound access on either the port which is used for HTTP (by default 80) or, the port that is used for HTTPS (by default 443).
- If you are using HTTPS protocol IIS must have been configured to work with the HTTPS protocol.

Configuration Types

- via script: 64bit and HTTPS only. The script configures the web components automatically.
- manually: The manual method can be used for HTTP or HTTPS. You can also use the method in order to structure your own custom configuration script.

Web Components Configuration Reset

UMC provides a script, **REMOVE_IdP_WebUI_configurator.bat**, to reset the configuration of the Web Components. The batch file can be found in C:\Program Files\SIEMENS\UserManagement\BIN, if the default installation folder is selected, and can only be used on a 64 bit machine.

CAUTION:

If you perform any modification to the IIS configuration after launching the configuration script **IdP_WebUI_configurator.bat** or you have configured UMC without using this script**,** you have to reset the Web components configuration and, only afterwards, configure the system again .

4.2.3.1 Configuring UMC Web Components Via Script

To configure all the Web components on the same UM ring server/UM server, UMC provides the script **IdP_WebUI_configurator.bat** which allows you to configure them to work with the HTTPS protocol and to configure the integrated Windows authentication (except the Firefox configuration that has to be performed manually).

The batch file can be found in **C:\Program Files\SIEMENS\UserManagement\BIN**, if the default installation folder is selected. If IIS has been previously configured to work with the HTTPS protocol, the script configures the Web components accordingly.

Note:

- If the user which is used to run the script is a Windows local user, the FQDN cannot be retrieved, this results in the registry key of the IDP being configured with only the machine name and not the domain name.
- If you have configured a site in IIS with a name which is not **Default Web Site,** you must open a command prompt as administrator from the installation folder of the . bat file. and specify the name of the site as first parameter: for example, C:\ Program Files\Siemens\UserManagement\BIN>IdP_WebUI_configurator.bat "your web site name".
- If you want to specify a specific "reverseProxy" value, different from the one retrieved automatically in the script and you want to use it in the Identity Provider configuration, you can set it as second parameter when launching the **IdP_WebUI_configurator.bat** script: for example, C:\Program Files\Siemens\ UserManagement\BIN>IdP_WebUI_configurator.bat "your web site name" "your reverse proxy address".
- By default the Identity Provider node.exe process is listening on port 8443. If you want to modify this default value you can set the desired port value as third parameter when launching the **IdP_WebUI_configurator.bat** script: for example, C:\Program Files\Siemens\UserManagement\BIN>IdP_WebUI_configurator.bat "your web site name" "your reverse proxy address" "port number".
- If you want to specify a certain parameter keeping the default values of the previous parameters it is necessary to pass an empty string for the parameters that you don't want to customize. For example, to specify only a certain port number without modifying the IIS site name and the reverse proxy address, you have to call the **IdP_WebUI_configurator.bat** script in this way: C:\Program Files\ Siemens\UserManagement\BIN>IdP_WebUI_configurator.bat "" "" "port number". The empty double quotes specify an empty value for the parameters that will be passed to the script.

General Recommendations

The Web components can be configured in any UM ring server and/or in any UM server. In order to guarantee IdP high availability and reliability, we suggest that you install and configure it on more than one machine and configure the IdP high availability/reliability.

Prerequisites

- IIS has been previously configured to work with the HTTPS protocol.
- The operating system must be 64 bit
- The machine is configured as a UMC ring server or server.

Workflow

1. On all the servers on which you want to configure the Web components, right-click **IdP_WebUI_configurator.bat,** which for example can be found in C:\Program Files\SIEMENS\UserManagement\BIN, if the default installation folder is selected, and select **Run as Administrator**.
2. Configure Firefox for Integrated Windows Authentication (optional).
3. Configure smart card authentication (optional).
4. Perform Additional Identity Provider Configuration (optional).

4.2.3.2 How to Configure UMC Web Components Manually

General Recommendations

The Web components can be configured in any UM ring server and/or in any UM server. In order to guarantee IdP high availability and reliability, we suggest that you install and configure it on more than one machine and configure the IdP high availability/reliability.

Prerequisites

If required IIS has been previously configured to work with the HTTPS protocol.

Workflow

1. Configure the following:
   – Identity Provider in IIS
   – Web UI and Service Layer API
   – Remote Authentication
   – URL Rewrite Rules
   – Adding the ServiceLayer to Whitelist

– Identity Provider .json file;

2. Perform the following additional Web configuration steps:
   – configure Integrated Windows Authentication;
   – configure Firefox for Integrated Windows Authentication;
   – configure Smart Card Authentication;

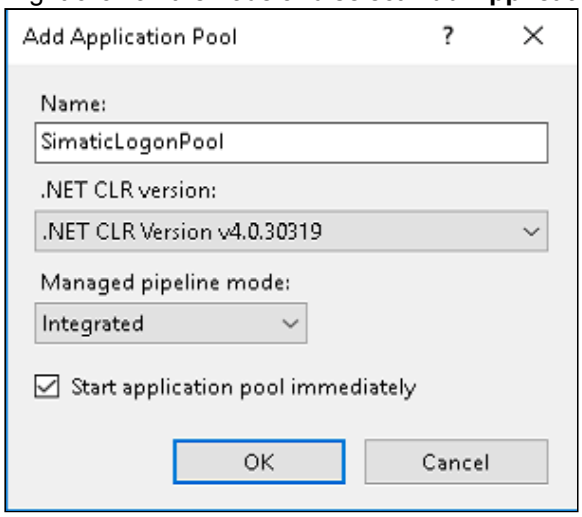
4.2.3.2.1 Configuring Identity Provider

Prerequisites

- The Identity Provider prerequisites are installed.
- The machine is a 64 bit UM ring server or UM server.

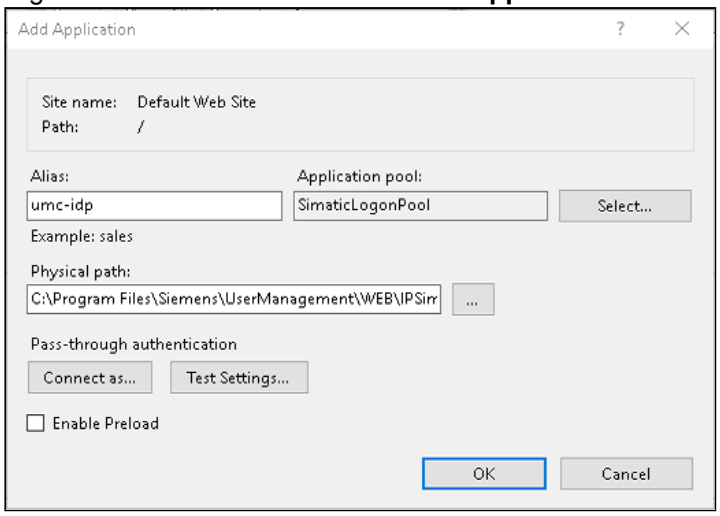
Procedure

1. Open **IIS Manager**.
2. In the tree on the left select the **Application Pools** node.
3. Right click on the node and select **Add Application Pool**: the following dialog box opens.

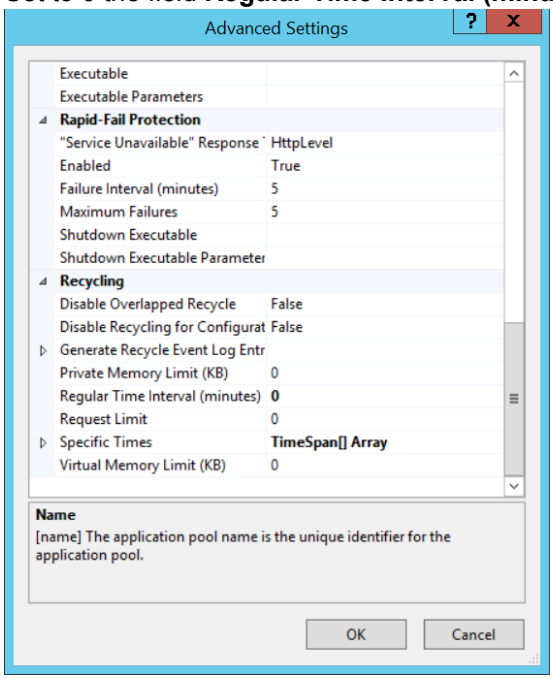


4. Insert the parameters as displayed in the previous image and click **OK**.
5. In the tree on the left select the **Default Web Site** node.

6. Right click on the node and select **Add Application**: the following dialog box opens.



7. Insert the parameters as displayed in the previous image and click **OK**. The path varies depending on where UMC is installed, for example C:\Program Files\Siemens\UserManagement\web\ipsimatic-logon.
8. On the applications pool page select the newly created application pool, and click **Manage Application** > **Advanced Settings**.
9. Set to 0 the field **Regular Time Interval (minutes)** and click **OK**.



4.2.3.2.2 Configuring Web UI and Service Layer API

Important:

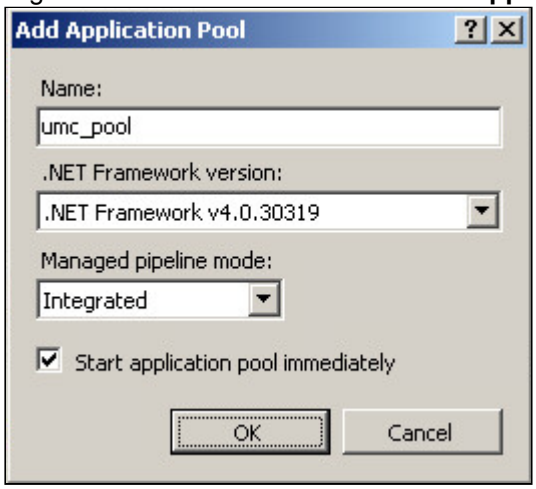
UMC contains two IIS 64 bit Native Modules: **um.ra.dll** and **um.slvm64.dll**

Prerequisites

- The prerequisites are installed.
- The machine is a 64 bit UM ring server or UM server.
- The Identity Provider (IdP) is correctly configured.

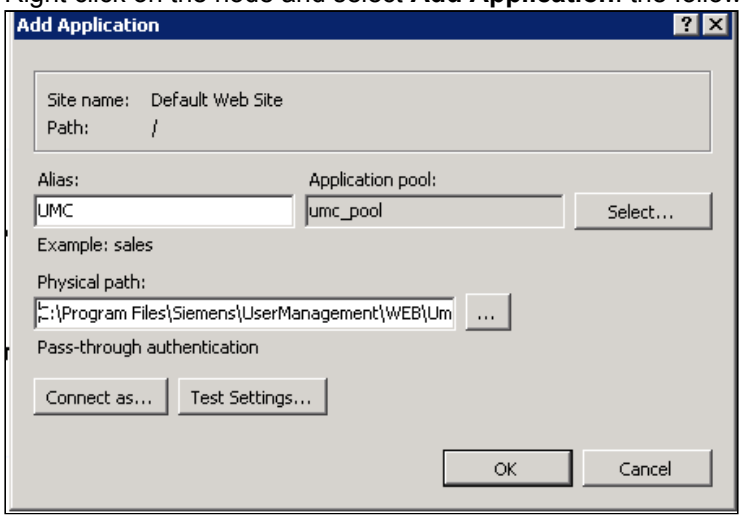
Procedure

1. Open the **Registry Editor**.
2. In the tree on the left go to the **HKLM\SOFTWARE\SIEMENS\User Management\WebUI\Settings** node.
3. Right click on the node, select **New > Key** and insert the **WebUI** key.
4. Right click on the **WebUI** node, select **New > Key** and insert the **Settings** key.
5. Right click on the **Settings** node, select **New > String Value**.
6. Double click on the newly inserted value and set as **Value name** the string **idpaddress** and as **Value data** the complete IdP URL, for example if the IdP is located on the local machine: https://FQDNmachinename/umc-sso or https://reverseproxyadress/umc-sso for complex scenarios like NLB scenarios. Depending on the IdP configuration the URL may start with **http** or **https**.
7. In the tree on the left go to the **HKLM\SOFTWARE\SIEMENS\User Management\CERT Library\Domain** node.
8. Right click on the **Domain** node, select **New > String Value** and insert the name **Web**.
9. Close the **Registry Editor**.
10. Open **IIS Manager**.
11. In the tree on the left select the **Application Pools** node.
12. Right click on the node and select **Add Application Pool**: the following dialog box opens.



13. Insert the parameters as displayed in the previous image and click **OK**.
14. In the tree on the left go to the **Default Web Site** node.

15. Right click on the node and select **Add Application**: the following dialog opens.



16. Insert the parameters as displayed in the previous image and click **OK**. The path of the application is, for example C:\Program Files\Siemens\UserManagement\WEB\Umc.
17. To verify that the application works properly, in the tree on the left go to the **UMC** node.
18. Right click on the node and select **Manage Application > Browse**. The Web UI application opens displaying the login page.

4.2.3.2.3 Configuring Remote Authentication

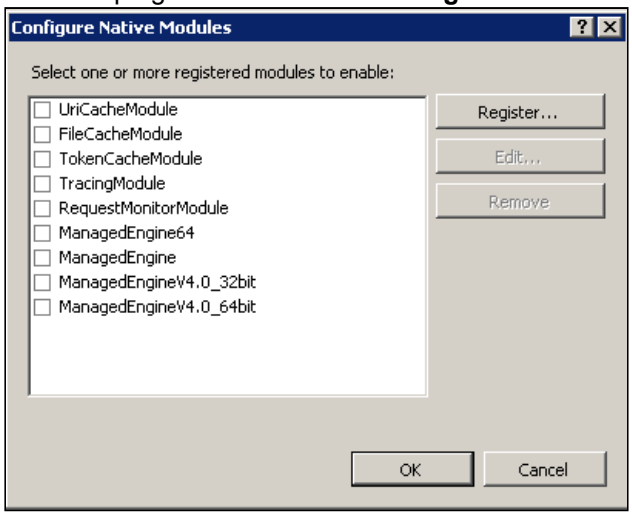
Prerequisites

- The general UMC prerequisites have been satisfied.
- The machine must be a 64 bit UM ring server or UM server.

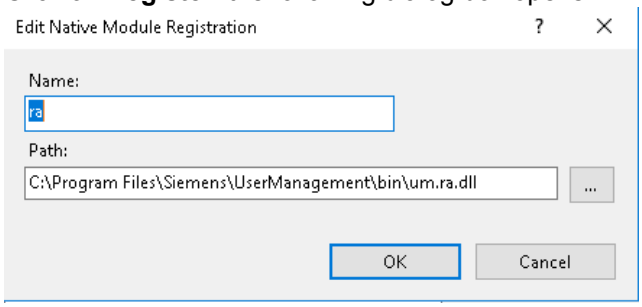
Procedure

1. Open **IIS Manager**.
2. In the tree on the left go to the root node.
3. On the right area of the screen double click on **Modules**.

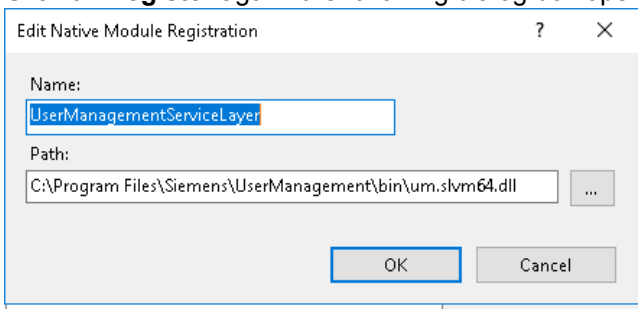
4. On the top right corner click on **Configure Native Modules**: the following dialog box opens.



5. Click on **Register**: the following dialog box opens.



6. Insert the parameters as displayed in the previous image and click **OK.**
7. Click on **Register** again: the following dialog box opens.



8. Insert the parameters as displayed in the previous image.
9. Once you have added the module make sure they are not selected and click **OK.**
10. Click **Modules** under the **UMC** application.
11. On the top right corner click on **Configure Native Modules.**
12. Select the **UserManagementServiceLayer module** checkbox then click **OK**.
13. Click **Modules** under the **ra** application, if ra is not present see note.
14. On the top right corner click on **Configure Native Modules**.
15. Select the **ra module** checkbox then click **OK.**

Note: If the ra application is not already present:

1. create a folder under the WEB (for example C:\Program Files\Siemens\UserManagement\WEB folder called *ra.*
2. add an application to the default site called "ra" specifying the path of the folder created in the previous step.

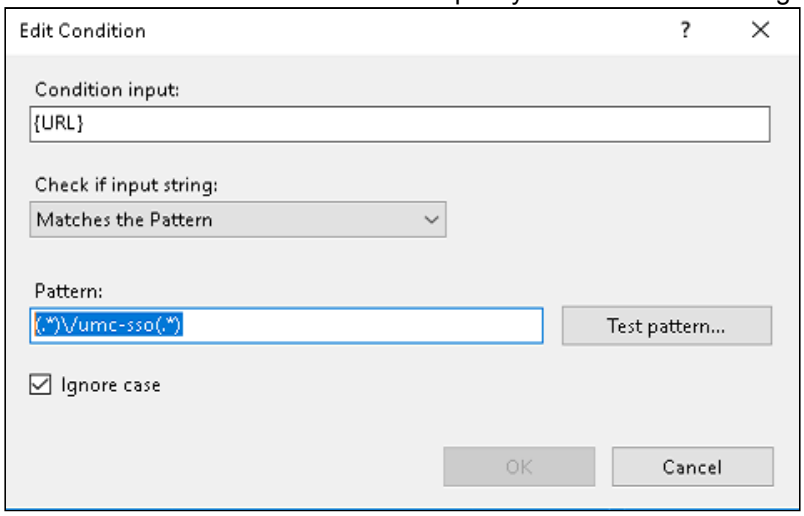
4.2.3.2.4 Configuring URL Rewrite Rules

You must manually configure the following URL rewrite rules in IIS.

Procedure

1. Go to **IIS Manager**.
2. In the **Connections** pane, select your server and then the top level site.
3. In the **Site** pane, double-click **URL rewrite.**
4. In the **Actions** pane, click **View Server Variables.**
5. Click **Add...** and specify *[http cookie].*
6. Go to the **Server** pane, double-click **Application Request Routing Cache**.
7. In the **Actions** pane, click **Server Proxy Settings** .
8. On the **Application Request Routing** page, select **Enable proxy**.
9. Check that the **Reverse rewrite host in response header** flag is false. It is recommended to set it as false in the case of a physics reverse proxy or in case you want to define a specific domain of the cookies.
10. In the **Actions** pane, click **Apply**.
11. In the **Server pane**, double-click **URL Rewrite**.
12. In the **Actions pane** on the right-hand side, click **Add rules**.
13. In the **Add Rules** dialog box, select **Blank Rule** and click **OK**.
14. In the **Edit inbound rule** pop-up, specify the following:
    – Name of the rule: UMC SSO Static
    – Pattern to use for matching the URL string: Matches the Pattern.
    – Using: Regular Expressions.
    – Pattern: (.*)
    – Specify the action type: Rewrite
    – Action properties Rewrite URL: The URL to rewrite, either http or https, local address 127.0.0.1, the port of reverse proxy, and /umc-sso for example: http://127.0.0.1:8443/umc-sso{C:2} (8443 is the standard port to be changed if idp listener port is customized).

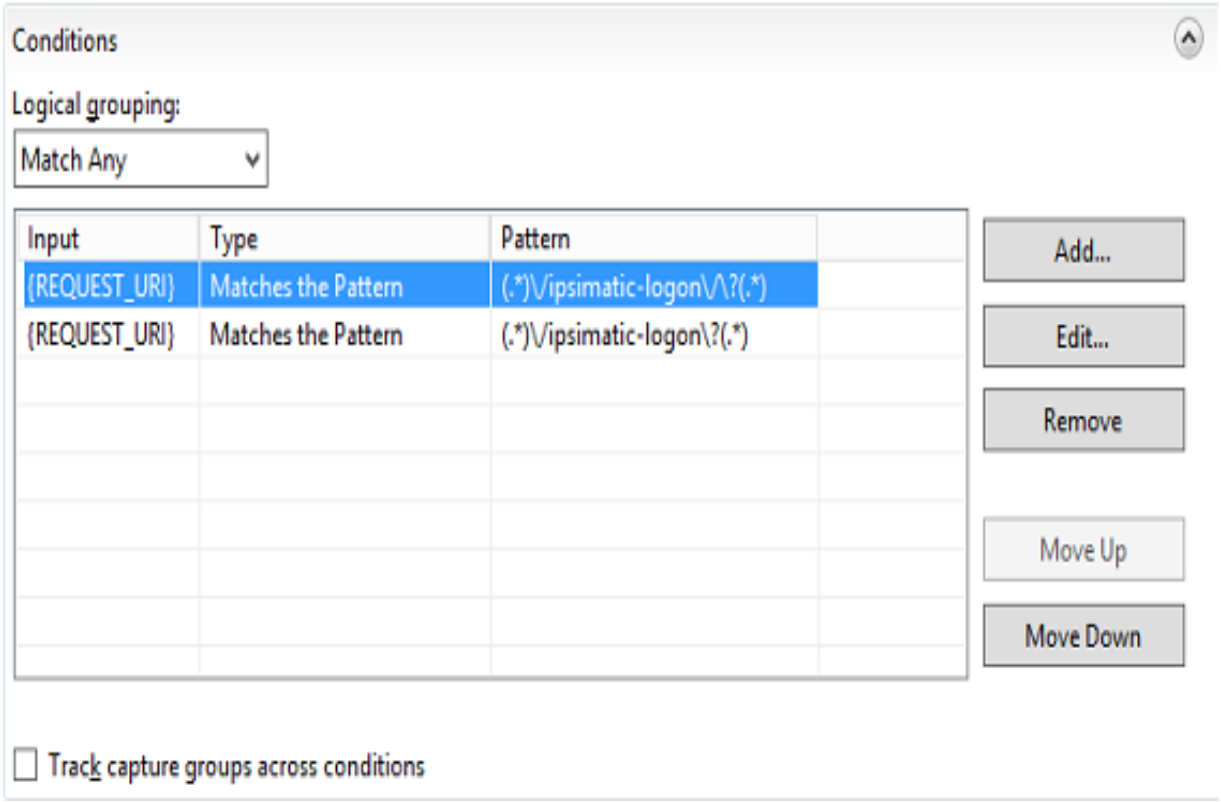
15. Click **Add** in the conditions area and specify the values in the image below.



16. Click **OK**.The pop-up is closed.
17. Click **Add** in the **Server Variables** area.
18. Select the **HTTP_COOKIE** server variable from the drop down list and insert {HTTP_COOKIE} ;ReverseProxyHost={SERVER_NAME};ReverseProxyPort={SERVER_PORT} in the value field.
19. Check the **Replace the existing value** checkbox, then click **OK**.The pop-up is closed.
20. In the action pane click **Apply**.

Procedure: ADD IDP Legacy rule

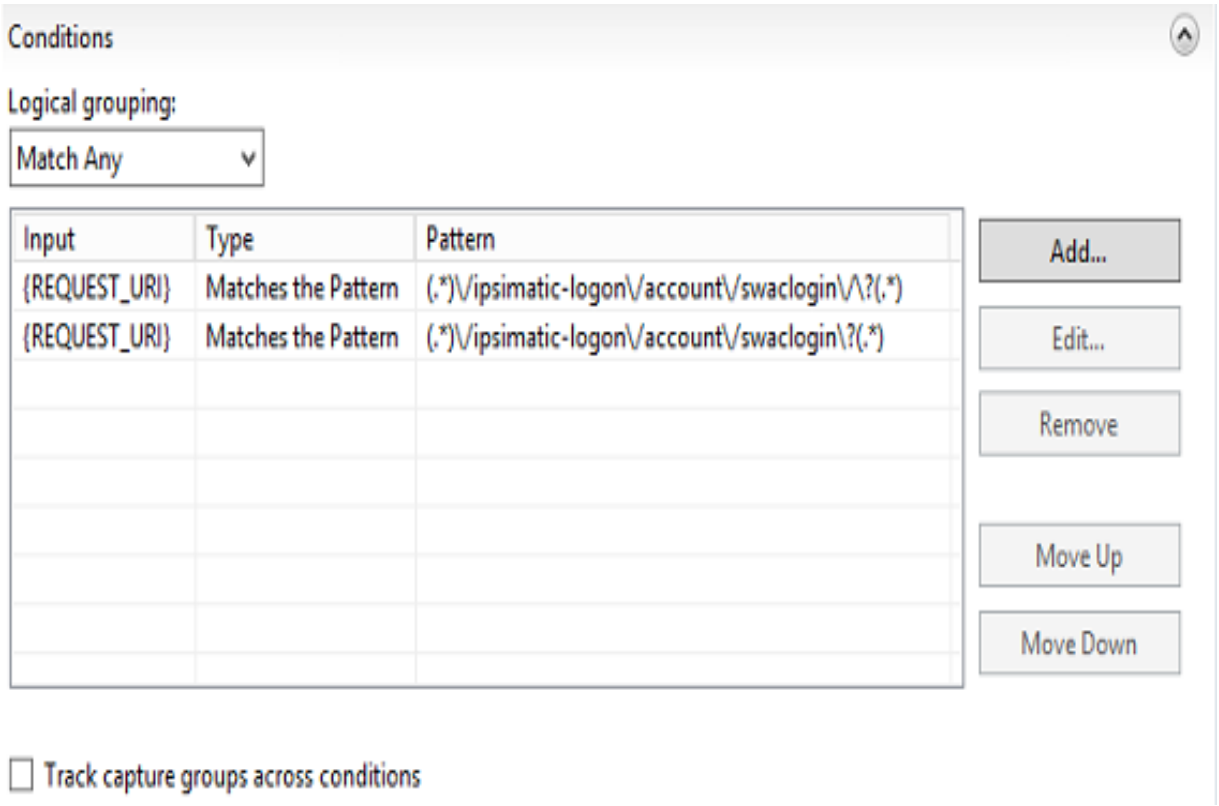
1. In the **Server pane**, double-click **URL Rewrite**.
2. In the **Actions pane** on the right-hand side, click **Add rules**.
3. In the **Add Rules** dialog box, select **Blank Rule** and click **OK**.
4. In the **Edit inbound rule** pop-up, specify the following:
   – Name of the rule: UMC IDP NODE SWITCH OFF
   – Pattern to use for matching the URL string: Matches the Pattern.
   – Using: Regular Expressions.
   – Pattern: (.*)
   – Specify the action type: Rewrite
   – Action properties Rewrite URL: The URL to rewrite, either http or https, local address 127. 0.0.1, the port of reverse proxy, and /umc-sso for example: http://127.0.0.1:8443/umc-sso {C:2} (8443 is the standard port to be changed if idp listener port is customized)
5. Click **Add** in the conditions area and specify the following conditions in the image below.



1. Click **OK**.The pop-up is closed.
2. Click **Add** in the **Server Variables** area.
3. Select the **HTTP_COOKIE** server variable from the drop down list and insert {HTTP_COOKIE} ;ReverseProxyHost={SERVER_NAME};ReverseProxyPort={SERVER_PORT} in the value field.
4. Check the **Replace the existing value** checkbox, then click **OK**.The pop-up is closed.
5. In the action pane click **Apply**.

Procedure: ADD SWAC Legacy rule

1. In the **Server pane**, double-click **URL Rewrite**.
2. In the **Actions pane** on the right-hand side, click **Add rules**.
3. In the **Add Rules** dialog box, select **Blank Rule** and click **OK**.
4. In the **Edit inbound rule** pop-up, specify the following:
   – Name of the rule: UMC IDP NODE SWITCH OFF (SWAC)
   – Pattern to use for matching the URL string: Matches the Pattern.
   – Using: Regular Expressions.
   – Pattern: (.*)
   – Specify the action type: Rewrite
   – Action properties Rewrite URL: The URL to rewrite, either http or https, local address 127. 0.0.1, the port of reverse proxy, and /umc-sso for example: http://127.0.0.1:8443/umc-sso{C:2} (8443 is the standard port to be changed if idp listener port is customized)
5. Click **Add** in the conditions area and specify the following conditions in the image below.



1. Click **OK**.The pop-up is closed.
2. Click **Add** in the **Server Variables** area.
3. Select the **HTTP_COOKIE** server variable from the drop down list and insert {HTTP_COOKIE} ;ReverseProxyHost={SERVER_NAME};ReverseProxyPort={SERVER_PORT} in the value field.
4. Check the **Replace the existing value** checkbox, then click **OK**.The pop-up is closed.
5. In the action pane click **Apply**.

4.2.3.2.5 Adding the ServiceLayer to Whitelist

In order for the WebUi to function correctly you must whitelist the URL of the Service Layer.

Note: The computer name, which is case sensitive, must be the same as that which is specified in the registry key.

Procedure

1. Whitelist the URL of the relying party using the **umconf.exe** program. Using either the *computername/UMC/slwapi/service* or *computername/UMC/slwapi/service* and *computername.userdnsdomain/UMC/slwapi/service.* See *UMCONF User Manual* for more details.

```
  "%bin%\umconf.exe" -c -w -d "http://%COMPUTERNAME%/UMC/slwapi/
service"
 or
  "%bin%\umconf.exe" -c -w -d "http://%COMPUTERNAME%/UMC/slwapi/
service"
  "%bin%\umconf.exe" -c -w -d "http://%COMPUTERNAME%.%USERDNSDOMAIN%/
UMC/slwapi/service"
```

2. Restart the **UMC Service**.

4.2.3.2.6 Configuring the Identity Provider Local Configuration

You must set the values of UMCDllFolderPath, reverseProxy and idpListenerPort in the Identity Provider local configuration file in order for the identity provider to work.

See Local Configuration File for more information on the configuration file.

Note: In order for modifications made to the Local configuration file to take effect you must restart the UMC Service.

4.2.3.3 Configuring Integrated Windows Authentication

The following procedures allows you to configure Integrated Windows Authentication of the Identity Provider (IdP) so that you can login on the Web UI using the current Windows session (see the *User Management Component Web User Interface Manual*). You have to:

1. Enable the Windows Authentication on IIS.
2. Install the Windows Authentication Role Service.

If you want to use Firefox, you must also perform some manual browser configurations.

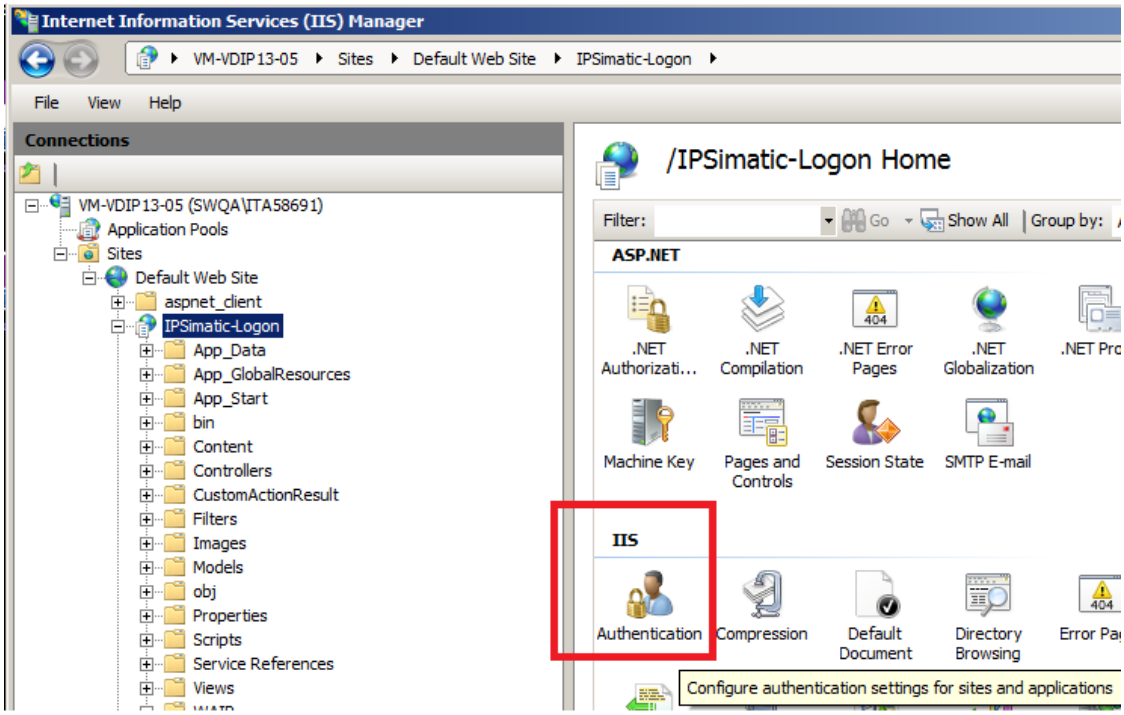
Prerequisites

- The Identity Provider prerequisites have been satisfied.
- The machine must be a 64 bit UM ring server or UM server.

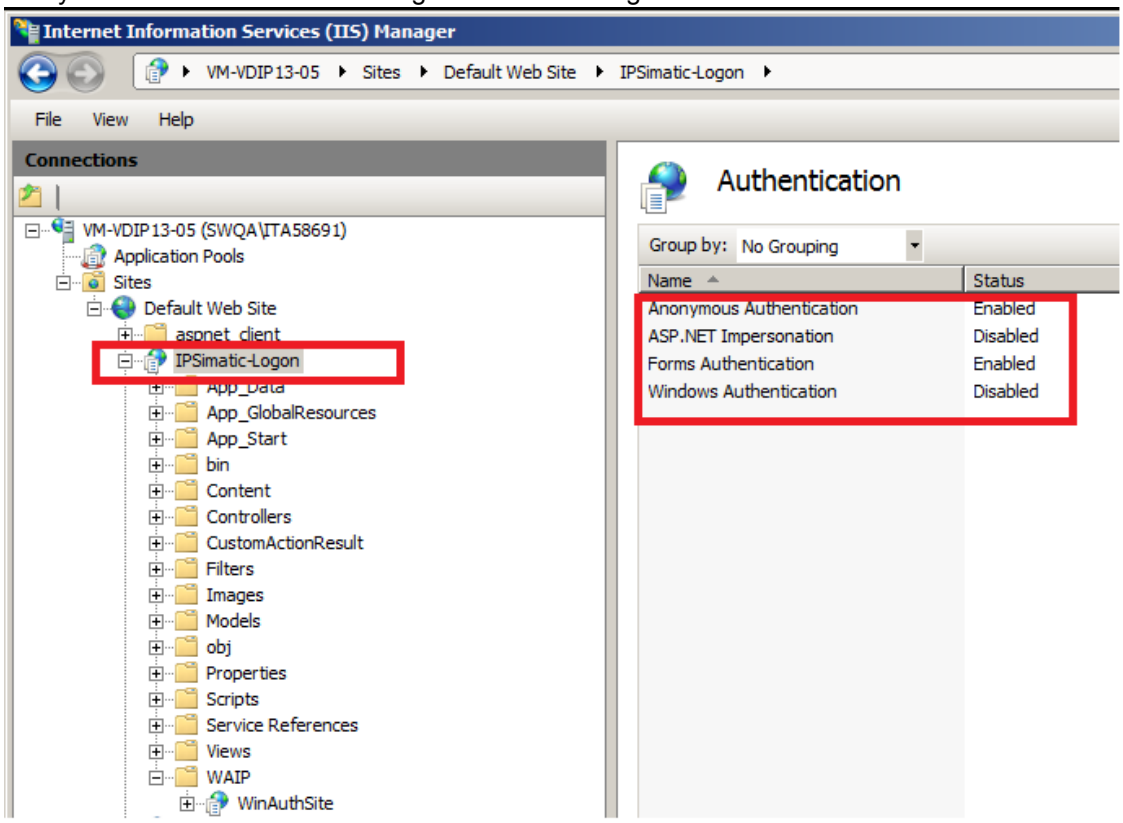
Enabling the Windows Authentication on IIS

1. Open **IIS Manager**.
2. In the tree on the left select the **IPSimatic-Logon** node.

3. Double click on **Authetication**.

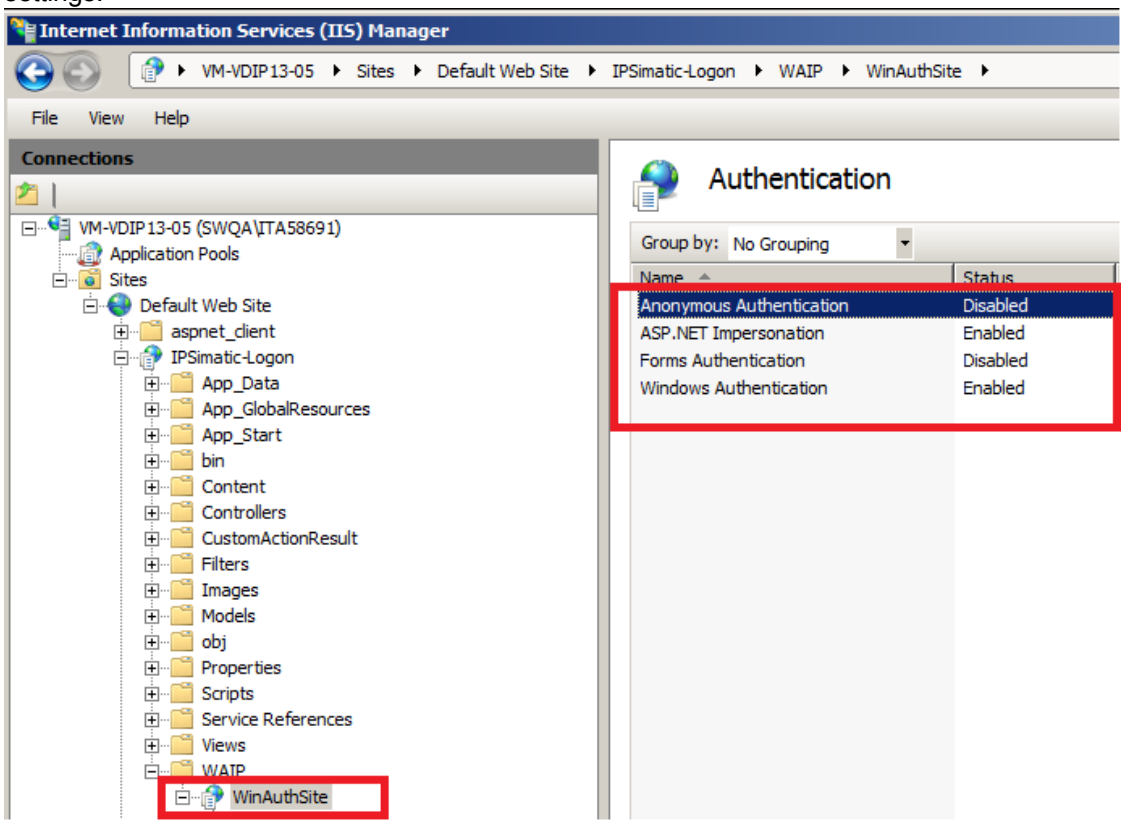


4. Verify that the authentication settings are the following:



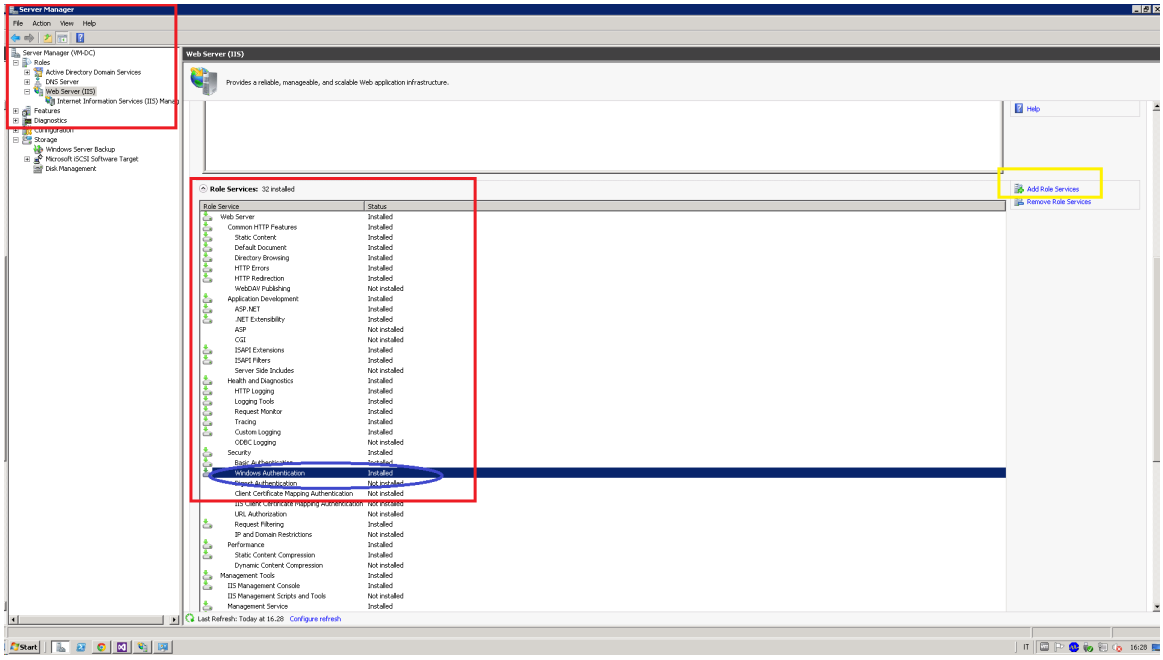
5. Right click on the **IPSimatic-Logon** node and select **Add Application** to add the **WinAuthSite** application, the path is for instance C:\Program Files\Siemens\UserManagement\web\ipsimatic-logon\WinAuthSite. Then click **OK**.

6. In the tree on the left select the **WinAuthSite** node and set the following authentication settings.



Installing the Windows Authentication Role Service

1. Open **Server Manager**.
2. In the tree on the left select the **Web Server (IIS)** node.
3. Install the **Windows Authentication** Role Service.



4.2.3.4 Configuring Firefox for Integrated Windows Authentication

The following procedure allows you to configure Firefox to work with the Integrated Windows Authentication of the Identity Provider (IdP) so that you can login on the Web UI using the current Windows session (see the *User Management Component Web User Interface Manual*). The string *<domain>* can be:

- equal to the computer name, if the machine on which the IdP is installed does not belong to an Active Directory domain (example: *myMachine*);
- equal to a FQDN (Fully Qualified Domain Name) such as *<computerName>.<domainName>.<extension>*, if the machine on which the IdP is installed belongs to an Active Directory domain (example: *myMachine.siemens.com*).

Prerequisites

The configurations of IIS for the Integrated Windows Authentication have been performed.

Procedure

1. Navigate to the URL **about:config** in Firefox. Click the **I'll be careful, I promise!** button.
2. In the **Search** dialog box, search for the preference **network.negotiate-auth.allow-non-fqdn**.
3. Double click on the property to set the value to **true** and close the window.

4.2.3.5 Identity Provider Configuration Management

The following configurations can be specified either locally, or centrally using the set configuration functionality in UMConf, see the *UMConf User Manual* for more information on managing the centralized configuration.

If the IdP has been configured via script these configurations are optional, however if it has been configured manually you must specify some values in the local configuration file.

Three configuration files are used by UMC Identity Provider:

- local configuration file: contains a set of data relative to the IdP instance, which must either be set by running the web configuration .bat or manually, this file can also be used to specify, any machine specific central configuration overrides.
- default configuration file: contains the default configuration for the IdP, which is installed by UMC and cannot be modified, these configurations are used when the configuration is not specified in either the local or central configuration file.
- central configuration file: contains the set of configurations which are to be applied to multiple servers and should be used to set any variations to the default file. Most of the settings present can be overridden by the local configuration file, if necessary.

Any local or central configuration modification is automatically loaded by the Identity Provider with a delay of less than 1 minute.

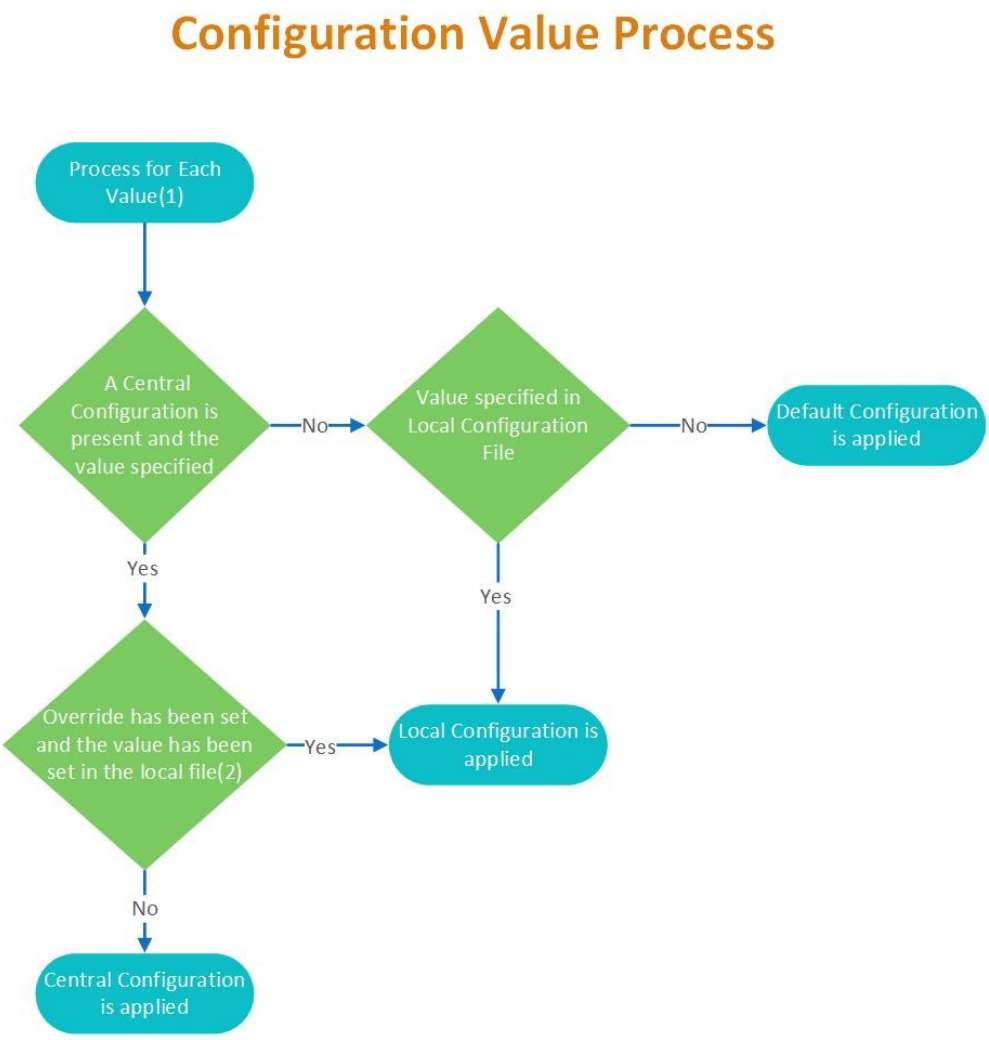


Diagram Notes

- **Note 1** Some values are only present in the Local Configuration file.
- **Note 2** Some Central Configurations values cannot be overidden by the Local Configuration File.

4.2.3.5.1 Local Configuration File

The local configuration file allows you to specify the settings which must only be applied to that specific machine. The file can be found in the subfolder WEB\umc-sso\config and is called configuration.json, for example: C:\Program Files\Siemens\UserManagement\WEB\umc-sso\config\configuration.json.

You can specify any of the attributes that are present in the default file in the local file. You can also set override to true to use the configuration specified locally instead of the central configuration.

Note:

- The values of **clusters**, **enableWhitelist**, **reverseproxy** and **reverseproxyPort** cannot be overridden by the local configuration if specified in the central configuration.
- To manually configure the IdP you must set the value of the fields: **UMCDllFolderPath, reverseProxy** and **idpListenerPort** .
- In order for modifications made to the local configuration file to take effect you must restart the UMC Service.

```
{
    "private": {
        "UMCDllFolderPath": "C:/Program Files/Siemens/UserManagement/bin",
        "useHttps": false,
        "httpsServerKey": "",
        "httpsServerCert": "",
        "configurationInterval": 60000,
    "idpListenerPort": 8443,
    "logs": {
            "winston": {
                "maxFiles": "2",
                "maxSize": "1000000",
                "traceLevel": "error"
            }
        }
    },
    "reverseProxy": "https://IDPTEST",
    "reverseProxyPort": "",
    "override" : false
}
```

Field	Description	Value
UMCDllFolderPath	The path of the user management installation, for example "C:/Program Files/Siemens/UserManagement/bin"	This value is propagated by the bat file and must only be modified in the case of manual IdP configuration.
useHttps	Specifies whether the HTTPS or HTTP protocol is to be used.	Set to false by default and is for future use only.
httpsServerKey	The public key of the https server.	For future use only.
httpsServerCert	The public cert of the https server.	For future use only.
configurationInterval	Specifies the poling interval on the central configuration and whitelisting. Internal use only.	Default 60000ms and must not be modified.

Field	Description	Value
idpListenerPort	Specifies the port number of the IDP node.js listener.	Default port number is 8443. To modify this option, just pass the custom port number to the **IdP_WebUI_configurator.bat** as third parameter. (Configuring UMC Web Components Via Script)
reverseProxy	The address of the reverse proxy.	
reverseProxyPort	The port of the reverse proxy.	Default 443.
override	Specifies if the value of the local configuration overwrites the central configuration.	Default is False. Possible values true or false.

The "logs" section is used to provide a unique point of configuration for the log systems. In the "Winston" section the configuration for the identity provider **node.js** server log is provided. It logs its messages in the file called **umc_sso_server.log**. The relative properties are described in the following table:

Winston

Field	Description	Value
maxFiles	Maximum number of files generated for this log	The default value is 2
maxSize	Maximum dimension of the files that are generated by the log	The value is defined in bytes. The default value is 1000000 bytes ≈ 1 Mbytes
traceLevel	Minimum severity level of messages to be recorded by the log	The value accepted can be in form of string or ID number: `{ error: 0, warn: 1, info: 2, verbose: 3, debug: 4, silly: 5 }` The logging level are described at the winston page: https://github.com/winstonjs/winston#logging-levels The default value is "error".

The following is an example of a configured local configuration file.

```
{
    "private": {
        "UMCDllFolderPath": "C:/Program Files/Siemens/UserManagement/bin",
        "useHttps": false,
        "httpsServerKey": "",
        "httpsServerCert": "",
        "configurationInterval": 5000,
    "idpListenerPort" : 8443,
    "logs": {
            "winston": {
                "maxFiles": "2",
                "maxSize": "1000000",
                "traceLevel": "error"
            }
        }
    },
  "reverseProxy": "https://mymachine",
    "reverseProxyPort": "",
  "languages": {
      "de-DE": {
        "id": "de-DE",
        "name": "Deutsch"
      },
      "en-US": {
        "id": "en-US",
        "name": "English US"
      }
      },
  "authenticationOptions": {
      "autoLogin": "",
      "disableCredentialsLogin": false,
      "enableFlexAuth": true,
      "enableIWA": false,
      "enablePKI": true
    },
    "override": true
}
```

4.2.3.5.2 Default Configuration File

The default file contains the default configurations which are used if the configurations are not specified in the central or local files. A copy of this file can created via the UMConf **getdefaultconfig** command, see *UMConf User Manual* for more information.

Default file

```
  {
  "configdata": {
    "authenticationOptions": {
```

```
      "authenticationLevelCredentialsLogin": "strong",
      "authenticationLevelWindowsLogin": "strong",
      "autoLogin": "",
      "disableCredentialsLogin": false,
      "enable2FactorAuth": false,
      "enableFlexAuth": false,
      "enableIWA": true,
      "enablePKI": false
    },
    "clusters": 1,
    "cookieFlags": {
      "httpOnly": true,
      "secure": true,
      "domain": ""
    },
    "cookiePath": "/",
    "disclaimerContent": {
      "de-DE": "Sie sind in eine geschützte Umgebung eingetreten. Um die
Umgebung zu verlassen, müssen Sie sich abmelden. Das Schließen des Browsers
ist nicht ausreichend, um zu gewährleisten, dass Sie die Umgebung verlassen
haben.\n<br/><br/>\n<b>Sicherheitsinformationen</b>\n<br/>\nUm Anlagen,
Systeme, Computer und Netzwerke vor Internetbedrohungen zu schützen, ist es
nötig, ein holistisches Konzept für die industrielle Sicherheit auf dem
neuesten Stand zu implementieren und kontinuierlich aufrechtzuerhalten.
Produkte und Lösungen von Siemens stellen nur ein Element eines solchen
Konzepts dar. Weitere Informationen über die industrielle Sicherheit finden
Sie unter http://www.siemens.com/industrialsecurity.",
      "en-US": "You have entered a protected environment. To exit, you must
log out: closing the browser is not sufficient to guarantee that you have
exited the environment.\n<br/><br/>\n<b>Security information</b>\n<br/>\nIn
order to protect plants, systems, machines and networks against cyber
threats, it is necessary to implement – and continuously maintain – a
holistic, state-of-the-art industrial security concept. Siemens products and
solutions only form one element of such a concept. For more information
about industrial security, please visit http://www.siemens.com/
industrialsecurity.",
      "es-ES": "Ha entrado en un entorno protegido. Para salir es necesario
cerrar sesión, no es suficiente cerrar el explorador para garantizar que se
ha salido del entorno.\n<br/><br/>\n<b>Información de Seguridad</b>\n<br/>\
nPara proteger plantas, sistemas, máquinas y redes contra ciberamenazas, es
necesario implementar -y mantener constantemente- un concepto de seguridad
industrial holística de última generación. Los productos y soluciones
Siemens constituyen solamente un elemento de dicho concepto. Para obtener
más información acerca de la seguridad industrial, visite: http://www.
siemens.com/industrialsecurity.",
      "fr-FR": "Vous êtes dans un environnement protégé. Pour sortir, vous
devez vous déconnecter: la fermeture de l’explorateur n’est pas suffisante
pour garantir votre sortie de cet environnement.\n<br/><br/>\n<b>
Informations sur la sécurité</b>\n<br/>\nPour protéger des plants, des
systèmes, des machines et des réseaux contre des menaces cyber, il est
nécessaire d’implémenter (et maintenir de manière permanente) une
optimisation globale du concept de sécurité industrielle. Les produits et
```

```
solutions Siemens  représentent seulement un élément de ce concept. Pour de
plus amples informations sur la sécurité industrielle, voir http://www.
siemens.com/industrialsecurity.",
      "it-IT": "Vi trovate in un ambiente protetto. Per uscire è necessario
disconnettersi: la chiusura del browser non è sufficiente a garantire
l'uscita dall'ambiente.\n<br/><br/>\n<b>Informazioni sulla sicurezza</b>\n
<br/>\nPer proteggere impianti, sistemi, macchine e reti dalla minaccia
cyber, è necessario implementare - e mantenere continuativamente - un
concetto di sicurezza industriale olistico e all'avanguardia. I prodotti e
le soluzioni Siemens rappresentano soltanto un elemento di tale concetto.
Per maggiori informazioni sulla sicurezza industriale, visitare il sito http:
//www.siemens.com/industrialsecurity.",
      "zh-CN": "您已经进入了一个受保护的环境。如要退出，您必须注销：关闭浏览器不足以保证
已退出环境。\n<br/><br/>\n<b>安全信息</b>\n<br/>\n为了保护工厂、系统、机器和网络免受网
络威胁，有必要实施—并持续维护—一个全面、最先进的工业安全概念。西门子产品和解决方案只是这种
概念的一个要素。有关工业安全的更多信息，请访问 http://www.siemens.com/
industrialsecurity。"
    },
    "disclaimerEnabled": false,
    "enableWhitelist": false,
    "idpUI": "/umc-idp/idpauthsite",
    "languages": {
      "de-DE": {
        "id": "de-DE",
        "name": "Deutsch"
      },
      "en-US": {
        "id": "en-US",
        "name": "English US"
      },
      "es-ES": {
        "id": "es-ES",
        "name": "Español"
      },
      "fr-FR": {
        "id": "fr-FR",
        "name": "Français"
      },
      "it-IT": {
        "id": "it-IT",
        "name": "Italiano"
      },
      "zh-CN": {
        "id": "zh-CN",
        "name": "中文"
      }
    },
    "maxCachedSessionsPerUser": 100,
    "reverseProxy": null,
    "reverseProxyPort": null,
    "sessionAge": 1800000,
    "ssoService": "/umc-sso"
```

```
  },
  "label": "$default$",
  "version": 0
}
```

Field	Description	Value
disclaimerContent	Contains the text to be displayed for each language.	The disclaimer text for each language. It consists in two letter language code and culture code, for example "de-DE": example text, "en-US": example.
disclaimerEnabled	Enables the visualization of disclaimers at login.	If set to true the disclaimer is visualized, if set to false (default) the disclaimer is not disabled.
enableWhitelist	Enables UMC whitelisting.	If set to true (default) whitelisting is enabled, if set to false whitelisting is disabled.
sessionAge	Specifies the amount of time that passes before the sessions expires.	It is set to 1800000 ms by default.
reverseProxy	The address of the reverse proxy.	If this value is set on the central configuration the local value is ignored even if the override is set to true.
reverseProxyPort	The port of the reverse proxy.	443 by default. If this value is set on the central configuration, the local value is ignored even if override is set to true.
ssoService	The endpoint of the single sign on protocol.	/umc-sso
idpUI	The address of the IDP UI.	Set to a default value " /ipsimatic-logon/idpauthsite"
maxCachedSessionsPerUser	The number of sessions which are logged in the cache for each users. When the number of sessions cached exceed the limit the oldest entry is removed.	Set to default value 100. value range from 10-1000.
cookiePath	The path of the domain in which the cookie is valid. This value must be set in the case of reverse proxy.	Default value "/umc-sso".

Field	Description	Value
clusters	Defines how many node process must be launched.	1 min and the max value should reflect the total number of processor cores.
cookieFlags	The security level of the session cookies.	• httponly: Internal use only. • secure: Internal use only. • domain: the validity domain of the cookies
languages	The language which can be selected on the login page. Internal use only.	
Authentication options	(see table below)	
Version	Internal use only.	
Label	Internal use only.	

Authentication options

Field	Description	Value
authenticationLevelCredentialsLogin	Specifies the security level of credential based authentication.	• Weak, • Medium • Strong (by default)
authenticationLevelWindowsLogin	Specifies the security level of Windows authentication.	• Weak, • Medium • Strong (by default)
enableIWA	Enables Windows authentication on IdP.	True or false (default).
enablePKI	Enables Smart Card authentication.	True or false (default).
enableFlexAuth	Enables Flexible authentication.	True or false (default).
enable2FactorAuth	Enables two factor authentication.	True or false (default).

Field	Description	Value
disableCredentialsLogin	If set to true the credentials fields are hidden on the IDP page so that only integrated authentication like Teamcenter, Windows or smart card authentication can be used.	True or false (default).
autoLogin	Enables Autologin.	• Windows authentication: "iwa" • Smart Card authentication: "pki" • Desktop <desktop|<plugin_id> • Web <web|<plugin_id> • Flex authentication <flexauth:<pluginname> Multiple authentication methods can be used by dividing each method with "||". "<desktop|<plugin_id>||<desktop|<plugin_id>"

4.2.3.5.3 Central Configuration File

The central configuration file contains the configurations that can be applied to multiple machines, any settings which are set in the central file are used by all the machines in the scenario, unless override is set to true in the local file.

You can use a UMConf command to retrieve the current central configuration and set a central configuration. The values which can be set in the central configuration are detailed in the description of the fields of the default configuration file.

A centralized configuration is set via UMConf or when certain configuration are performed via Web UI, for example configuring a disclaimer or authentication options.

The following json is an example of central configuration with some configurations which can be set centrally.

```
{
    "conf": [
        {
            "configdata": {
                "sessionAge": 600000,
                "reverseProxy": "https://IDPTEST3",
                "reverseProxyPort": "",
```

```
                "ssoService": "/umc-sso",
                "idpUI": "/umc-idp/idpauthsite",
                "cookiePath": "/",
                "clusters": 1,
                "cookieFlags": {
                    "httpOnly": true,
                    "secure": true,
              "domain" : "umdom1.net"
                },
                "authenticationOptions":{
                    "enableIWA":true,
                    "enablePKI":false,
                    "enableFlexAuth":true,
            "enable2FactorAuth":false,
                    "disableCredentialsLogin":false,
                    "autoLogin":""
                }
              },
              "label": "$default$",
              "version": 2
          }
      ]
}
```

4.2.3.6 How to Configure Smart Card (PKI) Authentication

The following configuration steps must be performed to enable authentication via smart card.

The operations can be performed in any order.

Workflow

- Configure Smart Card Authentication Infrastructure.
- Configure Smart Card Web Application (not needed if you configure UMC via script).
- Enable Login via Smart Card Authentication either locally on centrally.
- Set Account Policy for Smart Card Authentication.

4.2.3.6.1 Configuring Smart Card Authentication Infrastructure

Server side

The Smart Card Authentication can only be configured on machines where the Identity Provider has been configured. IIS authentication via certificate must be correctly configured in order for it to function.

Important:

The following IIS configuration recommendations must be taken into account:

- checks on the revocation list must be supported;
- Client Authentication Issuer certificate in the Certificate Manager has to be installed;
- the Trusted Root Certification Authorities store has to contain only self signed certificates;
- the use of the Client Authentication Issuer on 443 port or on the IdP port has to be enabled.

Client side

The following steps are needed to configure client side Smart Card authentication:

- smart card drivers must be installed on each client machine;
- if you use Firefox, the additional configuration for Security Devices must be performed.

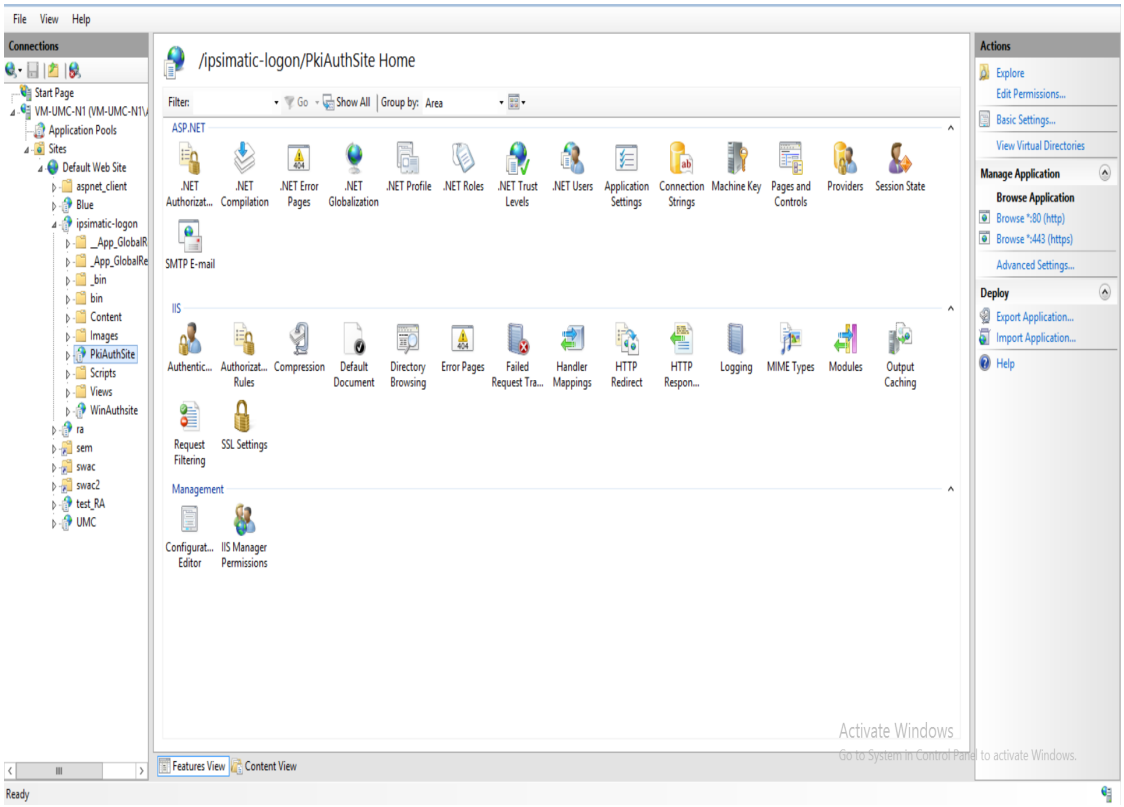
4.2.3.6.2 Configuring Smart Card Web Application

This procedure is not needed if you have used the **IdP_WebUI_configurator.bat** script to configure UMC.

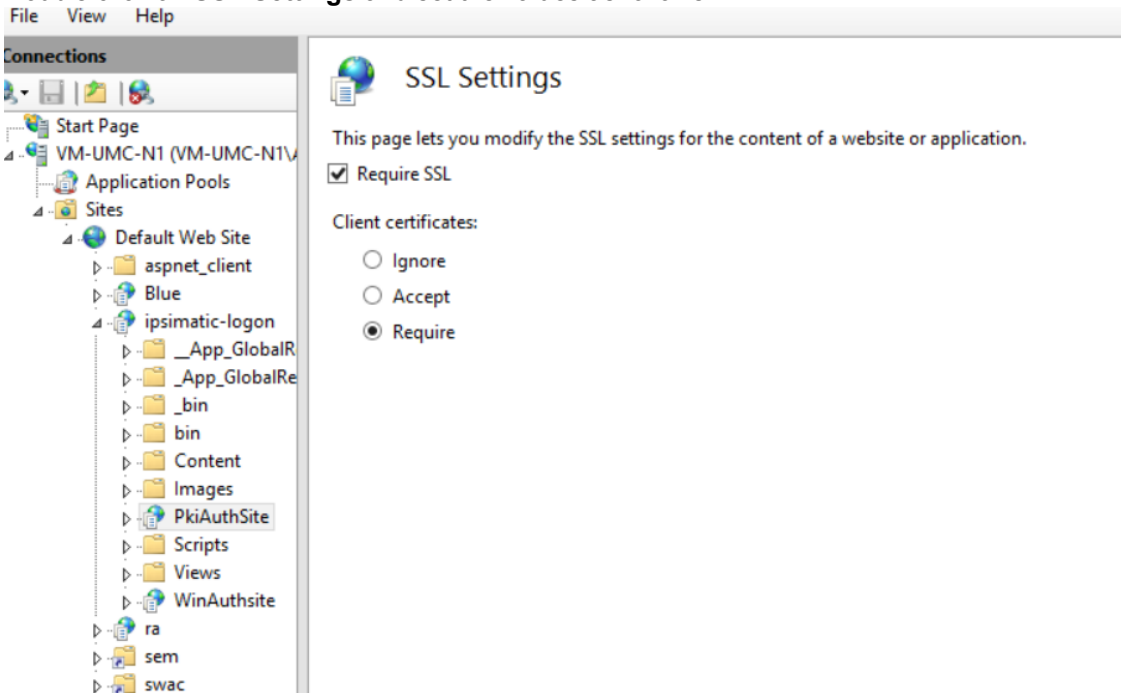
Procedure

1. Open **IIS Manager**.
2. Right click on the **IPSimatic-Logon** node and select **Add Application** to add the **PkiAuthSite** application, the path is for instance C:\Program Files\Siemens\UserManagement\web\ipsimatic-logon\PkiAuthSite. Then click **OK**.

3. In the tree on the left select the **PkiAuthSite** node.



4. Double click on **SSL Settings** and set the values as follows.



5. To verify that the smart card authentication application is correctly configured, open a browser instance.
6. Insert a smart card in the smart card reader.
7. Open the page at the following address: https://<address>/umc-idp/pkiauthsite/info.aspx; a json file opens displaying smart card information.

In case the json file is not correctly displayed, we suggest that you enable on IIS the detailed error responses and carefully verify smart card authentication infrastructure configuration.

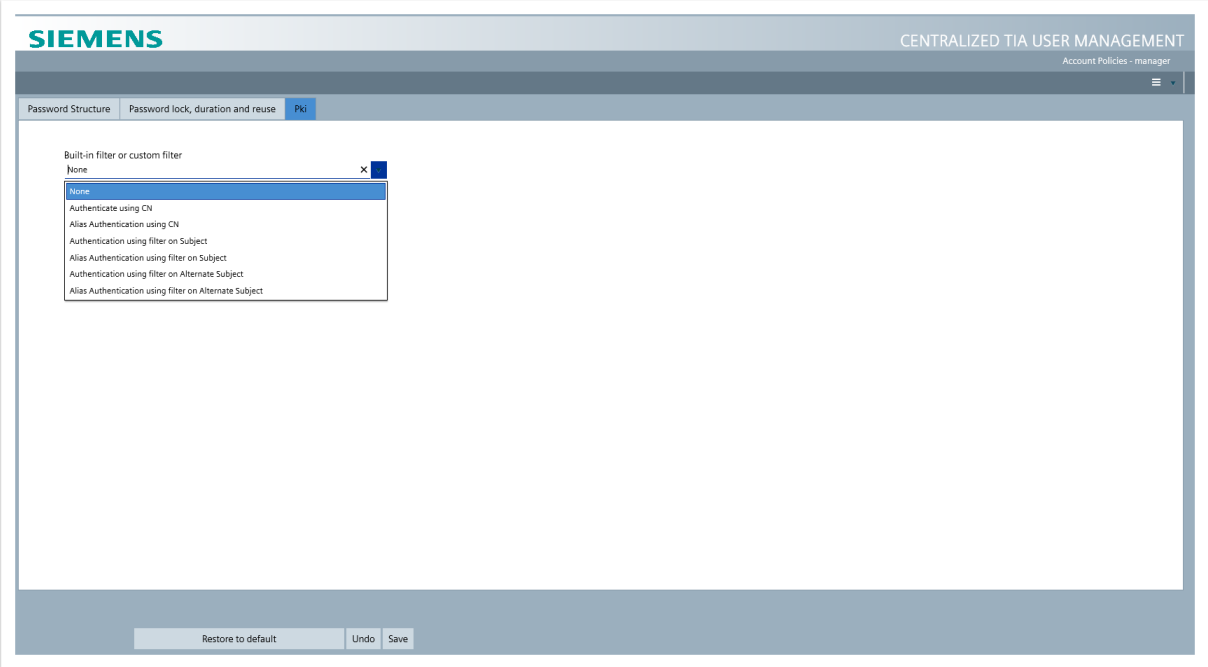
4.2.3.6.3 Setting Account Policy for Smart Card Authentication

The smart card authentication mechanism is based on a matching between the user data stored on the smart card and the data stored in UMC.

Procedure

1. To configure the data matching, go to the UMC Web UI account policy page with the proper access rights.
2. Define the field to be retrieved from the smart card to identify the user in UMC.
3. Select either of the following authentication options:
   – **simple authentication (no alias)**: in this case the selected field, CN (Common Name), Subject, Alternate Subject, is compared with the UMC user name; if they correspond the user is authenticated.
   – **alias authentication**: in this case you have to define an alias for a user in the user detail dialog; the value stored in the field is compared with the UMC alias, if they correspond the user is authenticated.

For more information see the account policy documentation in the *User Management Component Web User Interface Manual*.



Alternative Operations

- You can also define an alias using the dedicated UMX command. See *UMX User Manual* for more details.
- For AD users the alias can be set in the importing phase, for more information see Additional Provisioning Configuration.

Example

Consider the following user with the following values:

User name = John_Brown

Alias = john.brown@mycompany.com

For instance, the following two cases can occur depending on the account policy selection:

- **Authenticate using CN**: if value stored in the CN in the smart card is John_Brown (UMC user name value), the user is authenticated; otherwise authentication fails;
- **Alias Authentication using CN:** if value stored in the CN in the smart card is john.brown@mycompany.com (UMC alias value), the user is authenticated; otherwise authentication fails.

4.2.3.7 Enabling HTTPS in a HTTP UMC Scenario

Depending on the configurations you have made on the UMC Web components, you have to perform one of the following alternative procedures:

- Configure UMC Web components via script (**IdP_WebUI_configurator.bat**).
- Configure UMC Web components manually or customize them.

Prerequisites

A UMC Web component is installed and configured on your machine and IIS is **not** configured for HTTPS.

Configuring UMC Web components via script (no customization)

1. Configure IIS for the HTTPS protocol.
2. Launch the script **REMOVE_IdP_WebUI_configurator.bat**. The batch file can be found in C:\Program Files\SIEMENS\UserManagement\BIN, if the default installation folder is selected. Note that the script works on a 64 bit machine only.
3. Launch the configuration script **IdP_WebUI_configurator.bat** to configure UMC Web Components.

Configuring UMC Web components manually or customizing their configuration

1. Configure IIS for the HTTPS protocol.
2. If you have performed any modification to the IIS configuration after launching the configuration script **IdP_WebUI_configurator.bat** or you have configured UMC not using this script**,** you have to enable HTTP protocol manually .

4.2.3.8 How to Configure Two Factor Authentication by time-based one-time password

The following configuration steps must be performed to enable two factor authentication by TOTP (time-based one-time password). It can be used to increase the security level of an authentication method that would otherwise be standard or weak.

UMC two factor authentication consists in an initial authentication method: Windows or Password authentication, and token (TOTP), which is encrypted using the user's secret key, in order to elevate the user's security level to strong.

Two Factor Authentication allows the user to log in with limited access after it has been enabled, so that the user can generate the initial Secret Key.

Note: Two factor authentication by TOTP cannot be enabled for the built-in Administrator user from the Web UI. It can only be enabled via UMX commands.

Workflow

- Enabling Two Factor Authentication
- Using Two Factor Authentication

4.2.3.8.1 Enabling Two Factor Authentication

The two factor authentication by TOTP can be enabled from the WEB UI or UMX and UMConf.

Note: The two factor authentication cannot be enabled for the built-in Administrator user from the Web UI, it can only be Enabled via UMX commands. In the case of the built-in Administrator you must generate the first secret via the umx resettotp the command.

Workflow

- SADS has been enabled in Account Policies via WEB UI or UMX.
- Enable the two factor authentication in authentication options via WEB UI or centralized configuration management.
- Two Factor authentication has enabled for the user in their account policies via Web or encryption has been enabled for the user from UMX.

Enabling SADS from the Web UI

1. Login to UMC Web with user who has UM admin role.
2. From the menu on the upper right-hand corner of **UMC Home page**, select **Account Policies**. The **Account Policies** page is displayed.
3. In the **Advanced** tab, select the **Enable secure application data support for users and groups** check box to enable the SADS functionality. SADS capabilities at application level can

be enabled via **umx** or Web UI by modifying an account policy. For more details, see *UMX User Manual*.

4. Click **Save**.

Enabling Two Factor Authentication as an Authentication method

1. Login to UMC Web with user who has UM admin role.
2. Select the **Authentication Options** tab.
3. Select the enable two factor authentication check box.
4. Click **Save all changes to configuration settings**.

Enabling Two Factor Authentication for a user

1. From the **Users** page, select a row and click **Details** in the upper left-hand corner of the grid.
2. Select the **Account Policies** tab.
3. Select the **Enable 2FA** checkbox.
4. Click **Save**.

4.2.3.8.2 Using Two Factor Authentication

Two factor authentication by TOTP allows you to increase the security level of a login which has been performed using a method that would otherwise be weak or medium.

When 2FA is enabled the user is prompted to provide a token after logging in the second time, the first time the user logs in they are granted access in order to retrieve the secret key.

Workflow

1. Log in using an authentication methods which is either weak or standard.
2. The second time you login the you will be asked for a TOTP (time-based one-time password).
3. Generate a TOTP (time-based one-time password) using the previously retrieved secret key.
4. Insert the password and click **Sign in.**

Generating and Resetting Secret Keys

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

Prerequisites

- SADS has been enabled in Account Policies via Web (see How to Manage Account Policies in the *UMC Web UI User Manual*) or UMX.
- The Two Factor Authentication has been enabled as an authentication method via Web (see Configuring Authentications Options in the *UMC Web UI User Manual*) or UMConf centralized configuration management.
- The Two Factor authentication has enabled for the user in their account policies via Web (see Editing User Account Policies in the *UMC Web UI User Manual*) or Encryption has been enabled for the user from UMX.

Procedure

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

4.2.4 Installing and Configuring UMC Station Client

CAUTION:

No checks are currently performed at setup level on the UMC station client installation. Over-installation of the UMC station client causes serious system malfunction. In particular you must not install the UMC station client on a machine where you have already installed full UMC.

UMC Station Client can be configured:

- via script.

Prerequisites

- The Windows user logged in must have administrative rights.
- Full UMC installation or UMC station client has been executed on your machine. During the installation you have simply to proceed with the wizard.
- The UMC Web UI has to be properly configured for the UMC system in HTTPS, see Configuring Web UI. HTTPS is mandatory, therefore a valid SSL certificate must have been acquired from a Certification Authority or a self-signed SSL certificate has been created.

Configuring UMC Station Client via Script

1. Launch the **regx.ps1** script located in the subdirectory \BIN of the 32 bit installation folder.
2. The script requires the following parameters:
   – **UMC Server name** (only a ring master);
   – **user** (who must own the **UM_REGCLIENT** function right);
   – **password**.
3. The script additionally supports the following optional parameters:
   – **workstationAlias** (alias used in registration phase, instead of hostname; alias cannot contain special characters)
   – **force** (force registration for an alias already registered)
   – **update** (update registration for a client already registered)

Result

The system registers the machine as a UMC station client machine that provides a claim in which certified logon station details are included.

4.2.5 Configuring SLRA support

UMC provides Simatic Logon Remote Authentication support.

Prerequisites

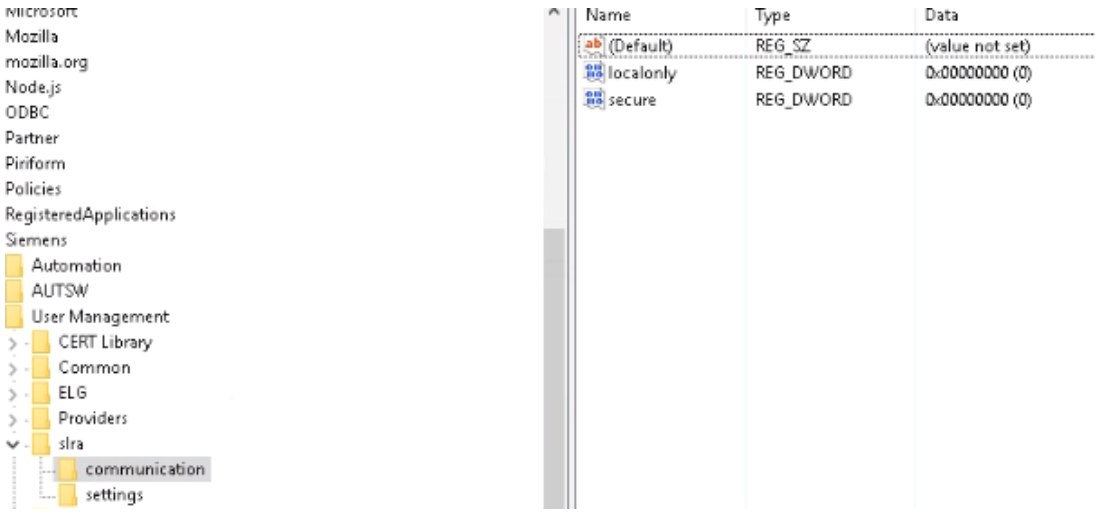
- The machine is configured as a UMC ring server or server.

Procedure

1. Open the Registry Editor, navigate to **HKLM\SOFTWARE\SIEMENS\User Management.**
2. Right-click on the node, select **New > Key** and insert the **slra** key.
3. Right-click on the **slra** node, select **New > Key** and insert the **settings** key .
4. Right-click on the **settings** node, select **New > DWORD Value.**

5. Double-click on the newly inserted value and set as Value name the string **enabled** and as **Value data 1 to enable SLRA.**

6. Right-click on the **slra** node, select **New > Key** and insert the **communication** key .
7. Right-click on the **communication** node, select **New > DWORD Value**
8. Double-click on the newly inserted value and set as Value name the string **secure** and as **Value data 1 to enable secure communication via TLS** or **0 if TLS is not required**
9. Right-click on the **communication** node, select **New > DWORD Value**
10. Double-click on the newly inserted value and set as Value name the string **localonly** and as **Value data 0 for enabling remote communication**, **1 if no remote communication must be allowed**.



Note: Certificates

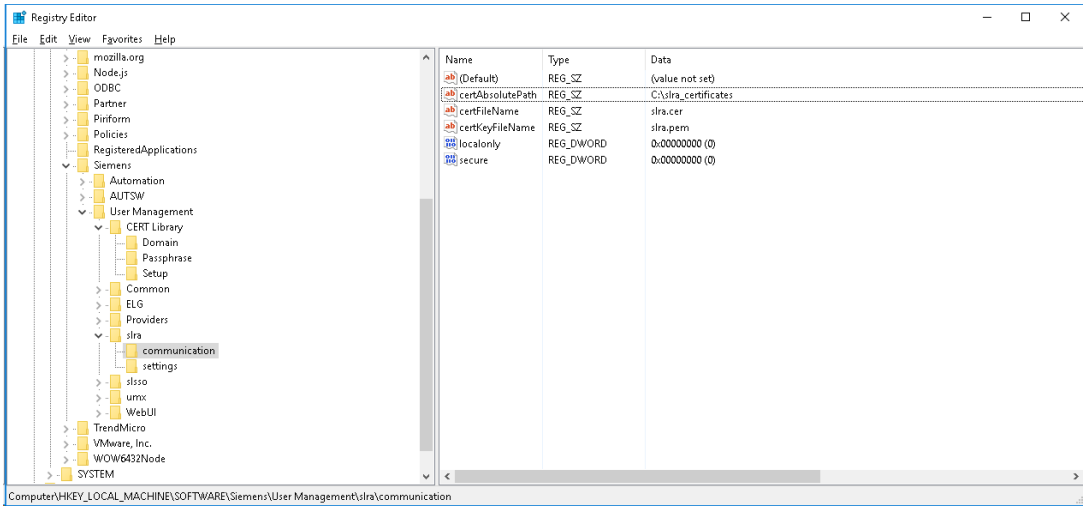
In case TLS is required, create the certificates ad save them in the default certificate folder **CERT/SLRAUTH** under C:\ProgramData\Siemens\UserManagement.

The default certificate path folder **CERT/SLRAUTH** inherits the access rights of parent **CERT** folder. The folder permissions must be modified if required.

Certificates path and names

Additionally, you can override the folder path and the certificate name using the following settings:

1. Right-click on the **communication** node, select **New > STRING Value**.
2. Double-click on the newly inserted value and set as Value name the string **certAbsolutePath** and as **Value the path where certificates are stored**.
3. Right-click on the **communication** node, select **New > STRING Value**.
4. Double-click on the newly inserted value and set as Value name the string **certFileName** and as **Value the certificate file name**.
5. Right-click on the **communication** node, select **New > STRING Value**.
6. Double-click on the newly inserted value and set as Value name the string **certKeyFileName** and as **Value the certificate file name**.



4.2.6 Configuring Desktop Single Sign On

Prerequisites

- The machine is configured as a UMC ring server or server .
- UMC Web components are configured on the machine with HTTPS.

Procedure

To enable Desktop Single Sign On:

- Use the UMCONF utility , s ee *UMCONF User Manual* for more details.

5 Configuring the Identity Provider in a High Availability/Reliability Scenario

The high availability and reliability of the Identity Provider (IdP) is supported thanks to the Network Load Balancing (NLB) technology. Network Load Balancing is a clustering technology that enhances the scalability and availability of TCP/IP-based services such as Web applications (i.e. UMC Identity Provider). To scale performance, the NLB distributes the incoming IP traffic over several web servers by using a virtual IP address, and a reverse proxy which must be specified in the UMC central configuration, for the entire Web server group and rerouting client requests to the servers of the group. Each server is characterized by a network address that identifies the entire group and a dedicated network address. It also ensures high availability by detecting host failures and automatically redistributing traffic to the surviving hosts.

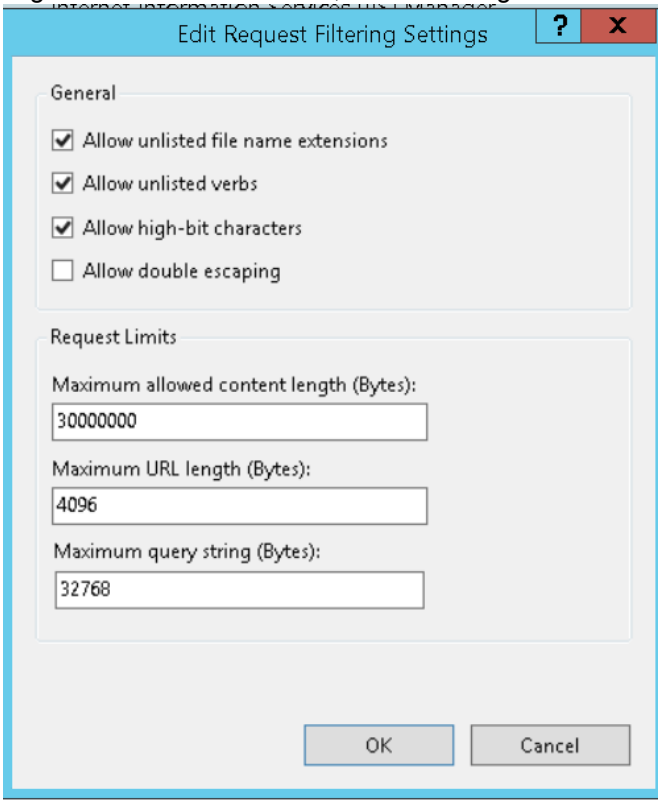
UMC specific information on NLB configuration can be found in the following sections:

- High Availability/Reliability General Issues
- NLB and Health State Integration

5.1 High Availability/Reliability General Issues

- The level of availability/reliability of the system depends on many factors, such as the IT infrastructure, the redundancy of the UMC architecture, the adopted NLB service and session state provider.
- The choices related to the previous factors have a deep impact on the system security. The triad of the security quality attributes is granted as follows:
  - *integrity*, the assurance that the information is trustworthy and accurate, is granted by our system;
  - *confidentiality*, a set of rules that limits access to information, is granted thanks to third party software that manage redundancy, such as NLB;
  - *availability*, the reliable access to the system by authorized people, is granted thanks to third party software that manage redundancy, such as NLB.
- If you want to have the Integrated Windows Authentication mechanism working properly without asking user credentials, you have to use Kerberos in order to authenticate against IIS. Kerberos requires a specific configuration in an NLB scenario. Refer to Microsoft Technical documentation for more details (see for instance http://blogs.msdn.com/b/vivekkum/archive/2008/06/15/step-by-step-kerberos-in-nlb-with-shared-content.aspx).

- If you configure a Reverse Proxy in order to use multiple web servers you must increase the value of the query string length on all the web servers, via IIS Manager to the values specified in the following screenshot.



- UMC WEB UI does not support NLB with more than one node, except if you use session affinity.

5.2 Health State Service

UMC Health State is an HTTP/HTTPS service that provides information on the health state of the authentication via UMC Identity Provider. The protocol depends on IIS configuration.

The value of the health state is contained in the field **status** of the HTTP response header:

- **status** = 200, the authentication can be performed successfully;
- **status** = 404, the authentication cannot be performed.

The health state information is derived from the one provided by the Health Check Service described in UMC Release Notes.

Example URL

```
https://<host_name>/umc-sso/GetHealthState
```

5.3 NLB and Health State Integration

UMC health state service can be used in a high availability/reliability scenario based on NLB technology to start/stop the use of UMC machines running the Identity Provider according to the result provided by the health state. We here provide an example script developed in PowerShell that queries the status of a node and stops or starts it according to UMC status using Microsoft Windows Server NLB powershell commands. The script can be scheduled to run periodically via Windows task scheduler.

PowerShell Script Example

CAUTION:

The sample code is provided for illustrative purposes only. It has not been thoroughly tested under all conditions. Therefore, we cannot guarantee or imply its reliability, serviceability, or function.

In the example two machines VM-UMC-N1 and VM-UMC-N2 are configured in NLB and their status is checked via the PowerShell function **CheckNodeHS**. According to the status, the node is stopped or started.

CheckNodeHS

```
Function CheckNodeHS([string]$nodeToCheck)
{
   $url="https://"+$nodeToCheck+"/umc.idp/GetHealthState"
   $r = [System.Net.WebRequest]::Create($url)

   #Ignore certificate exception
   [System.Net.ServicePointManager]::ServerCertificateValidationCallback =
{$true}
   try
   {
      $resp = $r.GetResponse()
   }
   catch [Net.WebException]
   {
      #404 is handled with an exception
   }
   if($resp.StatusCode -match "OK")
   {
      #200 returned
      Write-Host "Node "+$nodeToCheck+ " OK"
      Start-NlbClusterNode $nodeToCheck
   }
   else
   {
```

```
        #any other value than 200
        Write-Host "Node "+$nodeToCheck+ " NOT OK"
        Stop-NlbClusterNode $nodeToCheck
    }
}
```

Script

```
#MAIN
cls
Import-Module NetworkLoadBalancingClusters
$node1="VM-UMC-N1"
$node2="VM-UMC-N2"
$nodeStatus = Get-NlbClusterNode -hostname "VM-UMC-N1"
$status1 = $nodeStatus[0].State.ToString()
$status2 = $nodeStatus[1].State.ToString()
if ($status1 -match "converged" -and $status2 -match "converged")
{
    Write-Host "NLB status is good"
}
else
{
    Write-Host "NLB status is NOT good"
    Write-Host "Node 1: status is" $status1
    Write-Host "Node 2: status is" $status2
}
CheckNodeHS($node1)
CheckNodeHS($node2)
```

6 How to Upgrade to UMC 2.9 SP2

The following describes how to upgrade to the latest version of UMC from all previous versions of UMC, see the version specific notes as some versions require additional steps.

A prior version of UMC is installed and configured on all the machines in the scenario you need to upgrade. If a previous version of UMC is only installed and not configured, you simply have to install and configure UMC as if it were the first installation.

Prerequisites

- Follow the general recommendations for UMC upgrade.

Workflow

1. Upgrade UM secondary ring server.
2. Upgrade UM priority ring server.
3. Upgrade all the UM servers giving precedence to the ones belonging to the NLB cluster.
4. Upgrade all the UM agents.
5. Upgrade all the UMC station clients.

Note: If you use Web UI, you must clear the browser cache on all the machines which access the web UI.

6.1 General Recommendations

In this page you can find a set of notes guidelines which must be followed to upgrade UMC correctly.

Before You Start

- To check the machine role you can use the umconf **Show Status** command. See the *UMCONF User Manual* for more details.
- During the upgrade procedure, no UMC commands can be executed except those which are part of the procedure.

Version Specific Notes

This section contains a list of notes which only apply when upgrading from specific versions of UMC.

- Upgrading from 1.0: If you have installed and configured UMC 1.0, you have first to upgrade to UMC 1.1 (see UMC 1.1 Release Notes) and then upgrade the system.
- Upgrading from 1.1: If you have installed UMC 1.1 in a HTTP scenario, you have to convert the scenario from HTTP to HTTPS after upgrading.
- Upgrading from versions prior to 1.6: Mixed version scenarios may encounter issues if a user name which is longer than 30 characters is used. We strongly suggest that you align the installations to the most recent UMC version.
- Upgrading from versions prior to 1.9.1: As of 1.9.1 the value of the global account policy Password Expiration cannot exceed 1827 days. If the value was set in excess of 1827, you must re-set the value after upgrading.
- Upgrading from versions prior to 2.0: As the IdP underwent substantial changes, once you have upgraded your installation you must redo any settings which were performed on the webconfig, see Migrating IdP Configurations.
- Upgrading from versions prior to 2.0 on UM servers and the secondary ring server the Web Component configuration script cannot update the whitelisting. UM Servers and the secondary rings server must be added to whitelisting using UMConf on the primary ring server.
- Upgrading from versions prior to 2.0 verify the prerequisites are met: Application Request Routing and its prerequisites have been downloaded and installed (For iis 8 and above: https://www.microsoft.com/en-us/download/details.aspx?id=47332).

Long Term Mixed Version Scenarios

The following notes are relative to long term mixed version scenarios, which is a scenario where the version of UMC installed is not the same on all the machines in the scenario:

- As of UMC 1.9 we support long-term mixed distributed scenarios. If you have a scenario with a version which is prior to 1.9, you must upgrade all the UMC installations to at least UMC 1.9.
- Long term mixed versions are not supported on ring severs, therefore the version of UMC installed on ring servers must be aligned as quickly as possible.

6.1.1 Migrating IdP Configurations

When migrating from versions prior to UMC 2.0, as the IdP underwent substantial changes, once you have upgraded your installation you must redo any settings which were performed on the webconfig.

Where the following configurations correspond to configurations which are present in the new IdP.

Functionality	Old web config	New IdP json file
Enable Login via Smart Card Authentication	EnablePKI	(Disabled by default) see, Identity Provider Configuration Management.
Enable Login via Cookie Adapter or Custom Plugin	EnableFlexAuth	(Disabled by default) see, Identity Provider Configuration Management.

Functionality	Old web config	New IdP json file
Disable and Hide Window Authentication Link	EnableIWA	(Enabled by default) see, Identity Provider Configuration Management.
Enable the Automatic Login	AutoLoginMode	See, Identity Provider Configuration Management.
Disable the use of the Logon Station in Claims	EnableLogonStation	N/A it is now always enabled.
Enable the Identity Provider Log	LogFileName	N/A it is now always enabled and saved in the um-sso log which can be found, for example, in C:\ ProgramData\ Siemens\ UserManagement\ Log
Enable the Use of Paths in Cookies	ClaimIssuerAuthority	N/A it is now always enabled.
Enable the Use of Whitelisting	EnableWhitelistMembershipService	It is now enabled by default, see Identity Provider Configuration Management.
Enabling Anti Forgery Token	UseAntiForgeryToken	N/A
Disable the Display of the Security Disclaimer	UseDisclaimerMessage	N/A

6.2 Upgrading UM Secondary Ring Server

General Recommendations

- During the upgrading procedure only the priority ring server is available; thus, for a minimum amount of time, you do not have system redundancy support.
- During the upgrading procedure, session loss may occur.
- The Primary Ring Server and Secondary Ring Server do not support long term mixed version, and therefore the installations must be aligned as soon as possible.

Procedure

1. If NLB is configured, remove the secondary ring server from the NLB cluster.
2. If UMC Web components were configured on the machine, run the **Remove_IdP_WebUI_configuration.bat.**
3. Close all the running applications.
4. Launch the installer and select to upgrade the system. In case the installation asks you to reboot the system, perform the system reboot. When the system reboots the installer automatically starts.
5. Run the command **umconf -U** to upgrade the system. Refer to the *UMCONF User Manual* for more details
6. If UMC Web components were configured on the machine:
   – Run the **IdP_WebUI_configurator.bat** or manually configure the IdP.
   – Manually perform Identity Provider **web.config** customization on the .json configuration file,
7. If NLB was configured:
   – reconnect the machine to the NLB cluster;
   – remove the priority ring server and all the other UM servers (if any) from the NLB cluster.
8. if an upgrade is made to version 2.7 SP1, run the command: **sc config "up service" depend="UMC service"** to add the correct dependency to the UPSERVICE.

Note: If you use Web UI clear the browser cache on all the machines which access the web UI.

6.3 Upgrading UM Priority Ring Server

General Recommendations

- During the upgrading procedure only the secondary ring server is available; thus, for a minimum amount of time, you do not have system redundancy support and UMC database modifications are not possible.
- During the upgrading procedure, session loss may occur.
- The Primary Ring Server and Secondary Ring Server do not support long term mixed versions, and therefore the installations must be aligned as soon as possible.

Procedure

1. If UMC Web components were configured on the machine run the **Remove_IdP_WebUI_configuration.bat.**
2. Close all the running applications.
3. Launch the installer and select to upgrade the system. The system may ask you to reboot before or after upgrading UMC, in which case you must perform the system reboot. If the

reboot is performed before upgrading the installer will automatically starts when the system reboots.

4. Run the command **umconf -U** to upgrade the system. Refer to the *UMCONF User Manual* for more details.
5. If UMC 1.1 is installed in a standalone scenario in HTTP and you want to enable HTTPS upgrading to UMC 1.4, then you have to perform this additional procedure.
6. If UMC Web components were configured on the machine:
   – Run the **IdP_WebUI_configurator.bat** or manually configure the IdP.
   – Manually perform Identity Provider **web.config** customizations on the .json configuration file,
7. If NLB was configured, reconnect the machine to the NLB cluster.
8. If an upgrade is made to version 2.7 SP1, run the command: **sc config "up service" depend="UMC service"** to add the correct dependency to the UPSERVICE.

If you use Web UI clear the browser cache on all the machines which access the web UI.

6.4 Restarting UM Secondary Ring Server

If the certificates validity is already closer than two years to the expiration date, a restart of UM Secondary Ring Server is needed after the upgrade of UMC Primary Ring server, in order to execute the automatic certificate renewal in the right order. See Performing the Automatic Certificates Renewal for details.

6.5 Upgrading UM Server

General Recommendations

- During the upgrading procedure, session loss may occur.

Procedure

1. If UMC Web components were configured on the machine, stop the application pools of the UMC applications in **IIS Manager** and run the **Remove_IdP_WebUI_configuration.bat.**
2. Close all the running applications.
3. Launch the installer and select to upgrade the system. In case the installation prompts you to reboot the system, perform the system reboot. When the system reboots, the installer automatically starts.
4. Run the command **umconf -U** to upgrade the system. Refer to the *UMCONF User Manual* for more details.
5. If UMC Web components were configured on the machine:
   – Run the **IdP_WebUI_configurator.bat** or manually configure the IdP.

– Manually perform Identity Provider **web.config** customizations on the .json configuration file,

6. If the UM server was connected to NLB cluster, reconnect the machine to the cluster.
7. if an upgrade is made to version 2.7 SP1, run the command: **sc config "up service" depend="UMC service"** to add the correct dependency to the UPSERVICE.

6.6 Upgrading UM Agent

Procedure

1. Close all the running applications.
2. Launch the installer and select to upgrade the system. In case the installation prompts you to reboot the system, perform the system reboot. When the system reboots the installer automatically starts.
3. Run the command **umconf -U** to upgrade the system. Refer to the *UMCONF User Manual* for more details.

6.7 Upgrading UMC Station Client

Procedure

1. Close all the running applications.
2. Launch the installer and select to upgrade the system. In case the installation prompts you to reboot the system, perform the system reboot. When the system reboots the installer automatically starts.

Result

The machine is automatically registered and no additional steps are needed.

6.8 Upgrading the Web Components Manually

To configure the web components manually after an upgrade you must perform the configurations described below.

Workflow

1. Configuring Identity Provider

2. Configuring Web UI and Service Layer API
3. Configuring Remote Authentication
4. Configuring URL Rewrite Rules
5. Configure Upgrade-Specific URL Rewrite Rules
6. Adding the IdP to Whitelisting
7. Configuring the Identity Provider

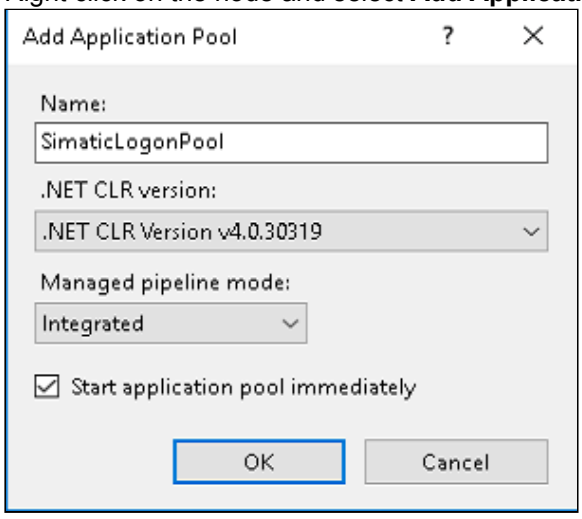
6.8.1 Upgrade - Configuring Identity Provider

Prerequisites

- The Identity Provider prerequisites have been satisfied.
- The machine must be a 64 bit UM ring server or UM server.

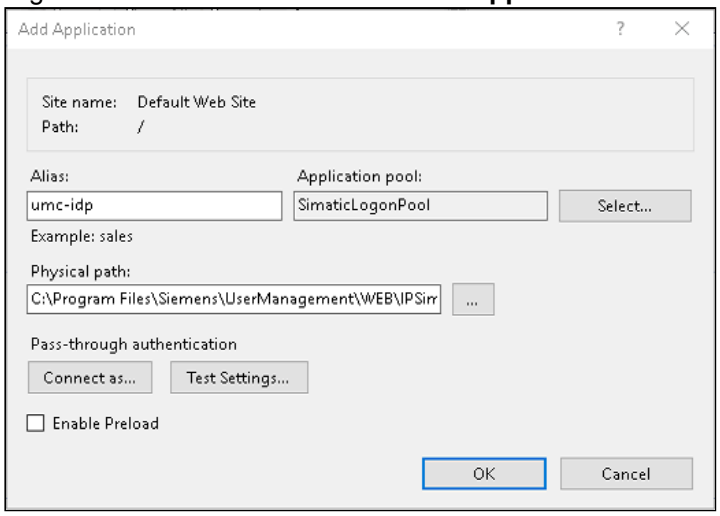
Procedure

1. Open **IIS Manager**.
2. In the tree on the left select the **Application Pools** node.
3. Right click on the node and select **Add Application Pool**: the following dialog box opens.

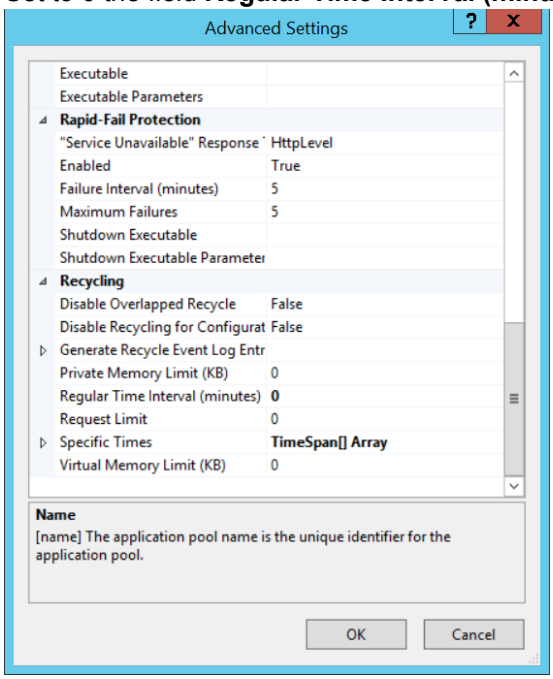


4. Insert the parameters as displayed in the previous image and click **OK**.
5. In the tree on the left select the **Default Web Site** node.

6. Right click on the node and select **Add Application**: the following dialog box opens.



7. Insert the parameters as displayed in the previous image and click **OK**. The path varies depending on where UMC is installed, for example C:\Program Files\Siemens\UserManagement\web\ipsimatic-logon.
8. On the applications pool page select the newly created application pool, and click **Manage Application** > **Advanced Settings**.
9. Set to 0 the field **Regular Time Interval (minutes)** and click **OK**.



6.8.2 Upgrade - Configuring Web UI

Important:

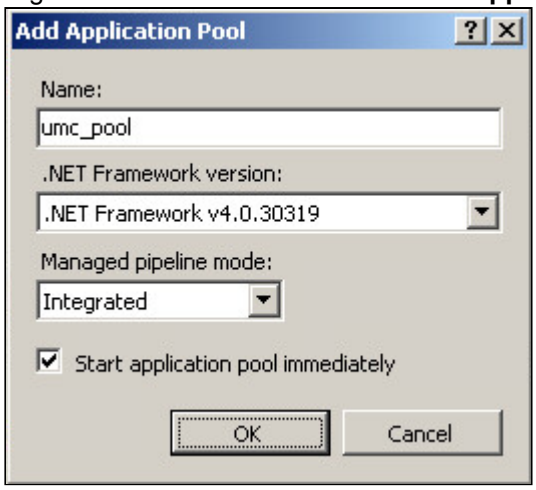
UMC contains two IIS 64 bit Native Modules: **um.ra.dll** and **um.slvm64.dll**

Prerequisites

- The prerequisites have been satisfied.
- The machine must be a 64 bit UM ring server or UM server.
- The Identity Provider (IdP) has been correctly configured.

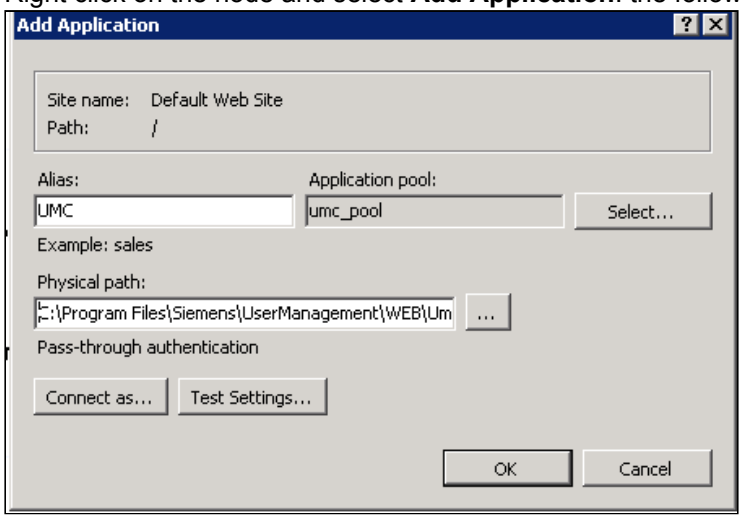
Procedure

1. Open the **Registry Editor**.
2. In the tree on the left go to the **HKLM\SOFTWARE\SIEMENS\User Management\WebUI\Settings** node.
3. Double click on idpaddress and change **Value data** to the complete IdP URL, for example if the IdP is located on the local machine: https://FQDNmachinename/umc-sso or https://reverseproxyadress/umc-sso for complex scenarios like NLB scenarios. Depending on the IdP configuration the URL may start with **http** or **https**.
4. In the tree on the left go to the **HKLM\SOFTWARE\SIEMENS\User Management\CERT Library\Domain** node.
5. Right click on the **Domain** node, select **New > String Value** and insert the name **Web**.
6. Close the **Registry Editor**.
7. Open **IIS Manager**.
8. In the tree on the left select the **Application Pools** node.
9. Right click on the node and select **Add Application Pool**: the following dialog box opens.



10. Insert the parameters as displayed in the previous image and click **OK**.
11. In the tree on the left go to the **Default Web Site** node.

12. Right click on the node and select **Add Application**: the following dialog opens.



13. Insert the parameters as displayed in the previous image and click **OK**. The path of the application is, for example C:\Program Files\Siemens\UserManagement\WEB\Umc.
14. To verify that the application works properly, in the tree on the left go to the **UMC** node.
15. Right click on the node and select **Manage Application > Browse**. The Web UI application opens displaying the login page.

6.8.3 Upgrade - Configuring Remote Authentication

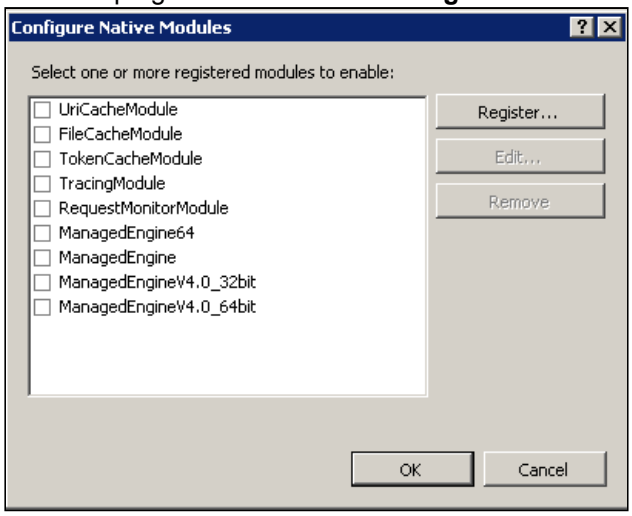
Prerequisites

- The general UMC prerequisites have been satisfied.
- The machine must be a 64 bit UM ring server or UM server.

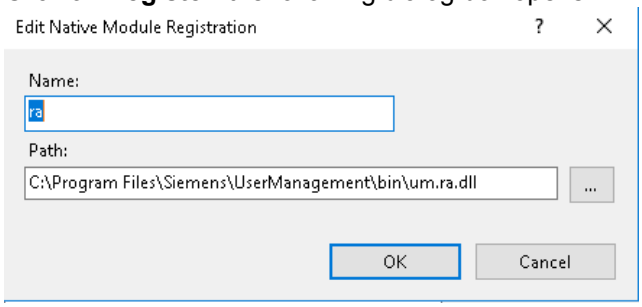
Procedure

1. Open **IIS Manager**.
2. In the tree on the left go to the root node.
3. On the right area of the screen double click on **Modules**.

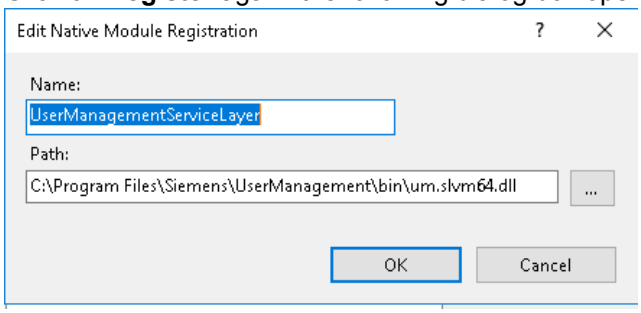
4. On the top right corner click on **Configure Native Modules**: the following dialog box opens.



5. Click on **Register**: the following dialog box opens.



6. Insert the parameters as displayed in the previous image and click **OK.**
7. Click on **Register** again: the following dialog box opens.



8. Insert the parameters as displayed in the previous image.
9. Once you have added the module make sure they are not selected and click **OK.**
10. Click **Modules** under the **UMC** application.
11. On the top right corner click on **Configure Native Modules.**
12. Select the **UserManagementServiceLayer module** checkbox then click **OK**.
13. Click **Modules** under the **ra** application, if ra is not present see note.
14. On the top right corner click on **Configure Native Modules**.
15. Select the **ra module** checkbox then click **OK.**

Note: If the ra application is not already present:

1. create a folder under the WEB (for example C:\Program Files\Siemens\UserManagement\WEB folder called *ra.*
2. add an application to the default site called "ra" specifying the path of the folder created in the previous step.

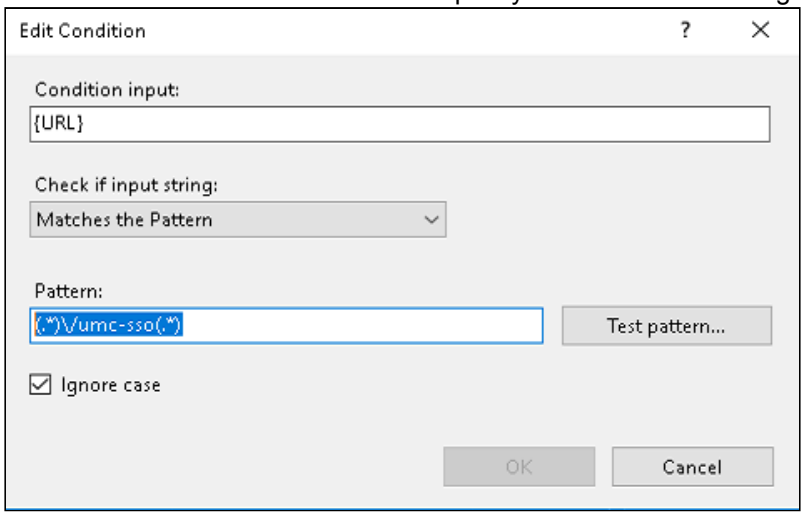
6.8.4 Upgrade - Configuring URL Rewrite Rules

You must manually configure the following URL rewrite rules in IIS.

Procedure

1. Go to **IIS Manager**.
2. In the **Connections** pane, select your server and then the top level site.
3. In the **Site** pane, double-click **URL rewrite.**
4. In the **Actions** pane, click **View Server Variables.**
5. Click **Add...** and specify *[http cookie].*
6. Go to the **Server** pane, double-click **Application Request Routing Cache**.
7. In the **Actions** pane, click **Server Proxy Settings** .
8. On the **Application Request Routing** page, select **Enable proxy**.
9. Check that the **Reverse rewrite host in response header** flag is false. It is recommended to set it as false in the case of a physics reverse proxy or in case you want to define a specific domain of the cookies.
10. In the **Actions** pane, click **Apply**.
11. In the **Server pane**, double-click **URL Rewrite**.
12. In the **Actions pane** on the right-hand side, click **Add rules**.
13. In the **Add Rules** dialog box, select **Blank Rule** and click **OK**.
14. In the **Edit inbound rule** pop-up, specify the following:
    – Name of the rule: UMC SSO Static
    – Pattern to use for matching the URL string: Matches the Pattern.
    – Using: Regular Expressions.
    – Pattern: (.*)
    – Specify the action type: Rewrite
    – Action properties Rewrite URL: The URL to rewrite, either http or https, local address 127.0.0.1, the port of reverse proxy, and /umc-sso for example: http://127.0.0.1:8443/umc-sso{C:2} (8443 is the standard port to be changed if idp listener port is customized).

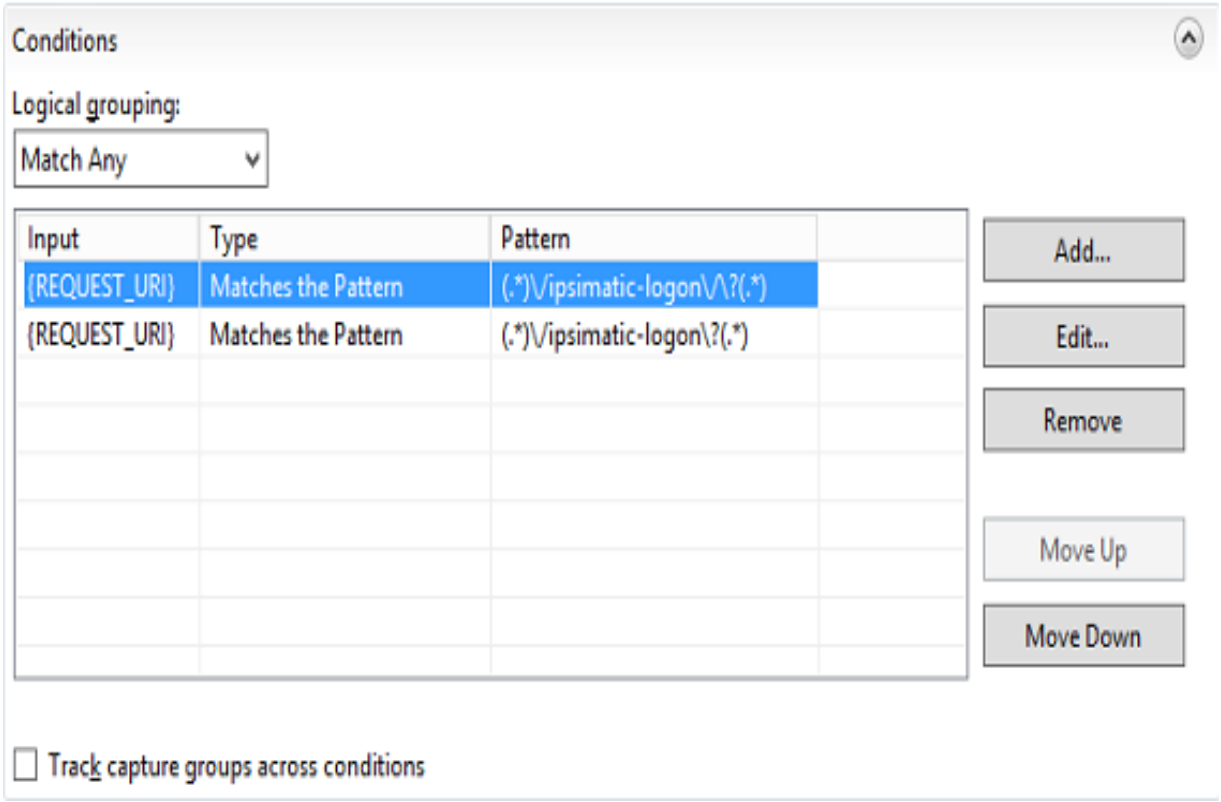
15. Click **Add** in the conditions area and specify the values in the image below.



16. Click **OK**.The pop-up is closed.
17. Click **Add** in the **Server Variables** area.
18. Select the **HTTP_COOKIE** server variable from the drop down list and insert {HTTP_COOKIE} ;ReverseProxyHost={SERVER_NAME};ReverseProxyPort={SERVER_PORT} in the value field.
19. Check the **Replace the existing value** checkbox, then click **OK**.The pop-up is closed.
20. In the action pane click **Apply**.

Procedure: ADD IDP Legacy rule

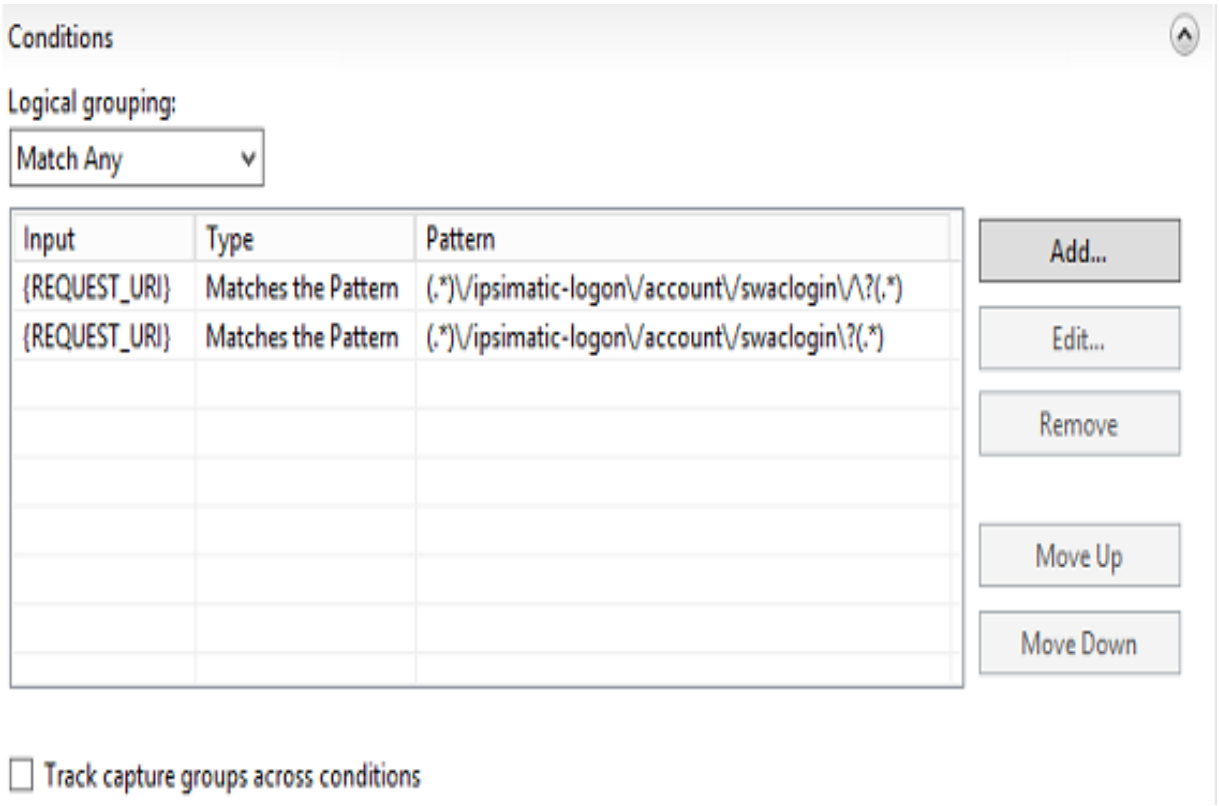
1. In the **Server pane**, double-click **URL Rewrite**.
2. In the **Actions pane** on the right-hand side, click **Add rules**.
3. In the **Add Rules** dialog box, select **Blank Rule** and click **OK**.
4. In the **Edit inbound rule** pop-up, specify the following:
   – Name of the rule: UMC IDP NODE SWITCH OFF
   – Pattern to use for matching the URL string: Matches the Pattern.
   – Using: Regular Expressions.
   – Pattern: (.*)
   – Specify the action type: Rewrite
   – Action properties Rewrite URL: The URL to rewrite, either http or https, local address 127. 0.0.1, the port of reverse proxy, and /umc-sso for example: http://127.0.0.1:8443/umc-sso {C:2} (8443 is the standard port to be changed if idp listener port is customized)
5. Click **Add** in the conditions area and specify the following conditions in the image below.



1. Click **OK**.The pop-up is closed.
2. Click **Add** in the **Server Variables** area.
3. Select the **HTTP_COOKIE** server variable from the drop down list and insert {HTTP_COOKIE} ;ReverseProxyHost={SERVER_NAME};ReverseProxyPort={SERVER_PORT} in the value field.
4. Check the **Replace the existing value** checkbox, then click **OK**.The pop-up is closed.
5. In the action pane click **Apply**.

Procedure: ADD SWAC Legacy rule

1. In the **Server pane**, double-click **URL Rewrite**.
2. In the **Actions pane** on the right-hand side, click **Add rules**.
3. In the **Add Rules** dialog box, select **Blank Rule** and click **OK**.
4. In the **Edit inbound rule** pop-up, specify the following:
   – Name of the rule: UMC IDP NODE SWITCH OFF (SWAC)
   – Pattern to use for matching the URL string: Matches the Pattern.
   – Using: Regular Expressions.
   – Pattern: (.*)
   – Specify the action type: Rewrite
   – Action properties Rewrite URL: The URL to rewrite, either http or https, local address 127. 0.0.1, the port of reverse proxy, and /umc-sso for example: http://127.0.0.1:8443/umc-sso{C:2} (8443 is the standard port to be changed if idp listener port is customized)
5. Click **Add** in the conditions area and specify the following conditions in the image below.



1. Click **OK**.The pop-up is closed.
2. Click **Add** in the **Server Variables** area.
3. Select the **HTTP_COOKIE** server variable from the drop down list and insert {HTTP_COOKIE} ;ReverseProxyHost={SERVER_NAME};ReverseProxyPort={SERVER_PORT} in the value field.
4. Check the **Replace the existing value** checkbox, then click **OK**.The pop-up is closed.
5. In the action pane click **Apply**.

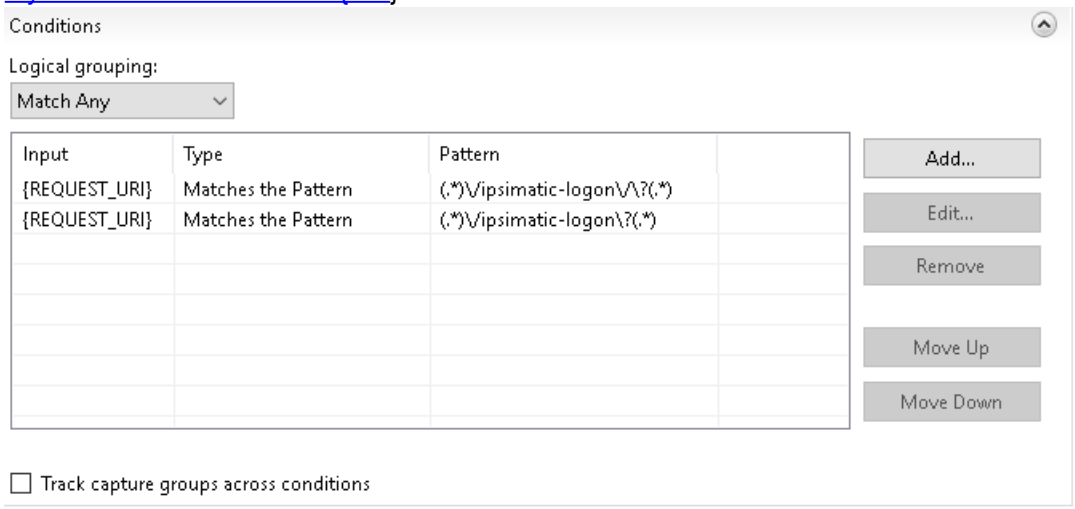
6.8.4.1 Upgrade - URL Rewrite Rules

Following the procedure described above repeat from step 8 adding two rules with their relative conditions:

UMC IDP Node Switch Off Rule

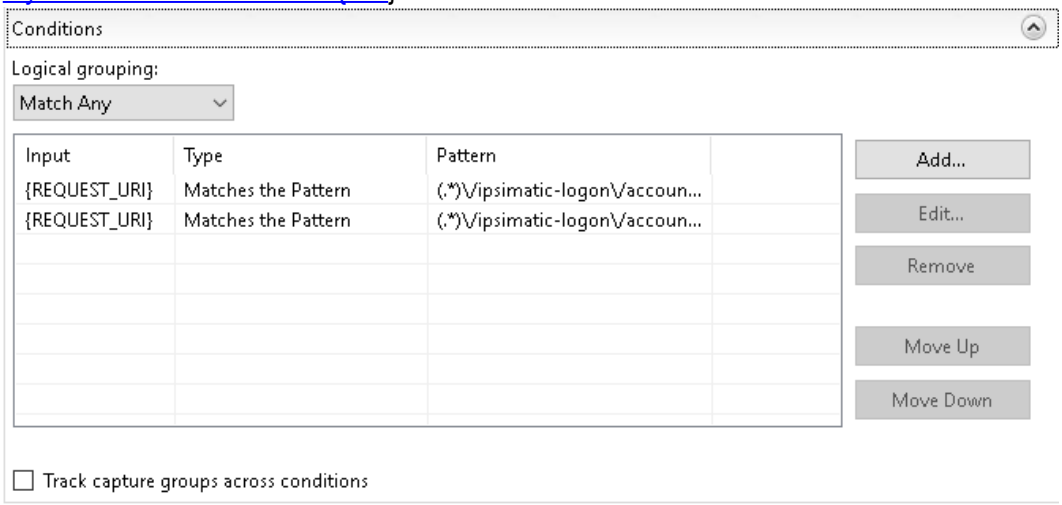
- Name of the rule: UMC IDP Node switch off
- Pattern to use for matching the URL string: Matches the Pattern.
- Using: Regular Expressions.
- Pattern: (.*)
- Specify the action type: Rewrite
- Action properties Rewrite URL: The url to rewrite, either https or https, the FQDN or machine name, the port of reverse proxy, the port of the reverse proxy, and /umc-sso for example: http://

mymachine-0:8443/umc-sso{C:2}



UMC IDP Node Switch Off Rule (SWAC)

- Name of the rule: UMC IDP Node switch off (swac)
- Pattern to use for matching the URL string: Matches the Pattern.
- Using: Regular Expressions.
- Pattern: (.*)
- Specify the action type: Rewrite
- Action properties Rewrite URL: The url to rewrite, either https or https, the FQDN or machine name, the port of reverse proxy, the port of the reverse proxy, and /umc-sso for example: http://mymachine-0:8443/umc-sso{C:2}



6.8.5 Upgrade - Adding the IdP to Whitelisting

For the WebUI to function correctly you must whitelist the URL of the Service Layer.

The computer name, which is case sensitive, must be the same as that which is specified in the registry key.

Note: When upgrading from versions prior to 2.0 you must add the Service Layer of the secondary ring server and any UM servers to whitelisting on the Primary Ring Server.

Procedure

1. Whitelist the URL of the relying party using the **umconf.exe** program. Using either the *computername/UMC/slwapi/service* or *computername/UMC/slwapi/service* and *computername.userdnsdomain/UMC/slwapi/service.* See *UMCONF User Manual* for more details.

```
"%bin%\umconf.exe" -c -w -d "http://%COMPUTERNAME%/UMC/slwapi/
service"
or
"%bin%\umconf.exe" -c -w -d "http://%COMPUTERNAME%/UMC/slwapi/
service"
"%bin%\umconf.exe" -c -w -d "http://%COMPUTERNAME%.%USERDNSDOMAIN%/
UMC/slwapi/service"
```

2. Restart the **UMC Service**.

6.8.6 Upgrade - Configuring the Identity Provider

You must set the values of UMCDllFolderPath, reverseProxy and idpListenerPort in the Identity Provider local configuration file in order for the identity provider to work.

See Local Configuration File for more information on the configuration file.

Note: In order for modifications made to the Local configuration file to take effect you must restart the UMC Service.

7 How to Uninstall UMC

Depending on the UMC installation, follow either of these procedures:

- Uninstall Full UMC
- Unistall UMC Station Client

7.1 Uninstalling Full UMC

CAUTION:

If UMC is also configured, the database files are not removed by the uninstallation procedure. This procedure has to be performed on all the machines, UM ring servers, UM servers and agents. We suggest that you perform the procedure on the UM agents first.

Procedure

1. If the machine is a 64 bit ring server where the Web Components have been configured, launch the script **REMOVE_IdP_WebUI_configurator.bat**. The batch file can be found in C:\Program Files\SIEMENS\UserManagement\BIN, if the default installation folder is selected. Note that the script works on a 64 bit machine only.
2. Delete the database files, the registry entries and so on by executing the **umconf** -D -f command, installed in the subdirectory **\BIN** (for example C:\Program Files\Siemens\UserManagement\BIN). Please refer to the *UMCONF User Manual* for more details.
3. Open **Program and Features** from the **Control Panel**.
4. Select the **UMC** entry and right click.
5. Select **Uninstall**.
6. The uninstall setup is launched: proceed with the uninstallation steps.

7.2 Uninstalling UMC Station Client

Procedure

1. Open **Program and Features** from the **Control Panel**.
2. Select the **UMC Station Client** entry and right click.
3. Select **Uninistall**.
4. The uninstall setup is launched: proceed with the uninstallation steps.

8 Troubleshooting

General

Problem Description	Solution
Cannot Authenticate with unexpected problem. umtracer gpclib shows a tentative to use pipes to open a connection to local machine.	Give access to the user that is launching the command to the CONF directory of UMC (auth. users, for example).
IdP shows a compilation error and raises an error while trying to access a temp folder (windows temp or temporary asp.net files)	IIS_IUSRS has no access to windows TEMP folder.
Web UI: cannot enter a UMC web application with error "Cannot connect to server"	**umc_pool** application pool was configured to run in 32 bit mode. Set the flag "Enable 32 bit" to FALSE in **umc_pool** configuration.
UMC Web UI shows the following error Error on Login: *An error occurred during communication with the server*.	IIS features missing: Basic authentication, Windows authentication, asp.net 4.5 was not installed.
Identity Provider Login pages shows error related to unknown Keys or security error related to webconfig.	IIS features missing: Basic authentication, Windows authentication, asp.net 4.5 was not installed. Relaunch Idp_webui_, and so on.
UMCONF error 4 while joining.	The list of UMC rings is already full - check on ring master with umconf -t and unjoin the secondary ring.
Windows 7 OS, Authentication error (4 or 1) while trying to auth, crash of um.server.exe, errors on LadLibraryEX()	Security KB missing - see *User Management Component Installation Manual*.
Windows Integrated Authentication. IdP page ask for credential even if the user is correctly logged in the AD (the client is joined to the same AD than the web server).	The AD (kerberos) is misconfigured. See the link below to prevent issues in our test domain controller: https://blogs.msdn.microsoft.com/chiranth/2014/04/17/setting-up-kerberos-authentication-for-a-website-in-iis/ set the IIS authenticated user override to "useauthenticatedUser as described here https://docs.microsoft.com/en-us/iis/configuration/system.webServer/serverRuntime with this command : " appcmd.exe set config "Default Web Site" -section:system.webServer/serverRuntime /authenticatedUserOverride:"UseAuthenticatedUser" /commit:apphost"

Problem Description	Solution
SMART CARD: Error 403.7 forbidden when trying to open info.aspx page and / or trying to authenticate.	Enable CRL (Client Revocation List), refer to your IT department for details.
The server error "Maximum request length exceeded" is raised.	A request exceeding the maximum IIS configuration limits has been sent to the server. You can modify IIS configuration if needed.
UMC operations hangs and return a generic or wrong error message.	Check is the umc processes are all active.
Operations that requires changes on UM configuration fails with error SL_NOTAMASTER.	Please check if the UM primary master is correctly running and reacheable. If the problem occurs also on the primary ring server, please restart um.ring.exe service.
Some operation fails sporadically with generic error.	um.racrmtsrv.log file contains UMC DB files access error. Please check the root cause of filesystem error (antivirus, backup, etc.).
Error on login " The validation of the parameter 'service' failed "	The service is not in the whitelist (service is a parameter passed to the login request and identify who is the caller) use umconf to add whitelist entry or login with umc admin user the first time (this add service in whitelist automatically) Same error appear if user try to open directly idp page : https://vm-umc6.umdom1.net/umc-idp/idpauthsite/index.html without start from https://vm-umc6.umdom1.net/umc
Problem on visualization of login screen (2.x)	Check if ARR is installed and also ciis component url rewrite if yes check the address and of redirection inside the rule, it must be coherent with registry entry for websettings

Provisioning

Problem Description	Solution	Additional Links
You cannot configure the provisioning.	Verify that the ring server machine is joined to the Windows domain.	NA
In the UMC Web UI you display *undefined* in the domain drop down list to import users/groups.	Verify that the ring server machine is joined to the Windows domain, that you have configured the UMC Provisioning service **UPService.exe** and that the Windows user associated to the service has Active Directory access rights.	NA
The import buttons do not appear in the UMC Web UI.	Verify that you have configured the UMC Provisioning service **UPService.exe** and check that the value of the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\User Management\WebUI\Settings\domains_support is set to **yes**.	See the Basic Post Setup Instructions of the *Release Notes,* the *UMCONF User Manual* and *UMX User Manual* for the commands.

Problem Description	Solution	Additional Links
You perform the import of an AD group and the members are not imported.	Verify that you have configured the UMC Provisioning service UPService.exe with the user that has write access on the UMC folder **C:\ProgramData\Siemens\UserManagement\CONF**. Alternatively the user must belong to the Windows group UM Service Accounts.	See Associate Active Directory Windows User with Provisioning Service.
You perform the import of an AD group and the members are not imported.	Verify that the **Group scope** is **Universal**.	See the *UMCONF User Manual.*
The search to import AD users/groups returns 0 and you presume that your search criteria will return many data.	You may have to modify the Active Directory administration limit **MaxPageSize**. Consider that the AD default is 1000, if your search returns more that 1000 results you have to modify this value to a value higher then the number of search results.	See the *Functional Limitations* of the *Release Notes.*
The import of an AD group having a high number of associated -users is not successful.	You may have to modify the Active Directory administration limit **MaxValRange**.	See the *Functional Limitations* of the *Release Notes.*
You experience an excessive slowness in operations involving AD provisioning (such as the import of users, the alignment of AD modifications and so on).	Check the CPU workload of your antivirus program as the antivirus can influence the AD provisioning performances.	NA

Using HealthState service for troubleshooting

Starting from UMC 1.8 it's possible to use a local endpoint to check umc health status (https://localhost:16/healthcheck). Please check HealthState documentation for more information.

9 Appendix

In this section you can find the following information:

9.1 Importing a Windows Local User on an Agent

Windows local user can be imported on an agent machine using a Powershell script called Siemens.UMC.ImportUser.ps1 which can be found in %ProgramFiles%\Siemens\UserManagement\BIN.

1. Run Powershell as Administrator.
2. Insert -server followed by the UMC server name.
3. Insert -user followed by username of the UMC user running the command, the user specified must have the UM_Admin function right.
4. Insert -pwd followed by password of the UMC user running the command.
5. Insert -username followed by the username of the windows local user to import. The username of the windows local user to import must be composed with one of the following patterns:
   – <computer name\name of the windows local user to import> in case of a Windows local user
   – " NT SERVICE\<SERVICE NAME>" in case of a Windows Virtual Service Account
6. Click **Enter**.

Example

```
.\Siemens.UMC.ImportUser.ps1 -server myumcservername -user
myumcadminusername -pwd myumcpassword -username mycomputername\
nameofwindowslocaluser
```

Example of Importation of a Virtual Service Account

```
.\Siemens.UMC.ImportUser.ps1 -server myumcservername -user
myumcadminusername -pwd myumcpassword -username "NT SERVICE\<SERVICE NAME>"
```

9.2 UMC Processes

Service Display Name	Service Description	Process Name	Process Description
UMC Secure Communication Service	Implements Communications for UMC	IPCSecCom.exe	UMC Secure Communication Service
		um.Ris.exe	UMC RIS Server
		um.ffsyssrv.exe	UMC FFSYS Server
		um.kei.exe	UMC Certification Server
		um.sso.exe	UMC Single SignOn Server
		um.jei.exe	UMC Join Server
UMCService	UMC Core Service	UMCService.exe	UMC Core Service
		um.server.exe	UMC Agent Server
		um.RACRMSRV.exe	UMC RACRM Server
		um.ring.exe	UMC Ring Server
		um.ELGSrv.exe	UMC Event Log Server
UPService	UMC Provisioning Service	UPService.exe	UMC Provisioning Service
		um.piisrv.exe	UMC Provisioning Server

9.3 Event Logging

UMC provides event logging. UMC event logging 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. The **um.ELGSrv.exe** server is available to manage the event logging.

The following table summarizes logged events.

	Event	Logged
Authentication		
	Successful login	⊖
	Unsuccessful Login	⊕

	Event	Logged
	Change Password	⊕
	Ticket Validation	⊖
Session Management		
	Session Creation	⊕
	Session Deletion	⊕
Configuration		
	User Create/Delete/Modify	⊕ (only from WEBUI)
	Role Create/Delete/Modify	⊕ (only from WEBUI)
	Group Create/Delete/Modify	⊕ (only from WEBUI)
	Unlock User	⊕ (only from WEBUI)
	User Locked (when automatic unlock configured)	⊕
	Global Account Policies changes	⊖
Two Factor Authentication		
	Secret key Creation	⊕ (only from WEBUI)
	Secret key Reset	⊕ (only from WEBUI)
	Time-based-one-time-password (TOTP) successfully checked	⊕
	Time-based-one-time-password (TOTP) unsuccessfully checked	⊕
SADS		
	Encryption enabled on Subject (User or Group)	⊕
	Application Key Decryption failure due to an error in User Authentication	⊕
Identity Provider		
	Host automatically added to the Identity Provider whitelist	⊕

	Event	Logged
	Identity Provider starts	⊕
	Identity Provider stops	⊕

Event logging offers the following features.

- In a redundant scenario, log files can potentially be generated from different servers. Mechanisms to manage reconciliation of data produced by different servers are available.
- Internal APIs allows one 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.
- A UMX command to list event log records is provided.

9.3.1 Event Logging Security Notes

The following security strategies have been implemented to grant system integrity for each server machine:

- Automatic cleanup of archive folder, to remove old archives before filling up the hard drive.
- Protection against excessive log activity, to avoid that archive size could increase too fast.

Automatic cleanup of archive folder

The archive folder contains a list of archive files, each of which has a maximum size equal to **1GB** (~500000 records). Every time this limit is reached, a new archive file is created and the files older than **30 days** will be deleted. This implies that archive files will be deleted only when log activity is really present and needs space disk.

To change the limit of 30 days:

1. Go to the **ELG** registry key: *HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\User Management\ELG\Settings.*
2. Add or update DWORD value **max_archive_time** with the new duration in seconds.

Protection against excessive log activity

Excessive log activity can be generated by an attempt to fill up server hard drive and make the system unavailable.

To manage this attack, archive files cannot store more than **100000** records by day (but log forwarding keeps on working).

When this limit is reached, an event log with action ELG CLOSE is written and any subsequent event logs will no longer be archived.

To recover the log archiving:

1. Go to the **ELG** registry key: *HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\User Management\ELG\Settings.*
2. Delete the DWORD value **num_archive_records_in_last_day**.
3. Restart the UMC service.

In the case the excess of log activity is generated on a disconnected server, event log ELG CLOSE is written and subsequent (local) event logs will no longer be archived.

To recover the (local) log archiving:

1. Go to the **ELG** registry key: *HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\User Management\ELG\Settings.*
2. Delete the DWORD value **num_archive_records_in_last_day_no_index**.
3. Restart the UMC service.

To change the limit of 100000 records by day:

1. Go to the **ELG** registry key: *HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\User Management\ELG\Settings.*
2. Add or update DWORD value **max_archive_records_by_day** with the new number of records.

9.4 Additional Provisioning Configuration

In order to make the import of Active Directory users and groups configurable, a file named **piisrv_config.json** is created in %program data%\siemens\usermanagement\conf.

The editing of this file is optional. The following rules apply in computing the list of the domains from which users and/or groups can be imported:

- if the property **domains** is not empty, this list is considered for import, otherwise
- the field **query_for_domains** defines the AD input query to compute the domain list.

After modifying the file, you have to:

- copy the file in each machine where the provisioning is configured and
- manually restart the **UPService**.

The file must have the following JSON format.

Configuration JSON example

```
{
  "add_alias_to": "",

  "domains": [{
                    "name": "domain1"
```

```
                }],
  "purge_time": "720",
    "query_for_domains": "(objectcategory=crossref)",
    "query_for_groups": "",
    "query_for_user": "",
    "query_for_users": "",
    "recycle_time": "1440",
     "update_mode":"noupdate",
     "polling_umc":"10",
     "polling_ad":"300",
      "import_users_from_nested_groups":
"no"
}
```

Important:

- If polling_umc and polling_ad are missing, by default the polling values are:
  - polling_umc 60 sec
  - polling_ad 600 sec
- "update_mode":"noupdate": (optional) If it is set to noupdate, no update will be performed from AD.

JSON description

Property	Type	Description
add_alias_to	string	The name of the AD field that has to be used as alias.
domains	string	It is an array of domains where each domain object contains the name. Formatted as follows: [{"name": "domain1"},{"name":"domain2"}] }, note that the domain suffix must not be used. By default the array is empty.
purge_time	string	If a user is deleted from AD, it is flag as *offline*. Offline users are permanently deleted from UMC database, after a number of minutes indicated in this field. The default is 24 hours (720 minutes). The following constraint must be valid: **purge_time <recycle_time.**
query_for_domains	string	AD query, see Microsoft documentation for more details. The query "(objectcategory=crossref)" is the default one. If the query in the file contains an error, the default query is executed.
query_for_users	string	*Not used.*
query_for_groups	string	*Not used.*
query_for_user	string	*Not used.*

Property	Type	Description
recycle_time	string	Number of minutes before provisioning server restart. The default is 24 hours (1440 minutes). The following constraint must be valid: **purge_time<recycle_time.**
polling_umc	string	The interval at which polling is performed on the UMC (default is 60 seconds)
polling_ad	string	The interval at which polling is performed on the AD (default is 600 seconds)
update_mode	string	Update mode for imported users and groups. The possible values are : **noremove, noupdate** or an empty string (the default)
import_users_from_nested_groups	string	Allowed values are yes or no. If the property is not present the default is no. If the property value is yes, the Provisioning looks for all the users in the subgroups of the group, imports them and associates them to the parent group.

Update behaviour

update_mode	Object	AD command	UMC command	Result
not present or empty string	user imported manually	rename / remove user from AD	na	The user is online but authentication fails.
not present or empty string	users import by group	unbinding user from group	na	The user is put offline, authentication fails.
not present or empty string	users import by group	rename / delete group	na	The user is put offline, authentication fails.
not present or empty string	users import by group	remove user from AD	na	The user is put offline, authentication fails.
not present or empty string	users import by group	rename user from AD	na	The user is put offline and authentication fails, a new renamed user is imported in UMC and authentication is available.
noremove \ noupdate	user imported manually	rename / remove user from AD	na	The user is online but authentication fails.

update_mode	Object	AD command	UMC command	Result
noremove \ noupdate	user imported manually	rename / remove user from AD	umx -sync	The user is online but authentication fails.
noremove \ noupdate	users import by group	unbindig user group	na	The user remains online and the authentication is successful.
noremove \ noupdate	users import by group	unbindig user group	umx -sync	The user is put offline, authentication fails.
noremove \ noupdate	users import by group	rename / delete group		The user is online the authentication is successful.
noremove \ noupdate	users import by group	rename / delete group	umx -sync	The user is put offline, authentication fails.
noremove \ noupdate	users import by group	remove user from AD		The user is online the authentication fails.
noremove \ noupdate	users import by group	remove user from AD	umx -sync	The user is put offline, authentication fails.
noremove \ noupdate	users import by group	rename user from AD		The user is onine the authentication fails, a new renamed user is imported in UMC and authentication is successful.
noremove \ noupdate	users import by group	rename user from AD	umx -sync	The user is put offline the authentication fails, a new renamed user is imported in UMC and authentication is successful.
noremove	users import by group / manually	update user		The user is updated.
noupdate	users import by group / manually	update user		The user is not updated.
noupdate	users import by group / manually	updated user	umx -sync	The user is updated.

9.5 Performing the Automatic Certificates Renewal

UMC Domain Certificates

In a UMC Domain the secure channel between UM machines is granted by means of two types of certificates managed by the communication system:

- The Network Certificate: It is created on the UM Ring master when the UMC domain is created. By default, its validity is 10 years, but it can be configured at the domain creation (see the *UMCONF User Manual* for details). The network certificate is distributed in the UM domain whenever a UM server/agent is joined/attached to the UMC domain.
- The Machine Certificate: It is assigned to every machine when it is joined/attached to the UMC domain. The machine certificate validity lasts until the Network certificate is valid.

Notes for the previous versions:

- UMC V 2.7
  - Network certificate validity = 10 years, it cannot be configured
  - Machine certificate validity = 5 years, it cannot be configured.
- UMC V<2.7:
  - Network certificate validity = 10 years, it cannot be configured
  - Machine certificate validity = 2 years, it cannot be configured.
- UMC V < 1.9 SP1 Upd2
  - Network certificate validity = 10 years, it cannot be configured
  - Machine certificate validity = 1 years, it cannot be configured.

Effects of Certificates expiration

When a TCP connection between UMC servers is already established, as long as it remains up the certificates expiration has no effect on the system. This behavior applies for both the certificate types (Network or Machine).

As soon as a disconnection occurs after a certificate expiration, or as soon as the UM RIS module of one of the connected machines is restarted, the communication is not established anymore.

In particular:

- In case of expiration of the machine certificate (for an UM ring server, UM server, UM Agent), the communication between this machine and the machines connected to it are affected.
- In case of expiration of the network certificate, this issue applies to all the UM servers and UM Agents in the UMC domain (the expiration of the network certificate corresponds to the contemporary invalidity of all the machine certificates).

Procedure for Certificates Renewal

The certificate renewal procedure is executed on a machine when less than two years are left until certificate expiration. The procedure starts automatically at the machine reboot. At the first reboot of the machines inside the two years from the certificates expiration date the following operations are performed:

- On the primary ring master, a new Network certificate and the ring Machine certificate are created and saved. Communication with the other machines continues by means of the previous certificates.
- On the secondary ring, the network certificate is propagated and saved, a new machine certificate is assigned, and the communication can use the new certificates.
- On the other servers and on the agents the network certificate is propagated and saved, and the new machine certificate is assigned. The communication with the ring master and with the other servers can use the new certificates.

Until the ring master reboot, the reboot of all the other machines of the UMC domain has no effect.

The required reboot order is the following: primary ring, secondary ring, servers, agents.

It is assumed that at least one reboot in the required order is done within two years from the certificate expiration dates.

In case only the machine certificate is expiring on a UMC machine (for example when coming from an UMC version inferior or equal to 2.7), the certificate renewal procedure must be executed only on that machine, by performing the machine reboot.

Result of certificate renewal

After the certificate renewal the following applies:

- The new Network and Machine Certificates have a 10 year validity.
- The NETID of every UM machine is changed, therefore the fingerprint is changed.
- The domain ID of the UMC domain is not changed.

The certificate renewal has no impact on the Identity Provider claim Key.

UMC Version Upgrade

When a UMC domain is upgraded to UMC V2.8 SP2 from a previous version, it is possible the certificates validity is already closer than two years to the expiration date. In this case the automatic procedure for the certificates renewal will start as soon as the domain is upgraded by means of the appropriate UMCONF -U command (see How to upgrade to UMC 2.8.2 in the *UMC Installation Guide* for details). Any reboot, if required, during the installation phase will not trigger the renew procedure.

CAUTION:

If the upgrade command UMCONF -U is not performed on the machine after a UMC upgrade, the automatic certificates renewal is disabled and a machine restart will never trigger the certificate renewal

Exceptions

- If the certificates are already expired, the automatic renewal cannot be performed and it is necessary to perform a manual procedure.