SIEMENS

Contents

User Management Component 2.9.2

UMC Security Concept

09/2020
A5E50361200-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

A5E50361200-AA
20200903_45901

Contents

1 Security Introduction

Security is the collection of functions, operations and guidelines that are necessary to protect your system. You must also ensure that certain boundary conditions are also observed in the application environment.Protection must be focused on specific areas (Integrity, Availability, Confidentiality) and is based on specific measures to minimize security risks.

To increase the current level of security, we focus on comprehensive consulting, cooperative partnerships and continuous innovation of measures and products through the exchange of ideas with security experts. Security is one of the system characteristics of Totally Integrated Automation (TIA). To help to make your plants, systems machines and networks more secure, a state-of-the-art holistic security must be implemented and maintained. Siemens products and solutions cover part of the holistic approach to security. Customers are responsible for protecting their plants, systems, machines and networks against unauthorized access.

Purpose of this Document

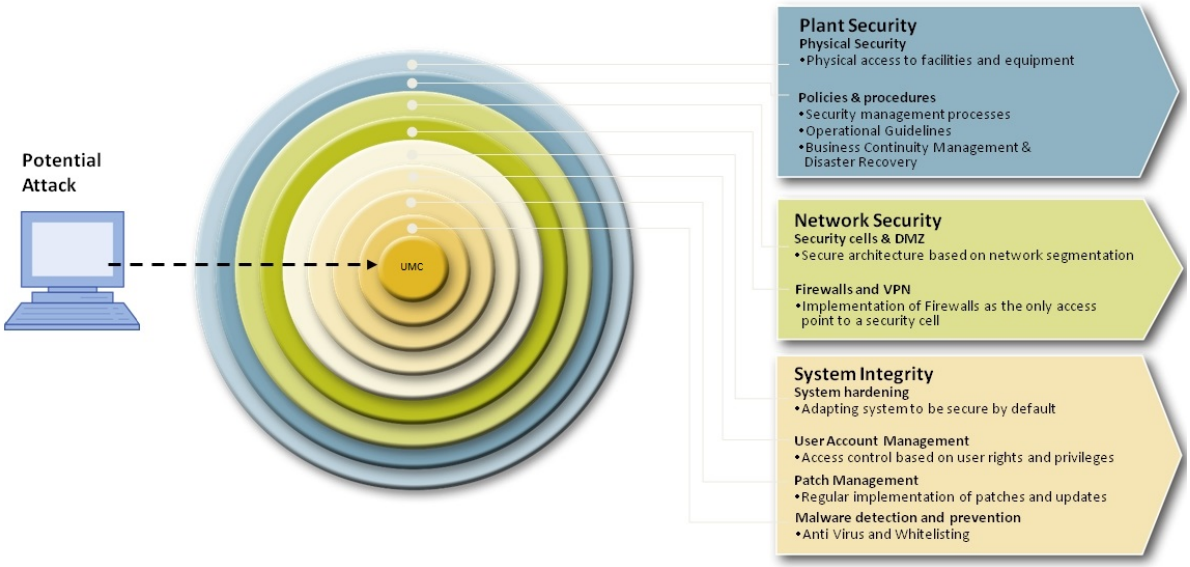
This document aims to provide a set of concepts, best practices and practical configuration settings to address the principal security risks and threats that may affect User Management Component (UMC). Although User Management solutions are often highly customized to suit the needs of specific industries and projects, some generic scenarios are provided to illustrate practical, security-aware, implementation methods. This document also provides a comprehensive overview of all the security settings and features that UMC offers.

2 Security Strategies

Computer systems and networks are inherently vulnerable to a wide variety of security threats that can be prevented or reduced by adopting specific security countermeasures. Each of these technical and organizational measures is specific for some specific attack (viruses cannot be prevented with firewalls) and can cover only a subset of the necessary protection goals. Nevertheless, only an overall strategy can provide protection.

The Siemens Industrial Security concept corresponds to a multi-layer defense, the so-called *defense-in-depth* concept. This strategy consists of several defense layers around the system to be protected, in this case the MOM/MES system:

- Plant Security Layer
- Network Security Layer
- System Integrity Layer



With a defense-in-depth approach, in which the required security measures shown here are seamlessly interwoven, it is possible to greatly improve the coverage and reliability of the protection of an automated system.

Only the operator can ultimately ensure that the system is operated securely, but the manufacturer, e. g.Siemens, can assist by providing security-hardened products with security functions and consulting services, so that the security concepts can be implemented.

The example network configuration, which you can find here, illustrates how network security (cells and firewalls) can be implemented. This document presents a step-by-step description of how this plant configuration has been made more secure by implementing security measures.

For more information on the topic of Industrial Security refer to http://www.siemens.com/industrialsecurity or to https://www.isa.org for information on *IEC 62243 Standards: Security for Industrial Automation and Control Systems*.

2.1 Plant Security Layer

Plant security covers everything related to physical access protection measures such as fences, turnstiles, cameras or card-readers and organizational measures, particularly a security management process, which ensures the long-term security of a plant. Plant security makes it so that technical IT security measures are more difficult to by-pass physically.

2.2 Network Security Layer

The central element of the Industrial Security concept is network security. This includes the measures of protection of automation networks from unauthorized access and the checking of all interfaces towards other networks, such as an office network and particularly remote access to the Internet. Network Security also encompasses increasing the protection applied to communication so that they are less susceptible to interception and manipulation, i.e. encryption during data transfer and authentication of the respective communication nodes and network segmentation.

For information on the implementation of Network Security see, Network Security Implementation.

2.3 System Integrity Layer

Securing system integrity should be regarded as the third pillar of a balanced security concept. System integrity helps to protect against data manipulation and unauthorized access to the automation process, which may interfere with production processes.

Siemens offers:

- Controllers and HMI systems with integrated security functions,
- Security functions for PC-based automation systems,
- System integrity for Motion control and drives.

For more information on how to implement system integrity see, System Integrity Implementation.

3 Security Implementation

The layers described in Security Strategies require configuration and tools. The pages listed below provide information on the implementation of the layers which can be used to increase the security of a UMC scenario. Note that plant security implementation is not in the scope of this manual.

- Network security implementation which consists of:
  - Security cells and perimeter networks,
  - Firewalls and VPNs.
- System integrity implementation which consists of:
  - System hardening,
  - Whitelisting,
  - Disaster recovery,
  - Security Controller,
  - Patch management,
  - Malware detection and management,
  - User Account Management.
  - WebUI Redirect Validation

3.1 Security Implementation Walk-through

To increase the security of a UMC scenario you should implement the following security measures:

- **Plant Security**:
  - Verify that in your plant necessary organizational and technical security measures are taken and kept up-to-date (e.g. security management process).
- **Network Security:**
  - Implement Firewalls so that access points are protected and communication to and from a security cell are regulated, only ports which are required should be open, in the case of UMC 4002 and 443.
  - Implement VPNs to establish secure network connections across public networks.
  - Create Security Cells so that plant is segmented into easier to control areas which are divide logically depending on function and location.
  - Create one or more Perimeter Networks so that direct communications between the lowest and highest level of the plant infrastructure are processed in the perimeter network before reaching lower levels of the plant.
- **System Integrity:**
  - Harden the system, by removing all the software components and functions which are not required, whitelisting software which is required, and then solidifying the system, you must also whitelist the hosts which can connect to an IDP.
  - Enable the code signing check, so that the systems logs if a UMC executable has been modified and therefore possibly compromised.

– Create backups of the system and database.
– Set-up patch management so that the operating system is maintained up-to-date and more secure.
– Implement user account management:
  - Configure authentication and authorization to verify users and limit what they can access.
  - Strengthen passwords and implement a password policy.
  - Apply a grant least privileges policy.

3.2 Network Security Implementation

The central element of the Industrial Security concept is network security. This includes the protection of automation networks from unauthorized access and the checking of all interfaces towards other networks, e.g. an office network, and particularly remote access to the Internet. Network security also encompasses protecting communication from interception and manipulation, i.e. encryption during data transfer and authentication of the respective communication nodes.

Network security can be made up of:

- Security Cells and Perimeter Networks
- Firewalls and VPNs

3.2.1 Security Cells and Perimeter Networks

Dividing networks and connected plants into security cells consists in dividing up a large corporate network into separate networks, each used for a specific business function. This strategy increases the availability of the overall system and is an effective way to mitigate security risks, segmentation of the plant into cells is an important part of applying the IEC 62443 standard. In the implementation of this approach parts of a network, e.g. an IP subnet, are protected by a security appliance and the network is secured by segmentation. Thus, devices within this 'cell' can be protected from unauthorized access from outside without affecting real-time capabilities, performance or other functions. Security threats that result in failure can thereby be restricted to the immediate vicinity.

The different ISA95 levels can be used to identify security cells, for example by keeping ERP (Enterprise Resource Planning) functions separate from MES (Manufacturing Execution System) functions, in addition in the example configuration different products are organized into security cells each with a separate firewall.

Network names grouped by their respective ISA-95 level

According to the ISA95 levels, the following levels can be identified:

- Enterprise Resource Planning Level
- Manufacturing Execution Systems Level
- Manufacturing Control Systems Level

Each level includes one or more networks. In addition we identify also perimeter networks.

When creating security cells, you should follow some design principles.

In this section we present also the example configuration organized in different security cells, for more details see *Security concept for the protection of industrial plants* document https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/digital-factory/industrial-security/online/documents/whitepapers/de/whitepaper-security-2016-v10-en.pdf

3.2.1.1 Enterprise Resource Planning Level

The Enterprise Resource Planning Level includes the Enterprise Control Network that is used to manage ERP systems, which may need to communicate with both MES and Process Control Systems located in other networks. This network is generally the outermost network used in a plant, it is therefore more exposed to potential security risks.

3.2.1.2 Manufacturing Execution Systems Level

The Manufacturing Execution Systems Level includes the Manufacturing Operations Network that contains MES/MOM servers. Typically, this network can be connected directly to a Process Control Network, while the use of a Perimeter Network is recommended with an Enterprise Control Network instead of direct connections.

3.2.1.3 Manufacturing Control Systems Level

This level includes:

- Process Control System Network
- Control System Network

- Field Device Network

Because the networks belonging to this level are physically very close to the field, it is important to keep them as separate as possible from the outer networks, to mitigate security risks and safeguard plant production. It is out of scope of this document to enter in the details of the security measures related to this level.

3.2.1.4 Perimeter Network

In addition to the secure lower level networks, we have also Perimeter Networks in our scenarios, sometimes called DMZs (Demilitarized Zones). These are networks used to isolate certain applications from outside networks, thereby mitigating security risks.

Typically, Web Servers are placed in this network, so that they can collect data from low level networks and, at the same time, they can provide web pages to outer networks (for example an Enterprise Control Network).

If you are planning to connect to UMC using the Remote Desktop Service, the Remote Desktop Service Server should be placed in this network.

3.2.1.5 Design Principles

When creating security cells, you should follow some common guidelines and implementation best practices, such as the following:

- a security cell is an independent part of the plant;
- all participants inside the cell trust each other;
- access to the security cell is permitted only through clearly-defined access points;
- access points are monitored and access is logged (data traffic, user, hardware);
- all participants of a security cell are directly connected (no bypass to the outside);
- participants with high network load will be integrated into a security cell to avoid bottlenecks.

3.2.1.6 Example Configurations with Security Cells

The following example illustrates a UMC scenario with most common networks grouped by level and product in to security cells, where the ring server is on a dedicated machine with multiple UMC servers distributed throughout the scenario.

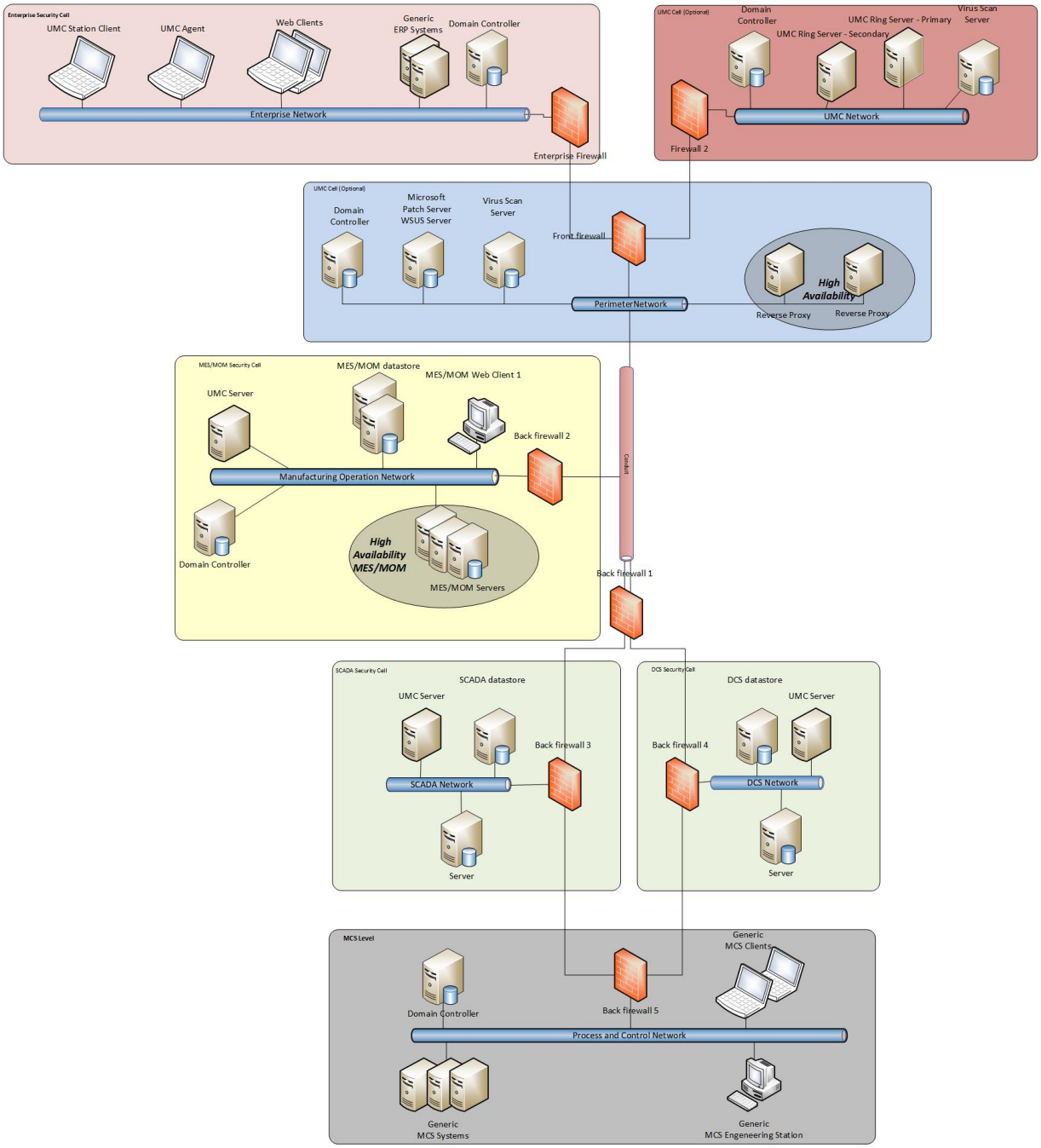
It is also possible to dedicate one of the servers present in the other cells as the ring server.

The following UMC machine roles are present in the configuration example:

- **UMC Ring Server (primary and secondary):** The owner of the UM configuration, which is responsible for managing the domain, and provides full implementation of authentication and user management features.
- **UMC Server:** a server which provides full implementation of authentication features.
- **UMC Station Client**: a machine where UMC station client software has been installed and that has been registered to be a trusted machine
- **UMC Agent:** a machine which works as a client of the UM server/UM ring server.

The following generic machines are present in the configuration example:

- **Web Clients**: web machine used to access the runtime UI Applications and to perform runtime configurations.
- **Generic ERP System**: machine where an Enterprise Resource Planning (ERP) system according to the ANSI/ISA95 standard is installed and configured.
- **MOM/MES Web Clients**: web machine used to access the MOM/MES runtime UI Applications and to perform runtime configurations.
- **MOM/MES Server**: machine hosting MES/MOM components for a production environment except for the datastore.
- **MOM/MES Datastore**: machine where the required databases will be hosted. Alternatively you can choose to create the databases on the production (and development) machine.
- **DCS Datastore: M**achine where the required databases will be hosted.
- **DCS Server: M**achine hosting DCS components for a production environment except for the datastore.
- **Scada Datastore:** Machine where the required databases will be hosted.
- **Scada Server:** machine hosting scada components for a production environment except for the datastore.
- **Generic MCS System**: machine/device hosting a generic Manufacturing Control System (MCS) according to the ANSI/ISA95 standard.
- **Generic MCS EngineeringStation**: development machine for the MCS solution.
- **Generic MCS Client**: client machine for the MCS solution.



3.2.2 Firewalls and VPNs

In order to grant network security, access points to security cells and communication between the different access points have to be secured. In this section we investigate both these aspects.

3.2.2.1 Access Points to Security Cells and Communications

One of the factors for designing security cells is that they should only have *one access point*. Any access to a security cell via this access point may occur only after having verified the legitimacy (people and devices must be authenticated and authorized) and any access must be logged.

The access points help to prevent unauthorized data traffic to security cells while allowing authorized and necessary traffic for the smooth operation of the system. The access point to a security cell can be designed according to the requirements of the configuration and functionality. An example of a security cell with a secure access point is a network where all the data traffic is protected by a firewall.

Note: Firewalls must be configured with rules to mitigate DDos attacks.

Access Points

In the configuration example, the access points to the different security cells are protected by firewalls, protect the TCP ports 4002 and the port which is used for the HTTPS IIS binding (normally 443) on the machine/s where UMC is running.

The tables below illustrates:

- the communication direction for the UMC machine roles in the example scenario;
- the communication protocols that have to be applied in order to guarantee network security.

Communication between UMC machines in different security cells

From down/ to across	UMC Station Client	UMC Agent	UMC Server	UMC Ring Server
UMC Station Client	N/A	N/A	https	https
UMC Agent	N/A	N/A	https or SSL/TLS	https or SSL/TLS
UMC Server	N/A	N/A	https	https or SSL/TLS
UMC Ring Server	N/A	N/A	https	https or SSL/TLS
Web Clients	N/A	N/A	https	https

UMC Communications

All UMC communications should be sent between servers using TLS/SSL cryptographic protocols in order to ensure network security whereas communications between clients and servers use HTTPS.

3.3 System Integrity Implementation

In information security the term *integrity* refers to something that is not subject to unauthorized changes, such as data, services. Increasing system integrity should be regarded as the third pillar of a balanced security concept. To improve system integrity you have to use automation systems and controller components, such as SCADA and HMI systems, which are protected against unauthorized access and malware or that meet special requirements such as know-how protection.

Customizations can be performed by system Integrators. However you must consider that the effects of the product and of the custom code must be distinguished. This distinction can be implemented via auditing custom code execution and deployment, or providing coding guidelines and making the customers responsible for compliant code and/or tracking execution.

System integrity can be improved through:

- System Hardening
- Whitelisting
- Disaster Recovery
- Security Controller
- Patch Management
- Malware Detection and Prevention
- User Account Management
- WebUI Redirect Validation

3.3.1 System Hardening

The term *hardening* in information security means the removal of all software components and functions that are not absolutely necessary to fulfill a given task. In other words, hardening summarizes all the measures and settings which aim to:

- reduce opportunities to exploit vulnerabilities in software;
- minimize potential methods of attack;
- limit the tools available for a successful attack;
- minimize the available rights following a successful attack;
- increase the probability of detecting a successful attack.

This is intended to increase local security and the resilience of a computer to withstand attacks.

Consequently a system can be described as "hardened" if:

- the software components and services installed are limited to those that are required for the actual operation,
- restrictive user management is implemented,
- the local Windows Firewall is enabled and is restrictively configured,
- Operating System Hardening: Before installing UMC it is recommended to harden the operating system, for example by uninstalling programs and Windows components that are not required and disabling unnecessary services.
- BIOS Hardening: Before installing UMC it is recommended to harden the computer BIOS,

System hardening can be achieved through:

- File System Configurations
- Create an Identity Provider Whitelist
- Enable Code Signing Check
- Decommissioning UMC Machines
- IIS Hardening, which can be achieved by configuring the minimal set of IIS features and roles as described in the *UMC Installation manual*.

For more information see the Federal Office for Information Security Web Site.

3.3.1.1 File System

This section describes file system security following the goals described in the System Hardening Overview section.

User Management Component has a predefined directory structure that is generated during installation. Folders, organized according to UMC needs, are configured with specific permissions during installation. These configurations are summarized below in User Management Component Access Control Table section.

In addition, to enhance the integrity of the file system, depending on customer security policies, it is possible to:

- encrypt the file system, using transparent file system encryption offered by the operating system;
- configure a white-listing software, for more information see Whitelisting.

User Management Component Access Control Table

The following tables list the product specific Windows Local Groups automatically configured during the installation for each system folder. It is not recommended to configure any additional groups or user permission on these folders. Additional details can be found in the User Account Management section.

Folder Path \ Windows Local Group	Administrators	UM Service Accounts	Users
%ProgramData%\Siemens\UserManagement\LOG	Full Control	Full Control	Read and execute
%ProgramData%\Siemens\UserManagement\DATA	Full Control (cannot write extended attributes)	Full Control	Read and execute
%ProgramData%\Siemens\UserManagement\CONF	Full Control	Full Control	Not accessible
%ProgramData%\Siemens\UserManagement\CERT\CHANNEL	Full Control	Full Control	Read and execute
%ProgramData%\Siemens\UserManagement\CERT\CHANNEL\UNTRUSTED	Full Control	Full Control	Read and execute
%ProgramData%\Siemens\UserManagement\CERT\TICKET	Full Control	Full Control	Read and execute
%ProgramData%\Siemens\UserManagement\CERT\TICKET\PRIVATE	Full Control	Full Control	Not accessible
%ProgramData%\Siemens\UserManagement\CERT\XCLIENT	Full Control	Full Control	Read and execute

Folder Path \ Windows Local Group	Administrators	UM Service Accounts	Users
%ProgramData%\Siemens\UserManagement\CERT\XCLIENT\PRIVATE	Full Control	Full Control	Not accessible
%ProgramData%\Siemens\UserManagement\CERT\SADS	Full Control	Full Control	Read and execute
%ProgramData%\Siemens\UserManagement\CERT\SADS\PUBLIC	Full Control	Full Control	Read and execute
%ProgramData%\Siemens\UserManagement\CERT\SADS\PRIVATE	Full Control	Full Control	Not accessible
%ProgramData%\Siemens\UserManagement\CERT\MACHINE	Full Control	Full Control	Read and execute
%ProgramData%\Siemens\UserManagement\CERT\MACHINE\PRIVATE	Full Control	Full Control	Not accessible
%ProgramData%\Siemens\UserManagement\CERT\NETWORK	Full Control	Full Control	Read and execute
%ProgramData%\Siemens\UserManagement\CERT\NETWORK\PRIVATE	Full Control	Full Control	Not accessible
%ProgramData%\Siemens\UserManagement\CERT\CLAIM	Full Control	Full Control	Read and execute
%ProgramData%\Siemens\UserManagement\CERT\CLAIM\HISTORY	Full Control	Full Control	Read and execute
%ProgramData%\Siemens\UserManagement\TEMP	Full Control	Full Control	Read and execute

Important:

The paths listed in the table above must be interpreted as follows:

- %ProgramData% and %ProgramFiles% are Windows environment variables;

3.3.1.2 Creating an Identity Provider Whitelist

Two types of whitelisting can be used to enhance the security of UMC;

- Whitelisting the programs to run on the machine using McAfee Whitelisting,
- Whitelisting host using the UMC functionality, which allows you to specify the hosts that can connect to identity providers to help protect the machine from potentially harmful connections.

Whitelisting a host allows them to:

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

If the host is not present in the list, the call is rejected. The service validation is always enabled and if the service is not validated, an error returns during the authentication phase. It is possible to insert the service, present in login request in the whitelist, automatically during the authentication phase. It can be done if you authenticate with **UMC administration user** and, if in the central configuration, the property "**enableWhitelist**" is set to **true** (see Identity Provider Configuration Management).

Procedure

1. Add each host to the whitelist by using the required **umconf** utility command as documented in the *Create Whitelist Entry* page of the *UMCONF User Manual.*
2. Restart the **UMCService** and then in IIS Manager recycle the Identity Provider application pool on each host.

3.3.1.3 Enabling Code Signing Check

Code signing certifies the code of an executable or script, so that it cannot be altered without the certificate being invalidated.

All UMC executable and dlls are code signed and associated to a certificate.

UMC provides a security measure that checks if its executables are signed when the services start and creates a log file with the list of errors found during the check. This functionality is disabled by default.

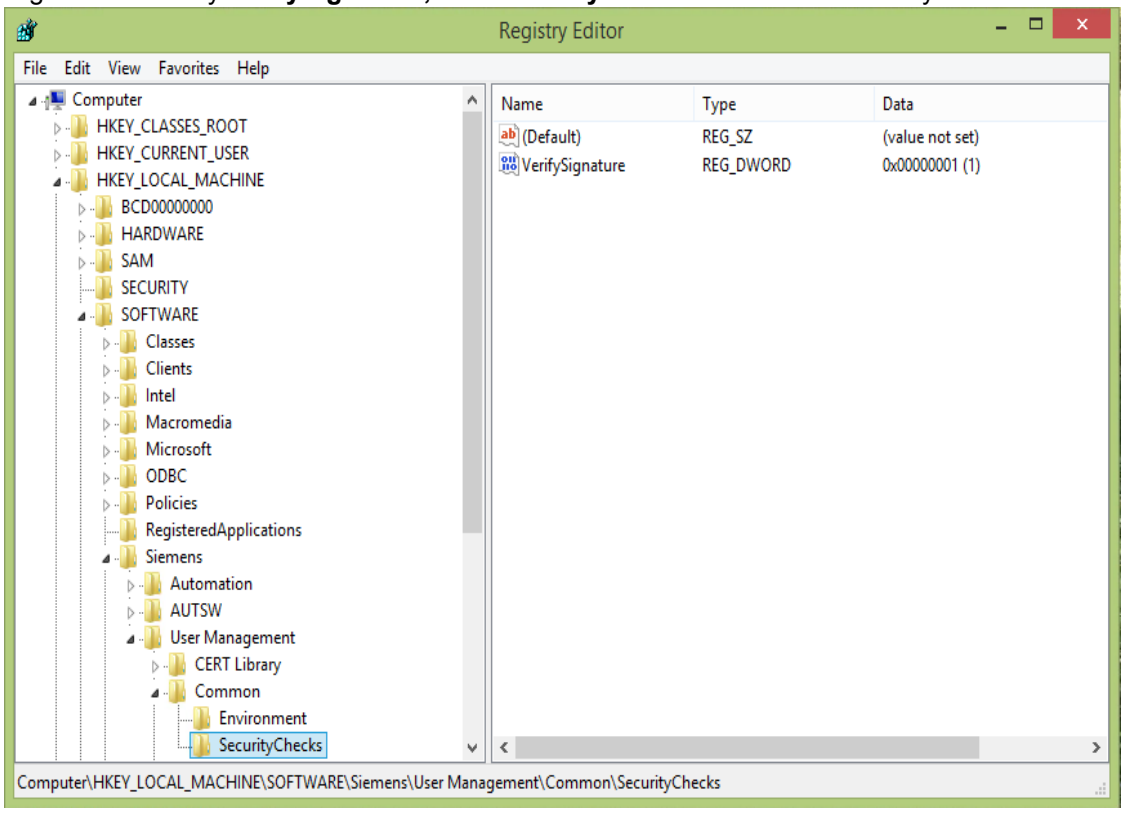
Note:

- The operating system may need to use the internet connection to verify the validity of the signature.
- in order to enforce this security check the following procedure must be performed on every machine on which UMC is installed.

Procedure

1. In Registry Editor go to: **HKEY_LOCAL_MACHINE > SOFTWARE > SIEMENS >User Management > Common**
2. Right-click **Common,** select **New** > **Key,** and insert **SecurityChecks** in the name.
3. Select the **SecurityChecks** key, right-click anywhere in the right panel and click **New,** then select **DWORD**.
4. Insert the name **VerifySignature**.

5. Right-click the key **VerifySignature,** select **Modify** and set the value of the key to 1.



3.3.1.4 Decommisioning UMC Machines

If a UMC installation is no longer required the machine should be decommissioned in order to reduce entry points during an attack.

In order to decommission a UMC machine follow the uninstall procedure in *How to Uninstall UMC* in the *User Management Component Installation Manual.*

3.3.2 Whitelisting

UMC has been tested using McAfee Application Control 6.1.3 as a whitelisting application. McAfee Application Control can be administered in different ways:

- Locally on a computer system (standalone)
- Centrally using McAfee ePolicy Orchestrator (ePO)

User Management Component has been tested using a local administration configuration, which can be handled exclusively by means of command line input. The commands are intelligible and self-explanatory and McAfee provides excellent reference material. McAfee Application Control can be easily handled using batch files or scripts.

In both cases, once McAfee Application Control has been installed on the computer, you first need to run the solidify function on all local hard disks and partitions, that scans all connected drives to detect the presence of executable files. After the execution of the solidify function:

- only the programs found can be executed in the future;

- all executables found during the scan are protected against manipulation (renaming, deletion, etc.) and new files cannot be executed.

The duration of the execution of the solidify function depends on the volume of data and on computer performance and may take several hours.

3.3.2.1 Executing McAfee Solidify Function

You should follow the instructions below during integration of the McAfee Application Control, or prior to its installation. Performing this procedure, all components signed by selected certificates can make changes to the binaries on the system and launch new applications.

Prerequisites

You must have the Siemens certificate which is associated to the binary files (e.g. .exe, .dll) , that are installed by the UMC installer in the **bin** folder. If you have not already retrieved the Siemens certificate see, Obtaining the Siemens Certificate.

Procedure

1. Install and configure the operating system.
2. Install all necessary programs and components.
3. Install all security updates that are available for the operating system and programs.
4. Install a virus scanner and update it with the latest virus signature files.
5. Set up the system architecture according to the recommendations based on the UMC *Installation Manual* and *Security Concept Manual* in order to keep malware risks to the absolute minimum prior and during integration of McAfee Application Control.
6. You should disconnect the machine from external / third-party networks (e.g. at the frontend Firewall).
7. Run a complete virus scan on the machine.
8. Install the McAfee Application Control locally.
9. Open the McAfee Application Control command line (**Start** > **Programs** > **McAfee** > **Solidifier** > **McAfee Solidifier Command Line**).
10. Start solidification by typing **sadmin solidify** or **sadminso** command, and wait for the process to complete.
11. Add Siemens UMC certificate as updaters using the command **sadmin cert add -u** "certificate".
12. Enable the configuration typing **sadmin enable** (The McAfee Solidifier Control will be activated when the machine is rebooted).

Result

All partitions and local hard disks of the computer system are now scanned for the presence of executable files (applications), e.g. exe, com, bat, dll, as well as Java, Active-X control elements, and scripts. The McAfee Application Control then signs and authorizes all files found during the scan for future use. It also protects the files against manipulation such as deletion, or renaming. On successful completion of the "solidification" process, the Solidifier command line reports the number of files scanned per partition or hard disk, including the number of files that have been authorized. After the restart, you can query the status of McAfee Solidifier by entering the **sadmin status** command in the Solidifier command line.

Obtaining the Siemens Certificate

All the binary files (e.g. .exe, .dll) , that are installed by the UMC installer in the **bin** folder, are associated with the Siemens certificate. You can retrieve the certificate from one of these files according to the following procedure.

Procedure

1. In the User Management Component **bin** folder, select a **.exe** (or another binary file).
2. Right click and select **Properties**.
3. Select the **Digital Signatures** tab.
4. Select the certificate **SIEMENS** and click on the **Details** button.
5. Click on **View Certificate** button and select the **Details** panel.
6. Click on **Copy to File** button and select **Base-64 encoded X.509 (.CER)** option.
7. Save the file in **..\Program Files\McAfee\Solidcore\Certificates**.

3.3.3 Disaster Recovery

If a security incident, such as a malware infection, occurs or a storage device fails (hard disk crash), regular creation of backups is absolutely necessary in order to purge the automation system and thereby re-establish the smooth and trouble-free operation as quickly as possible.

System Backup

A system backup stores data in the system partition. In the case of UMC this is necessary in order to save system data relative to UMC, like certificates and whitelisting.

This means that the volume is backed up with the following data

- Hardware-specific files (for example "Ntldr", "Boot.ini"),
- Windows operating system files,
- The installation of the operating system,
- The installation of all programs.

Database Backup

The UMC Database can be backed up by performing an Export Package, which saves UMC data: Users, Groups, Roles, Function Rights, see the *UMX User Manual* for more information.

Important:

Database backup is related to disaster recovery fall back strategies. Data loss prevention cannot be granted and is strictly related to the backup strategy (e.g. chosen interval for creating backups).

3.3.4 Security Controller

The Security Controller (SeCon) is a program, integrated by default in User Management Component installation, that configures application-specific security settings during installation.

SeCon can automatically configure the following settings:

- Group settings
- Registry settings
- Windows Firewall exceptions
- DCOM settings
- File and/or directory permissions settings

These settings are configured depending on the installation (package selection).

Security settings related to the UMC package

The settings required for UMC are group settings and file and/or directory permissions. Before UMC setup program performs the installation, the Security Controller dialog box appears displaying the system settings that the setup will make on the PC station. Group settings and file and/or directory permissions can be found at following link Windows Group Configuration. You can call up the Security Controller from **Windows Apps**, clicking **Siemens Automation** and then **Security Controller**. For more information refer to the Security Controller documentation.

Important:

When changing the plant configuration or changing the roles of users, be aware that local group memberships must be adapted accordingly. Settings must be reapplied if a change is made to the work environment.

3.3.5 Patch Management

In general, office PC systems are protected against malware and, any weak points that are discovered in the operating system or in the user software must be eliminated by installing updates and patches. Similarly industrial PCs and PC-based control systems in the plant network need corresponding protective measures.

Systems should be updated and patched regularly to address potential security risks and known exploits. To accomplish this, Microsoft removes security gaps in its products and provides these corrections to its customers via official updates/patches.

To enhance the security and stability of operations in the UMC solution, the installation of patches is recommended. Siemens will provide customer support only if these updates have been installed and only for problems that are unrelated to such updates.

You can find information on Microsoft updates and the Windows Server Update Services (WSUS) on the following Microsoft pages:

- http://technet.microsoft.com/en-us/
- http://www.microsoft.com/wsus

The support for implementing patch management in your system is available from the Industrial Security Services. You can find additional information and the corresponding contacts at the following address http://www.industry.siemens.com/topics/global/en/industrial-security.

3.3.6 Malware Detection and Prevention

This section focuses on protecting the automation system or the computers of the automation system against malicious software. Malicious software and malicious programs (*malware*) refer to computer programs that have been developed to execute undesirable and possible damaging functions. The following types are differentiated:

- computer viruses
- computer worms
- trojan horses
- and other potentially dangerous programs, for example:
  - backdoor
  - spyware
  - adware
  - scareware
  - grayware

A virus scanner or antivirus program is a software that detects, blocks and, if necessary, removes malware.

The use of a virus scanner on the computers of an automation plant must not interfere with the process mode of a plant. The following two examples illustrate the problems that can arise in an automation system through the use of a virus scanner:

- even when infected with malware, a computer may not be switched off by a virus scanner if this would then lead to a loss of control of the production system (e.g. for an OS server).
- a project file "infected" by malware (e.g. a database archive) may not be automatically moved to quarantine, blocked or deleted.

The virus scanner server is a computer which centrally manages virus scan clients, loads virus signature files (virus patterns) over the Internet from the virus scanner vendor and distributes them to the virus scanner clients. The virus scanner client is a computer that is checked for malware and managed by the virus scanner server. In accordance with the rules for dividing components into security cells, the virus scanner server must be singled out in a separate network (Perimeter network / DMZ). Although at the moment there are no known compatibility issues, current release officially only supports Trend Micro OfficeScan 10.6.

Virus Scanner - Configuration Example

In the configuration example (see Example: Network Configuration with Security Cells), the virus scanner is placed in the perimeter security cell.

3.3.7 User Account Management

We have seen that a concept of defense that confronts an attacker with several hurdles (defense-in-depth concept) is required to defend against the various threats and to achieve an appropriate level of protection. At the same time, however, this means that authorized personnel must also be restricted by some hurdles. In practice, there are normally different access rights or classes of rights. Specific users may only access specific parts of the system, devices or applications. Some users have administrator rights, others only have read or write access rights.

The management of user and operator permissions involves the assignment of permissions in the Windows environment (to execute UMC modules Windows users must be granted the permissions which belong to the appropriate UMC group) as well as the assignment of roles to users based on activities. These procedures are rigorously separated from each other, but both are strictly applied under the principle of minimum required rights.

The management of user accounts is achieved through:

- Assigning Least Privileges
- Windows Group Configuration
- Operator Authentication and Authorization
- Password Strength
- Physical Protection

3.3.7.1 Least Privileges

UMC come with a set of built in roles:

- The **Administrator** role is used to allow "root" privileges to a specific user. Use this role only for installation and disaster recovery purposes. In addition, use strong password policy for users associated with this role and revoke this role when not necessary. This role cannot be associated with a group. This role cannot be deleted and only users which have the **Administrator** role can modify other users with this role.
- The **UMC Admin** role is used to manage users, groups and all the other UMC entities.
- The **UMC Viewer** role is used to access the user management configuration without making modifications.

The lowest privileges should be used to administer UMC functionalities using operation accounts in order to perform administrative operations. In order to follow this principle, you could, for example, assign a specific UMC user to the UMC provisioning service (see the specific command in the *UMCONF User Manual*).

3.3.7.2 Windows Group Configuration

The strategy of role-based access control includes restriction to minimally required rights and functions for users, operators, devices, network and software components.
In accordance with the distributed management of users in groups of the ALP (Add User Account to Local Group and Assign Permission) principle recommended by Microsoft, local users must be grouped first so that the required permissions (folder, releases, etc.) can be assigned to these groups.

If management is performed centrally by a domain, the AGLP (Access Global Local Permission) principle should be observed. According to this principle, user accounts are initially assigned to the domain-global groups in the Active Directory. These groups are then assigned to local computer groups which, in turn, receive permissions to the objects.

The generation of UMC Windows groups and the configuration of file permissions is automatically performed during the UMC setup.

To check if all necessary configurations have been applied, see below.

UMC Windows Local Groups

User Management Component requires some specific Windows Local Groups to be present on the computers on which it runs.
These Windows Local Groups are used to:

- manage file system permissions on UMC folders;
- manage permissions on other Windows low level resources (kernel objects);

In this way, if certain Windows users must interact with UMC folders, or other protected resources, you can associate them to appropriate Windows Local Group(s), instead of configuring their access rights manually for each one. The following table provide all the details of the Windows Local Groups that are used by UMC.

Name	Description	Main application fields
Administrator	This group contains the local Administrators of the machine and must be used to configure UMC.	Configuring UMC.
UM Service Accounts	This group is designed to run the um services. This group can access the contents of come folders, see File System for the list of folders created by the setup and their access rights. *Members of this group should not be configured as interactive users for security reasons.*	Identities used to run services.
UM_USERS	For future use.	*For future use.*

3.3.7.3 Operator Authentication and Authorization

All MES/MOM, TIA, SCADA and PCS7 data and related functionalities must be exposed in a secure way. Systems or people that have to access the functionalities have to be authenticated and authorized. With authentication we mean that the system verifies the identity of the external system or the user that will access some functionalities. In the case of users, the typical user credentials are user name and password. The user accesses the system providing the credentials, if the authentication is successful, the user is granted access. This process must not be mistaken for authorization, which defines the actions that authenticated users/systems can perform in the system. A typical way to implement authorization is by defining groups and roles that summarize the rights a user can have for system resources.

Authentication

In enterprise environments there is the growing need to guarantee high interoperability among the different systems that are part of the enterprise itself, without neglecting important qualitative attributes such as security, which is the focus of this document. This excerpt from *A Guide to Claims-Based Identity and Access Control (2nd Edition)* at http://msdn.microsoft.com/en-us/library/hh446528.aspx illustrates that MES/MOM service applications (based on REST - REpresentational State Transfer) are typically consumed in a "session-less" flow and every request is an independent operation. No session cookies are handled within this type of communication because there is no concept of a sequence of operations. Typically, Web Services expect every request to present the necessary authentication details and treat them in two possible ways:

- **unauthorized requests** are rejected and cause a response with HTTP code 401 containing one or more WWW-Authenticate headers, each specifying the details of the required authorization scheme and realm. Clients have to analyze those headers to understand how to obtain a token to include in a valid request.
- **authorized requests** carry the authorization header containing the authentication token issued by the Identity Provider STS.

The User Management Component implements the functionalities of authentication and authorization.

Authorization

A user or a group can be associated to a set of permissions through the role object in order to be grant the permission to perform a set of operations on a collection of objects.

3.3.7.4 Password Strength

The following general recommendations should be applied:

- to maintain at least the default values for the password account policies or to make them more restrictive;
- to force the user to change the password at first login, if the password assigned to a new user does not satisfy the password account policies;
- to force the user to change the password, if the password has been reset and does not satisfy the password account policies;

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

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

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

In addition UMC provides the following user global account policy default values:

Field	Description	Default values
SL_PWD_MIN_LEN	Minimum password length (number of characters)	8
SL_PWD_MAX_LEN	Maximum password length (number of characters)	120
SL_PWD_MIN_LOW_CHAR	Minimum number of lower case characters allowed in the password	1
SL_PWD_MIN_UP_CHAR	Minimum number of upper case characters allowed in the password	1
SL_PWD_MIN_ALPHA_CHAR	Minimum number of alphanumeric characters allowed in the password	1
SL_PWD_MIN_NUM_CHAR	Minimum number of numeric characters allowed in the password	1
SL_PWD_MIN_OTHER_CHAR	Minimum number of special characters allowed in the password	0

3.3.7.5 Physical Protection

To ensure security levels in UMC, the primary prerequisite is that the target system that hosts the UMC Server be correctly configured. In particular, it is mandatory:

- Physical access to UMC servers must be prevented;
- to use the administrative account only for administrative operations;
- use a dedicated account for the UM Server launcher (this account must belong to the Windows Group **UM Service Accounts** created by UMC setup);
- Avoid directly modifying the files contained the folders used by the UM Server, listed below, they can only be modified using tools provided by UMC:
  – %ProgramData%\Siemens\UserManagement\CONF
  – %ProgramData%\Siemens\UserManagement\CERT

3.3.8 WebUI Redirect Validation

During a login request, UMC WebUI sends to the identity provider a parameter whose value is the address to which redirect the browser. To prevent the browser being redirected to malicious sites, validity checks have been implemented on this parameter format and content.

These checks monitor:

- the structure of the parameter (to be written as follows: https://hostname:port/path). This check is enabled by default and cannot be disabled.
- the hostname contained in the redirect parameter must be the same as the hostname used in the network request. This check is disabled by default, but can be enabled by performing the following procedure.

How to enable the check of the redirect URL

Manually add a register key named **ctx_host_check** under the register path: **HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\User Management\WebUI\Settings**. The regkey must be a DWORD variable, which values can be:

- **0**: the check is disabled.
- **1**: the check is enabled.

For scenarios in which UMC is installed behind a reverse proxy, do as follows:

Add a STRING type regkey called **reverseproxy** under the register path: **HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\User Management\WebUI\Settings**. It must contain the address of reverse proxy used in the configuration (to be written as follows: https://hostname:port). This address must be provided to UMC because in this scenario the address that comes with the network request is not the reverse proxy address but the internal machine one, which of course does not match with redirect parameter.

4 Definitions and Abbreviations

Abbreviation/Acronym	Explanation
UMC	User Management Component
MES/MOM	Manufacturing Execution System/ Manufacturing Operation Management
IDP	Identity Provider
DMZ	Demilitarized Zone