GE VERNOVA

DIGITAL

PROFICY CIMPLICITY HMI/SCADA

Secure Deployment Guide
Version 4.0

GE VERNOVA

Proprietary Notice

The information contained in this publication is believed to be accurate and reliable. However, General Electric Company assumes no responsibilities for any errors, omissions or inaccuracies. Information contained in the publication is subject to change without notice.

Trademark Notices

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company.

Microsoft® is a registered trademark of Microsoft Corporation, in the United States and/or other countries.

All other trademarks are the property of their respective owners.

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:
doc@ge.com

Table of Contents

1. CIMPLICITY Overview

GE CIMPLICITY HMI/SCADA is a versatile software application that is scalable from a Human Machine Interface (HMI) to a fully networked Supervisory Control and Data Acquisition (SCADA) system. CIMPLICITY HMI/SCADA can be run on a single server or in a variety of client/server architectures (see the section Sample Reference Architectures).

This *Secure Deployment Guide* describes the optimal security architecture and configuration for the CIMPLICITY Server, CIMPLICITY Clients, and the communication between the CIMPLICITY Server and other components. Some security guidance is applicable to all CIMPLICITY Server installations and other security recommendations should be evaluated based on the size, complexity, and criticality of the process being monitored and controlled.

NOTE: This document is not a replacement for GE installation and other reference documents which may include more detailed information about security features that are outlined in this document. Additionally, users are encouraged to visit the Support Site for current versions of this document. Visit https://digitalsupport.ge.com/communities/CC_Home.

1.1. Cybersecurity Overview

1.1.1. Sensitive Data

CIMPLICITY involves the management of sensitive data at many levels. A comprehensive training plan for all users, including employees and subcontractors, addresses the protection of sensitive data. It is recommended that users track participants of such a training program for audit purposes.

1.1.2. Security Protections

Cybersecurity requires a robust and ongoing process to ensure steps are continually being taken to protect assets. It is recommended that ongoing assessments, testing and other security measures be built into CIMPLICITY's deployment. Examples may include vulnerability scanning, penetration testing, robustness testing, and white/gray/black box testing.

CIMPLICITY undergoes a rigorous process itself but because CIMPLICITY supports multiple use cases, users must evaluate and incorporate cybersecurity protections for each application on a case-by-case basis.

2. Sample Reference Architectures

The CIMPLICITY Server supports a wide variety of industry sectors, types of Industrial Control Systems (ICS), and organizational models. The appropriate architecture for an installation varies based on these and other factors. This section provides five sample reference architectures along with an explanation of the security benefits and applicability of the architectural choices.

Use these five sample architectures as guidance to design an appropriate architecture for an ICS. The appropriate architecture may be a variant of these five samples based on an organization's operational needs and risk management decisions.

Hardware or protocols that allow for the mutual authentication of end points is recommended so that data coming from servers and requests from clients can be trusted. CIMPLICITY supports the OPC Unified Architecture (OPC UA) protocol that provides mutual authentication and data encryption.

The Control System Zone provides the highest level of trust. Each zone extending from this zone is a lower level of trust with the Corporate Zone being the least trusted level. In descending order, the network segment with the highest level of trust to the lowest level of trust is as follows:

- **Control System Zone**
- **Control System DMZ**
- **Support DMZ**
- **Corporate Zone**

Always limit the connections that originate in a lower trust zone and connect to a higher trust zone. These connections could be governed by a whitelist. The more trusted zones should originate communication to lower trust zones wherever possible. For example, a process in the Control System Zone could query the orders of the day from the Corporate Zone, as shown in Figure 4.

2.1 Single Computer Solution in the Control System Zone

A single computer can be both the CIMPLICITY Server and the CIMPLICITY Client used as the HMI by an operator (see Figure 1). This architecture is recommended for small installations that have only a single operator or engineer requiring access to monitor and control the process.

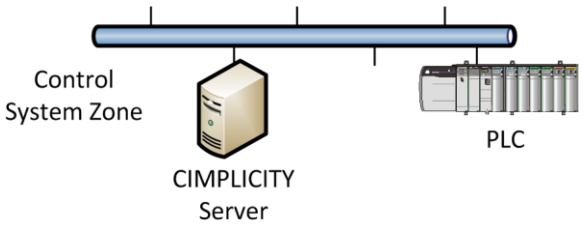


Figure 1 Single Computer Architecture

The CIMPLICITY Server application communicates with programmable logic controllers (PLCs) and other controllers in an ICS.

Place this single computer in a Control System Zone that is isolated from the Corporate Zone, internet, and all less-trusted zones by a firewall or air gap (that is, no communication path available between the Control System Zone and other networks).

2.2 Server, Client, and Supporting Components in the Control System Zone

A typical CIMPLICITY HMI/SCADA deployment includes a CIMPLICITY Server and multiple CIMPLICITY Clients. It may also include additional components in the CIMPLICITY solution (see Figure 2). This reference architecture keeps all CIMPLICITY communication to and from the CIMPLICITY Server on the Control System Zone protected by a firewall.

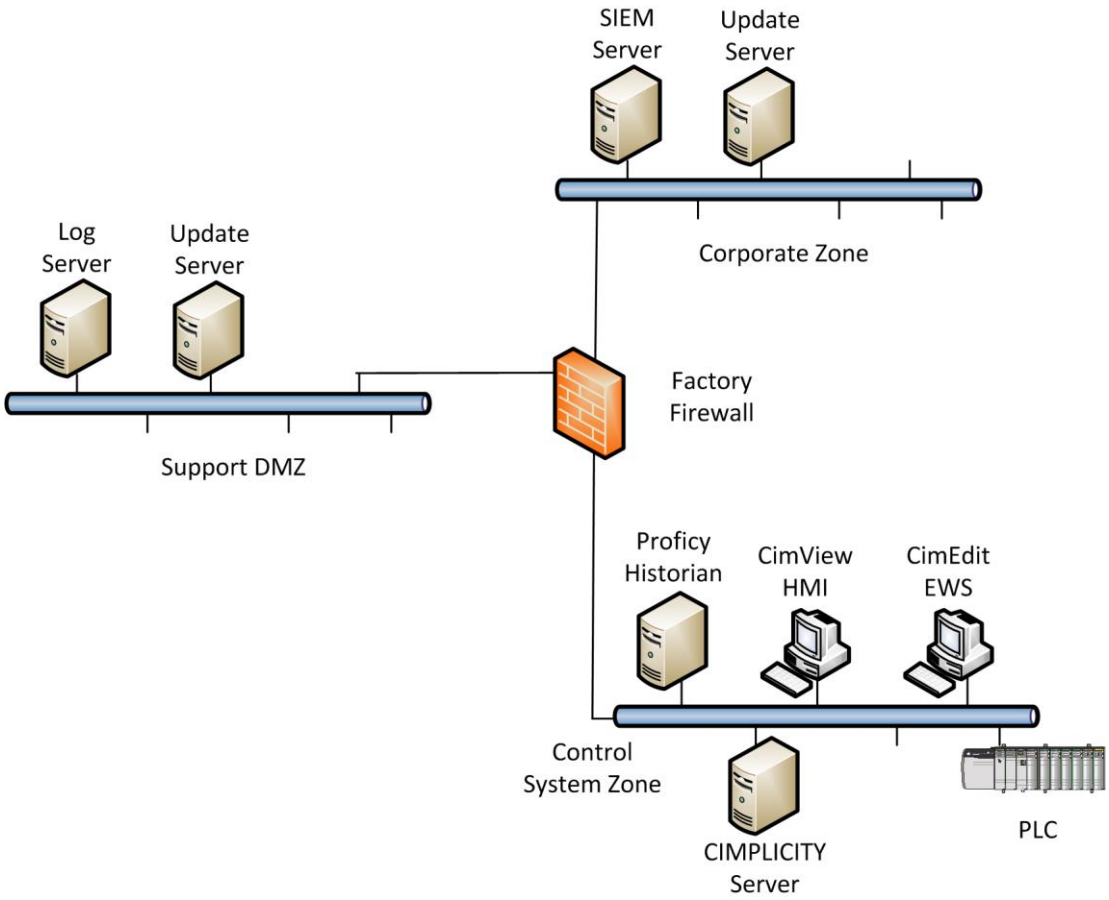


Figure 2 Control System Zone Only Solution

A semi-trusted Support De-Militarized Zone (DMZ) is introduced in this architecture for cyber-maintenance of the increased number of computers and network infrastructure. Such maintenance may include bringing security patches, anti-virus signatures, and other software updates into the Control System Zone.

Best security practices for Support DMZ include:

- Implementing a least privilege firewall ruleset by limiting each rule to the minimum set of source IP addresses, destination IP addresses, and destination TCP (Transmission Control Protocol)/UDP (User Datagram Protocol) ports required for the rule.
- Selecting support methods or protocols that use TCP, rather than UDP, and a minimal number of ports when possible. UDP is more easily spoofed because there is no initial handshake. The ideal protocol uses a single TCP port to provide the support or update service.
- Initiating the TCP communication from the more trusted zone. In other words, the computer in the more trusted zone pulls the updates from the less trusted zone. In Figure 2, the Update Server in the Support DMZ initiates a TCP session with a computer in the Corporate Zone to pull updates. Similarly, the CIMPLICITY Server in the Control System Zone initiates a TCP session with the Update Server in the Support DMZ to retrieve the updates.

The second purpose of the Support DMZ is to support network and security monitoring in the Control System Zone. Many organizations have developed a monitoring and incident response (IR) capability. An Incident Response team exercising this capability should operate within the Corporate Zone. This IR capability and IR team may be leveraged to monitor the ICS but it primarily needed to send log files to the Corporate Zone.

Figure 2 shows a Log Server with the role to receive log files from the Control System Zone and forward them to the Corporate Zone. These log files could be syslog files from switches, routers, firewalls or servers, alerts from anti-virus or intrusion detection systems (IDS), alerts from PLCs, sensors, and anything else that can send a message in the network.

The best security practice for this communication is similar to the practices previously listed. Initiate the TCP session on the more trusted zone and use a minimum number of ports (preferably one). The difference with this type of communication is that the logs and alerts are pushed out from the Control System Zone to Support DMZ and then to the Corporate Zone rather than pulled as described above when discussing updates.

2.3 Historical Data and Alarms on Semi-Trusted Control System DMZ

The third reference architecture adds the sharing of control system data with networks and systems outside the Control System Zone. Sharing historical control system data with systems in the Corporate Zone is the most common case. However, data may be shared with a cloud for big data analysis, mobile devices for alarm monitoring or key performance indicators, external organizations for maintenance and efficiency purposes, as well as a variety of other cases. The general industry trend is to share more control system data with outside systems and find ways to extract information and value from this data.

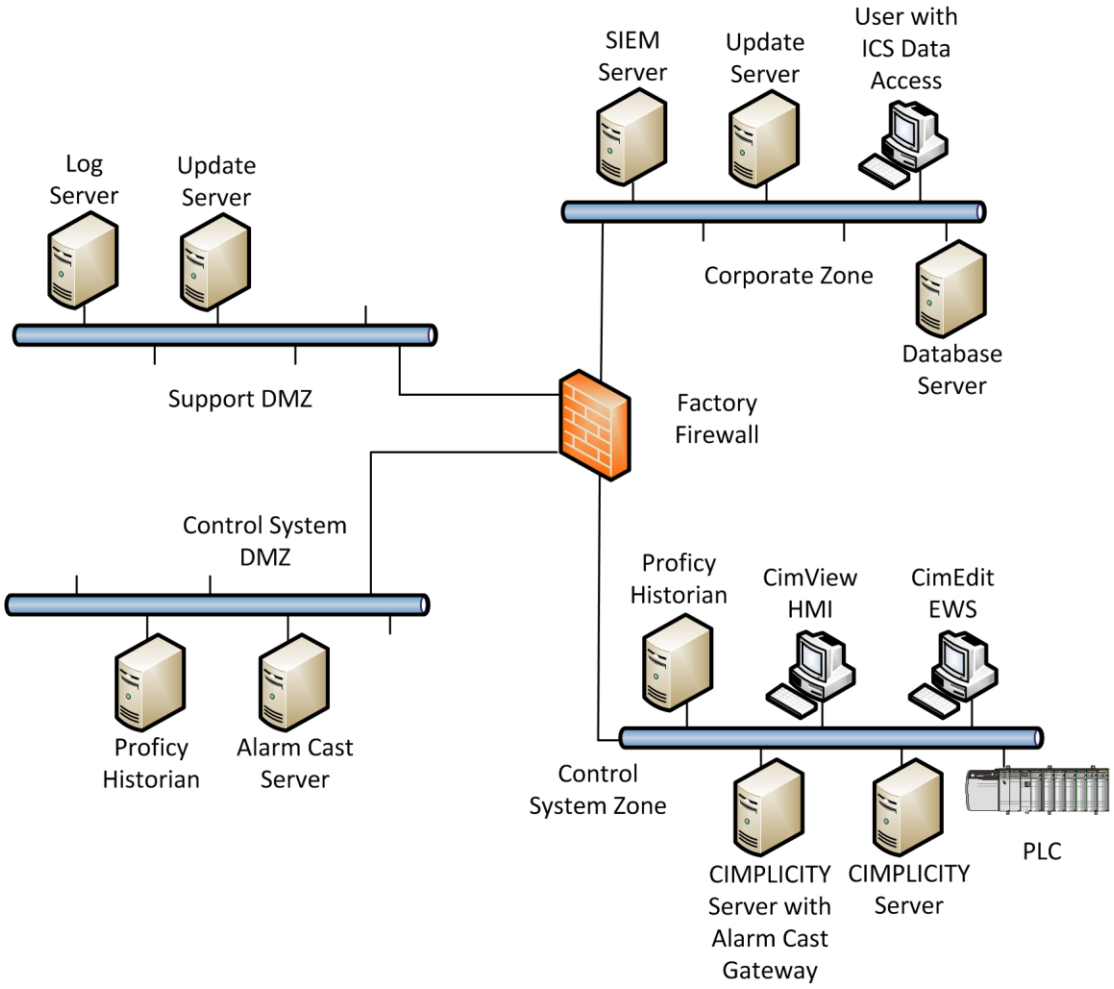


Figure 3 Control System DMZ Zone

Figure 3 shows the addition of a Control System DMZ to the Figure 2 architecture. Many organizations combine the Control System DMZ and Support DMZ into a single DMZ but by separating them, security advantages can be gained:

- The community of systems and users that requires access to these DMZs can vary greatly. Often, the number of users in the Corporate Zone that require access to the Control System DMZ can be large. Some organizations let all users access historical ICS data on the Control System DMZ. The computers in the Support DMZ typically communicate with a very small number of servers in the Corporate Zone. Separating the two DMZs eliminates the risk of attackers with access to the Control System DMZ being able to access the Support DMZ.
- The Support DMZ may require more TCP ports with more administrative purposes allowed through the firewall. This is a different attack surface than is commonly required in the Control System DMZ. By separating the two DMZs, the attack surface of each DMZ is reduced.
- It is easier to physically disconnect each DMZ to address an immediate threat without removing services from devices or services not at risk to the threat.

The cost of an additional DMZ is minimal (an additional network switch) given that most firewalls have four or more network ports. However, the implementation of a secure security practice firewall ruleset has a much greater impact on risk reduction than deploying a separate Control System DMZ for pushing control system data to the Corporate Zone. A single DMZ combining computers in the Control System DMZ and Support DMZ (Figure 3) is the most common DMZ architecture in ICS and meets the security recommendations in most ICS security standards and guideline documents.

The Control System DMZ shows two common methods for sharing CIMPLICITY data and alerts with the Corporate Zone and other external zones:

GE Historian

GE Historian may exist in the Control System Zone to provide historical data to operators and engineers working on an ICS. An additional Historian can be deployed in the Control System DMZ to provide historical data to users and systems in the Corporate Zone and other external networks.

The historical data is pushed from the CIMPLICITY Server in the Control System Zone to Historian in the Control System DMZ.

This firewall rule supports this communication:

Source IP	Destination IP	Destination Port
CIMPLICITY Server	Historian in DMZ	TCP/14000

The historical information could be pushed from Historian in the Control System DMZ to a server in the Corporate Zone. The Corporate Zone server may be another Historian, SQL Database Server, or any server that supports a communication protocol available in Historian. The more common, but less secure, case has users and servers in the Corporate Zone accessing Historian in the Control System DMZ. In either case, a single destination port, TCP/14000, must be allowed through the firewall between Historian and the other permitted communicating computers.

Alarm Cast Server

GE's Alarm Cast Server provides alarms, primarily for support purposes, to a variety of third-party devices, such as mobile phones, pagers, serial modems, and direct connections. Since this communication is with a less trusted zone, often a mobile data network and Internet, communication must not occur directly between the Control System Zone and the less trusted zone.

The CIMPLICITY Server in the Control System Zone can be configured as an Alarm Cast Gateway that pushes configured alarms to an Alarm Cast Server located in the Control System DMZ.

This firewall rule allows this communication:

Source IP	**Destination IP**	**Destination Port**
CIMPLICITY Server	Alarm Cast Server in DMZ	TCP/8070-8089

The firewall must be configured with rules that enable the required communication between the Alarm Cast Server and the intermediate or end systems receiving the alarms. Configure these rules in a least privilege manner.

For example, if the Alarm Cast Server is forwarding messages via e-mail, use this firewall rule:

Source IP	**Destination IP**	**Destination Port**
Alarm Cast Server in DMZ	Mail Server in Corporate Zone	TCP/25 (SMTP)

2.4 Remote Access to CIMPLICITY Screens Using WebSpace

Section Historical Data and Alarms on Semi-Trusted Control System DMZ provides control of system historical data and alarms to users and applications outside the Control System Zone. The risk of this data-sharing approach is minimized by the architecture and the fact that a user or application in a less trusted zone does not have access to a CIMPLICITY Server that could perform control functions.

CIMPLICITY is a versatile product and offers other methods to view control system information and perform remote control, as explained in this section and in section Emergency Remote Access for Control and Administration. These methods introduce additional risk that is partially mitigated by additional controls, and these risks and mitigations should be considered in the Design Phase of any CIMPLICITY project.

Some organizations want the ability to view the same screens as an operator or engineer in the Control System Zone from the Corporate Zone or some other less trusted zone. CIMPLICITY's WebSpace functionality makes this easy to deploy and offers important security controls. See Figure 4 for such a configuration.

The Webspace Plug-in for Operations Hub provides similar functionality with similar security concerns as Webspace access. All of the guidance around Webspace deployment applies to the Webspace Plug-in for Operations Hub deployment as well.

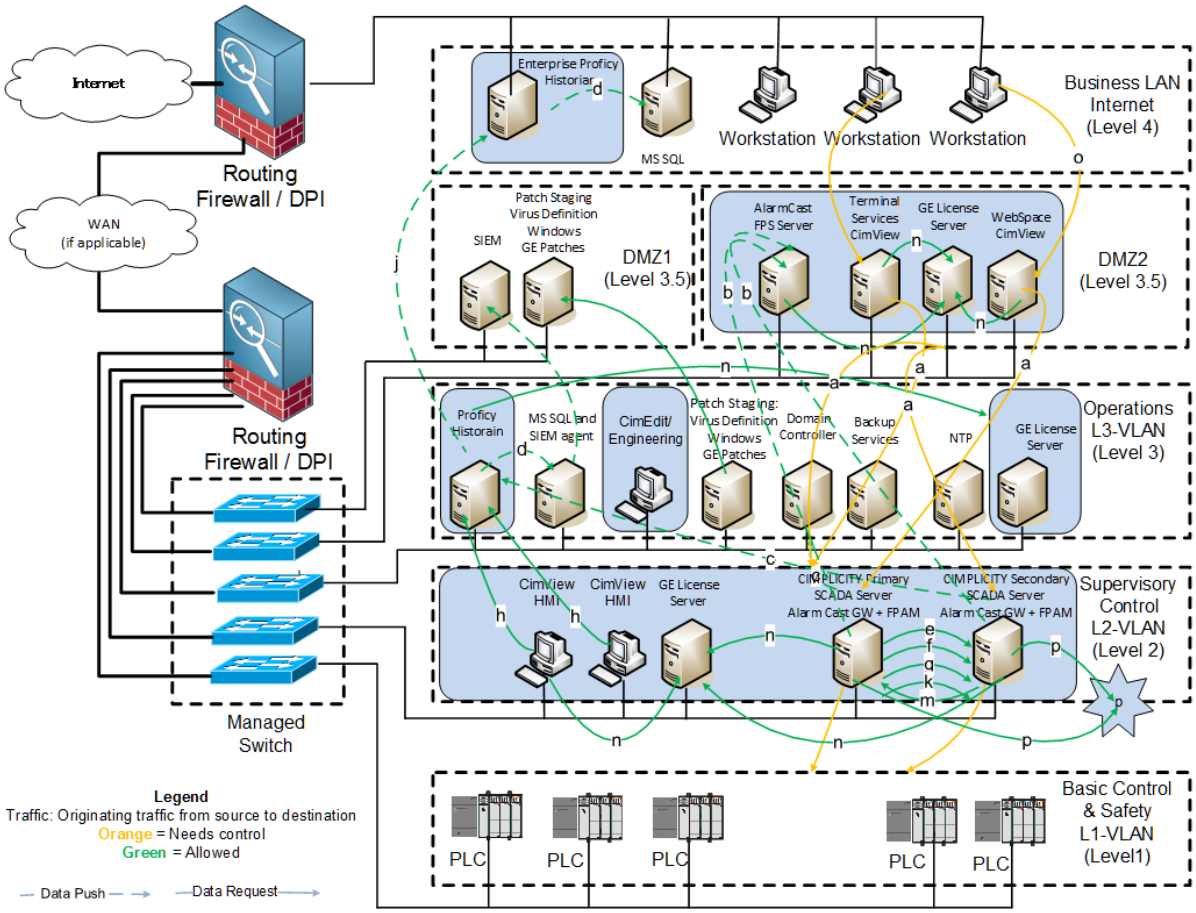


Figure 4 Remote Access to CIMPLICITY Screens with WebSpace Solution and Terminal Services Solution

When adhering to Figure 4 configuration, the first control to build is to prevent a user in the Corporate Zone from accessing a CIMPLICITY Server in the Control System Zone. By placing a second CIMPLICITY Server, the WebSpace Server, in the Control System DMZ, users only need to access the Control System DMZ rather than the Control System Zone.

The WebSpace Server in the Control System DMZ is running CimView and communicates with a CIMPLICITY Server in the Control System Zone using CIMPLICITY client/server networking. The CIMPLICITY option for secure sockets is set for this connection (see section Computer). The firewall rules required to support this architecture that allows the following communication between the WebSpace Server and the CIMPLICITY Server include:

Source IP	Destination IP	Destination Port
WebSpace Server	CIMPLICITY Server	TCP/32000, 32256, 32512, 32768
CIMPLICITY Server	WebSpace Server	UDP/32000

In the Figure 4 configuration, the second control pertains to the CIMPLICITY Server and WebSpace configuration, which is explained in sections Securing the CIMPLICITY Server and WebSpace . This control adheres to these basic principles:

- Use the CIMPLICITY Server security controls to limit WebSpace users to monitoring capability only. Do not allow control capability from outside the Control System Zone.
- Secure the communication between the web client and the WebSpace application.
- Secure the communication between the CIMPLICITY Server in the Control System Zone and the CIMPLICITY Server in the Control System DMZ.
- Limit the data access from the CIMPLICITY Server/WebSpace in the Control System DMZ to what is required in the Corporate Zone or another external zone. It is likely unnecessary to make all points and information accessible outside of the Control System Zone.

Want to Know More?

Search “Installing WebSpace”, “Configuration Guidelines” and “Terminating Sessions” in the *WebSpace User Guide.*

2.5 Emergency Remote Access for Control and Administration

Section Remote Access to CIMPLICITY Screens Using WebSpace provides the recommendation to keep complete control and administration within the Control System Zone. However, in emergency situations, remote key support personnel and administrators may require control outside the Control System Zone. Some organizations allow regular remote access for control and administration purposes to save support costs. The type and frequency of remote access for control and administration is a risk decision that each organization must make.

Some users find it advantageous to have secure remote access capability for control and administration available so an insecure method is not cobbled together when needed in an emergency. The WebSpace solution described in this section could be used for remote control of the process and remote administration of the CIMPLICITY applications. This is accomplished by modifying the user permissions for those users who require remote control.

Another approach is to deploy a Terminal Server in a DMZ. This Terminal Server must have CIMPLICITY installed for remote control of the process and remote administration of CIMPLICITY applications. In this case, remote desktop (RDP) is enabled on certain key machines in the Control System Zone and a firewall allows remote desktop connections into the Control System Zone from designated machines through an authentication process.

Some organizations with experience and a support capability for Terminal Services prefer using a Terminal Server rather than WebSpace to provide view-only capability to users in the Corporate Zone or other less trusted zones. In this case, view-only restrictions are configured and enforced by the CIMPLICITY Server.

If both a Control System DMZ and a Support DMZ are deployed, the decision about where to place the Terminal Server is based on the intended use of this server. If the Terminal Server is used by only a small number of highly privileged users who require remote control and administration, then it could be placed in the Support DMZ, as shown in Figure 4. If the Terminal Server is used by a larger population of users, it could be placed in the Control System DMZ.

CIMPLICITY requests dynamic ports and, when hardening the operating system (OS), restricting the range of client ports can support a more focused firewall configuration.

An essential step to protect a system is to terminate all remote access connections.

Table 1 Data Flow Connection Descriptions

This table explains the data flow connections shown in Figure 4.

Flow	Description	Origination	Destination	Destination Port *= default (configurable)	Encryption Protocol
a	View to Server connection	CIMPLICITY Viewer	CIMPLICITY Server	TCP/IP 32000	IP-SEC
b	Alarm cast FPAM to FPS server. Requires Alarmcast enterprise license.	Alarm cast FPAM	Alarm cast FPS Server	TCP/IP *8003	IP-SEC
c	Historian collector to Archiver	Historian collector	Historian Archiver	TCP/IP 14000	IP-SEC
d	Historian Archiver to SQL	Historian Archiver	SQL Server for alarm storage	TCP/IP *1433	TLS 1.2
e	Point manager synchronization	Primary CIMPLICITY Server	Secondary CIMPLICITY Server	TCP/IP 49152-65535+	IP-SEC
f	Alarm manager synchronization	Primary CIMPLICITY Server	Secondary CIMPLICITY Server	TCP/IP 49152-65535+	IP-SEC
g	User registration manager synchronization	Primary CIMPLICITY Server	Secondary CIMPLICITY Server	TCP/IP 49152-65535+	IP-SEC
h	Reading Historian Data	CIMPLICITY Viewer	Historian Archiver	TCP/IP 14000	IP-SEC

Flow	Description	Origination	Destination	Destination Port *= default (configurable)	Encryption Protocol
j	Historian to Historian collection	L3 Historian	L4 Historian	TCP/IP 14000	IP-SEC
k	Router ping for redundancy	Primary CIMPLICITY Server	Secondary CIMPLICITY Server	TCP/IP *4000	IP-SEC
m	Router ping for redundancy	Secondary CIMPLICITY Server	Primary CIMPLICITY Server	TCP/IP *4000	IP-SEC
n	License Server	Any License Client	GE License Server	TCP/IP 3333	IP-SEC
o	Webspace client to Webspace Server	Webspace Client	Webspace Server	TCP 491	SSL with 56-bit DES to 168-bit 3DES or 256-bit AES
p	Project Primary server identity broadcast	CIMPLICITY primary Server	Any CIMPLICITY Client	UDP 32000	IP-SEC
p	Web Server Port for CIMPLICITY web based configuration	any HTTP client	CIMPLICITY Configuration WebServer	TCP *9443	TLS 1.2
	CIMPLICITY OPC UA browse microservice on Primary server	CIMPLICITY Configuration WebServer	CIMPLICITY OPC UA browse microservice	TCP *4956	TLS 1.2
	CIMPLICITY configuration microservice on Primary server	CIMPLICITY Configuration WebServer	CIMPLICITY configuration microservice	TCP *4955	TLS 1.2
	Internal REST port for Webspace session manager service (new in 11.1)	CIMPLICITY Configuration WebServer	CIMPLICITY webspace-session-manager	TCP *4957	TLS 1.2
	Internal socket port for Webspace session manager service to CimView communication (new in 11.1)	CIMPLICITY CimView	CIMPLICITY webspace-session-manager	TCP *4958	TLS 1.2

Want to Know More?

- For information on Microsoft's terminal device commands for managing remote connections, go to https://technet.microsoft.com/en-us/library/jj215449(v=wps.630).aspx
- Windows dynamic port range is configurable as explained here; http://go.microsoft.com/fwlink/p/?linkid=158023
- Search "Terminating a Session" in the Webspace documentation.

3. Securing the CIMPLICITY Server

Many decisions made during the CIMPLICITY Server application installation and CIMPLICITY Project creation have a significant impact on the security of the CIMPLICITY solution. This section covers:

- Preparing the Windows Server platform before the CIMPLICITY Server installation
- Selecting secure options as part of the CIMPLICITY Server installation
- Setting the available security options during Project creation and initial configuration

3.1 Securing the Operating System (OS) Platform

The CIMPLICITY Server can be installed on a variety of Microsoft Windows operating systems. It is a good security practice to always run software that has had security patches and other operating system support fixes provided by Microsoft and applied by the owner/operator as part of a cyber maintenance program. Deploying the CIMPLICITY Server on the latest supported version of the Microsoft OS provides the greatest period before the OS needs upgrading. At the time that this *Secure Deployment Guide* was written, CIMPLICITY Server supports Windows Server 2012 R2. For a deeper examination of securing Windows Server 2012 R2, go to:
https://digitalsupport.ge.com/communities/en_US/Documentation/WINDOWS-HARDENING-GUIDE-and-RECOMMENDATIONS-WINDOWS-SERVER-2012-R2

Even though deploying the CIMPLICITY Server on the latest supported OS increases the lifetime before an OS upgrade is required, owners/operators must ensure that support exists within the organization for whatever OS is used in the deployment. Support capabilities may result in deploying CIMPLICITY on an older OS even with the knowledge that the lifetime is reduced until an OS upgrade.

3.1.1 Minimize Attack Surface

Every listening port, running service, and installed application offers the potential for a software vulnerability. Before installing the CIMPLICITY Server software, these security practices can help minimize the attack surface:

- Remove unnecessary software such as third-party applications, utilities and libraries
- Close listening TCP and UDP ports that are not needed
- Stop unnecessary running services
- Remove or disable user accounts that should not be using CIMPLICITY, including the Guest account.

Before installation, a baseline scan with the Nmap tool can assist with the reduction of attack surface by identifying open ports. The recommended command line for Nmap is as follows and should complete in approximately 30 to 45 minutes:

nmap -Pn -n -sS -sU --O -pU:0-65535,T:0-65535-v *<host IP address>*

Once complete, Nmap identifies open ports, and verification is needed that applications require all the open ports. Table 1 Data Flow Connection Descriptions lists the communication pathways, ports, and port ranges (in some cases, the default ports that are configurable).

It is recommended that Nmap be installed on a separate VMware image for temporary placement on each network requiring security scanning. The Nmap installer and instructions can be found at https://nmap.org/download.html

3.1.2 Secure, Hardened OS Configuration

Windows operating systems have hundreds of security settings. In recent years, Microsoft has configured the OS installation to be secure by default for most security configuration settings but many of these settings are still not in optimal secure status.

Microsoft provides guidance documents that represent the industry consensus for the optimal security configuration for each operating system, as well as Group Policy Objects (GPO) that make setting this optimal security configuration simple. Similar recommendations are also available from the Center for Internet Security, www.cisecurity.org and other organizations.

Review the screen saver settings in Windows to verify the “On resume, display login screen” is checked to ensure information is not visible. This prevents any unwanted actions.

Owners/operators must establish and implement a secure Windows OS configuration on the computer before installing the CIMPLICITY Server application.

The *Windows Hardening Recommendations - Windows 2012 R2* is available for users at https://digitalsupport.ge.com/communities/en_US/Documentation/WINDOWS-HARDENING-GUIDE-and-RECOMMENDATIONS-WINDOWS-SERVER-2012-R2

This document discusses the configuration changes that can be made to Windows to minimize the potential for attack. The information pertains specifically to hardening the operating system and can be applied to systems that contain components discussed in this solution.

The *Windows Hardening Guide and Recommendations – Windows 2012 R2* also includes guidance on securing communications in solutions laid out in Figure 4. The IP-SEC configuration instructions in the Windows hardening guide must be followed to protect the client-server communications from attackers with access to the network used for this communication.

3.1.3 Security Patching

Microsoft issues security patches monthly but it is important to note that most of the installation packages are missing recent security patches. Therefore, apply all security patches to the OS and other software before installing the CIMPLICITY Server application.

Security patches issued by GE can be found at https://ge-ip.force.com/communities/CC_Knowledge?contents=Service_Packs__c&product=CIMPLICITY__c

Installation instructions are included in the ReadMe file of each SIM.

3.1.3.1 Patch Installation Status

To see the status of all patches, view the installed SIMs via the CIMPLICITY Workbench > Help>About. The *About* box displays the product version number and all installed SIMs, as shown in Figure 5:

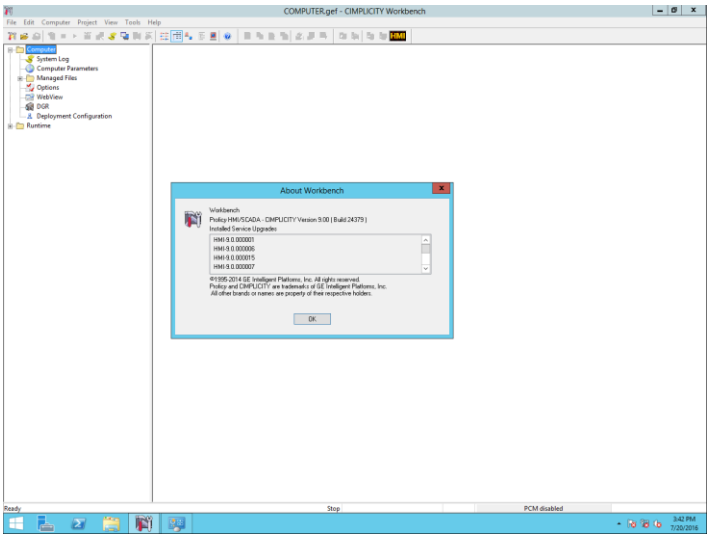


Figure 5 Viewing SIMs installed on CIMPLICITY

NOTE: CIMPLICITY patches are cumulative and installing the most current SIM ensures users have all available fixes.

3.1.4 Antivirus Software

Antivirus software does not stop custom malware or new malware that is not yet discovered by antivirus vendors. It does, however, stop mass market malware that is the most common cause of cyber security incidents in control systems.

Every modern Windows operating system includes a pre-installed security software known as Microsoft Defender(formerly known as Windows Defender). This integrated software functions as an antivirus and antimalware solution, with the primary purpose of safeguarding your computer against a wide array of malicious software forms, such as viruses, spyware, ransomware, and various types of malware. It's important to verify that Microsoft Defender is active, though it usually comes enabled by default.

To help ensure your Microsoft Defender detects the latest threats, get updates automatically as part of Windows Update.

At each SIM release for CIMPLICITY, product is tested with latest windows updates (therefore with latest version of Microsoft Defender). To know these details, visit the "Windows Defender Anti-Virus Details" section of the readme.chm file released with the SIM (refer below table). It is important to establish a system for processing immediate alerts and performing periodic reviews of routine updates, such as reviewing SIM releases every quarter.

Parameter	Last scan	Additional Information	
Virus & threat protection	21/08/2023 03:10	Last update	21/08/2023 15:55
		Security intelligence version	1.395.939.0
		Version created on	20/08/2023 21:52

Note: Anti-virus scans associated with file access can cause issues with the configuration and runtime performance of CIMPLICITY. To achieve optimal performance, exclude project folders and all their sub folders from anti-virus scans, in addition the data and log folders in the CIMPLICITY install should be excluded from anti-virus access scans.

Want to Know More?

- For information on turning on Microsoft Defender

  https://learn.microsoft.com/en-us/mem/intune/user-help/turn-on-defender-windows

- For information on updates to Microsoft Defender Security intelligence go to https://www.microsoft.com/en-us/wdsi/defenderupdates

3.2 Server Installation

The first step before installation is to ensure that the downloaded CIMPLICITY software is authentic. GE provides a MD5 hash file associated with each software download. Authenticate application software downloads by calculating the MD5 for each download and verifying it against the GE-provided hash.

The installation of the CIMPLICITY Server has this significant security option: *"Would you like to integrate this product with the Windows Firewall?"*

Selecting **yes** adds several CIMPLICITY applications to the Windows firewall rules (see Figure 6). Select this option if the CIMPLICITY Server is using the Windows firewall; otherwise, CIMPLICITY communication is blocked from reaching the CIMPLICITY Server application.

The exceptions added by the installation process do not restrict communication by source or destination IP address as a best security practice of least privilege recommends. Owners/operators requiring a high level of security, even in a trusted zone, must consider adding source and destination IP address restrictions to the CIMPLICITY exceptions. A properly configured firewall at the security perimeter restricts less-trusted zones from accessing the CIMPLICITY Server.

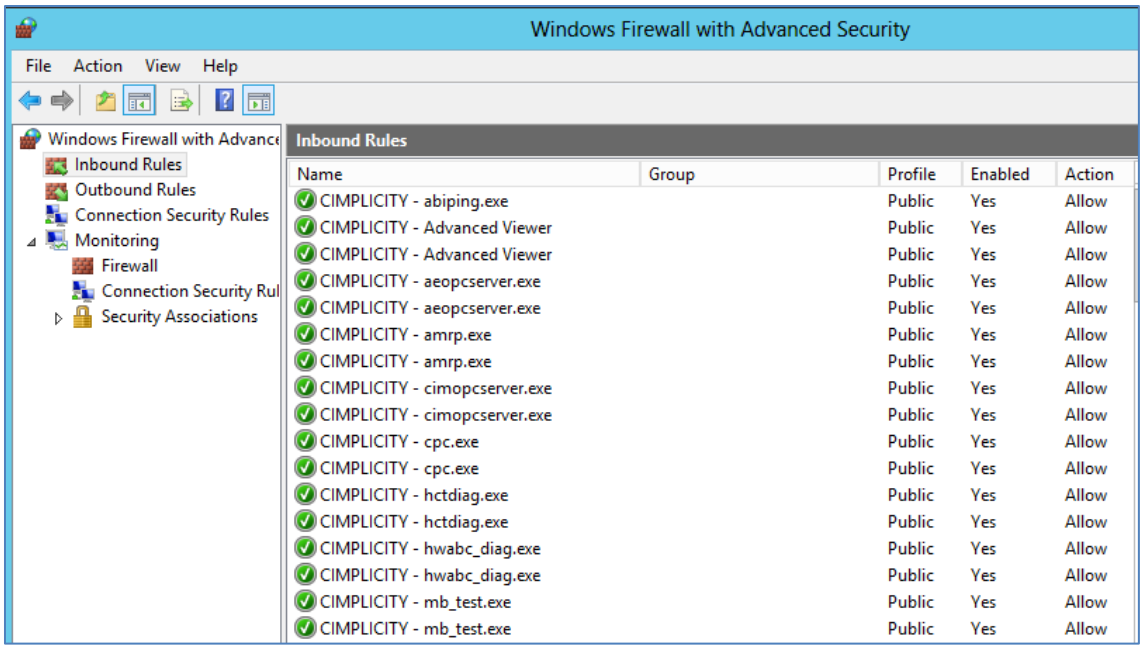


Figure 6 Integrating CIMPLICITY Server with the Windows Firewall

The CIMPLICITY Server also requires installing Microsoft's SQL Server database software. This database software must run in mixed mode authentication and is configured automatically when the CIMPLICITY installation process is used. CIMPLICITY Server applications use the default **sa** account to log in to the SQL Server database, but the installation process requires that the **sa** account password be set, as well as meet password complexity requirements (that is, a minimum of 8 characters with 3 characters being uppercase, lowercase, numerical, or a special character).

3.3 Server Redundancy

ICS owners/operators have recognized the importance and value of redundancy for many decades. A redundant CIMPLICITY Server can prevent a software, hardware, or network fault in the primary CIMPLICITY Server from causing a loss of ICS availability. Availability is an important security objective.

NOTE: Owners/operators must determine if the CIMPLICITY Server redundancy is required in the design phase of the project.

Only a subset of the PLC communication protocols supported by the CIMPLICITY Server support a redundant configuration. During the design phase, and before making a CIMPLICITY Server redundancy decision, review the list of supported protocols for redundancy.

CIMPLICITY Server supports both automatic redundancy and manual redundancy. Automatic redundancy is typically used for normal operational conditions when a primary CIMPLICITY Server outage is unplanned. The secondary CIMPLICITY Server becomes the active server when the primary CIMPLICITY Server is unavailable in the network. The secondary CIMPLICITY Server communicates with the PLCs, RTUs, and other field devices as well as populating the CimView screens when it becomes the active server.

A failover to the secondary CIMPLICITY Server is initiated through manual redundancy when the primary CIMPLICITY Server requires an outage for cyber maintenance or is in a repair state.

CIMPLICITY Server redundancy requires the creation of a Windows user account with the same user name and password on both the primary and secondary Windows servers. This configuration requires the following:

- Accounts in the Administrator group
- Two accounts in the same workgroup
- File and printer sharing and the Netlogin service in the Windows firewall
- File sharing and password-protected sharing
- Remote WinRM group in the Registry
- Remote Registry

Since these configuration changes make each CIMPLICITY Server more vulnerable, place these servers in the Control System Zone and possibly isolate them from other computers in this zone. Restrict the Windows firewall configuration changes by source IP and destination IP addresses.

Since the primary and secondary CIMPLICITY Servers in a redundant configuration are typically in the same zone for architectural and performance reasons, configuring firewall rules for required communication is not necessary. Review the following port information for a redundant relationship:

- REDUND_PROBE_PORT uses TCP/4000 to periodically verify the status of the primary and secondary CIMPLICITY Servers, which can be changed.
- TCP and UDP 32000 are required for Project announcements.
- TCP ports 32256, 32512 and 32768 are required for communicate between the primary and secondary CIMPLICITY Servers.
- Cabling redundancy requires the TCP port range of 5000-6000.
- Starting secondary happens via REST call, so requires port 9443 (Webserver port on secondary server).

3.4 Computer

There are a few important security settings configured for all Projects in the CIMPLICITY Server computer. The settings define the security controls for communication between clients and the CIMPLICITY Server, as well as CIMPLICITY Server to Historian communication. These settings are in the *CIMPLICITY Options* window (see Figure 7) that can be opened via Computer>Options>Properties. This tab requires a Windows user in the Administrator group. Right click on `startup.exe` and select **Run as Administrator** to perform this configuration. Most other configurations in CIMPLICITY are performed by a standard user. In general, only configurations impacting the Registry and accessible by all users require Administrative privileges.

Selecting the **Use secure sockets** check box in the *Startup Options* tab (see Figure 7) forces the use of low-level encryption to encrypt communications to and from the CIMPLICITY Server. The encryption algorithm is RC4 with a key length of 54-bits. This does not stop a sophisticated and motivated adversary from breaking the encryption, but it makes the communication appear as random data to anyone who can access the network or otherwise collect the CIMPLICITY Server communication. It is recommended to use the IPSec configuration outlined in the Windows Hardening guide for the CIMPLICITY communications.

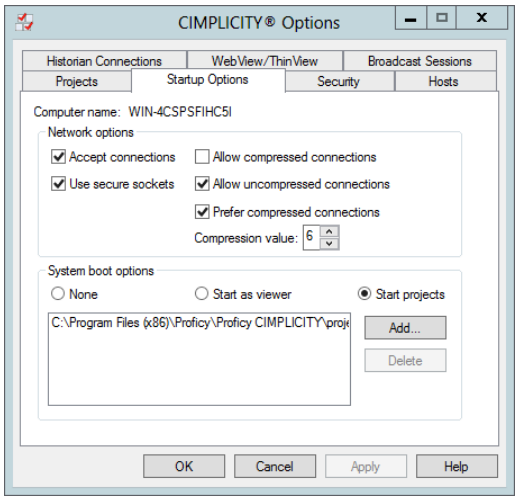


Figure 7 CIMPLICITY Options, Startup Options Tab

This privacy level of encryption is sufficient for the Control System Zone, but CIMPLICITY users may consider additional encryption for communication in a less trusted zone and where data confidentiality requirements are high.

The *Security* tab on *CIMPLICITY Options* (see Figure 8) allows configuration of the auto logout after a specific period of inactivity. Often, the appropriate auto logout configuration is determined by the computer's location:

- Typically, auto logout is not enabled on an operator's computer in a 24x7x365 manned control room. This computer is usually available at all times, and the physical security of the control room is relied upon to protect the computer when unattended.
- A computer in a plant or on a factory floor can be configured with auto logout to log out after a set period of inactivity and have another lower-privileged account configured to log in in its place to provide access to users with view-only privileges. This prevents an engineer or operator with highly privileged credentials from leaving a computer vulnerable while still allowing workers to view the status of processes.

  During the design phase and before commissioning, determine the appropriate settings for this security feature.

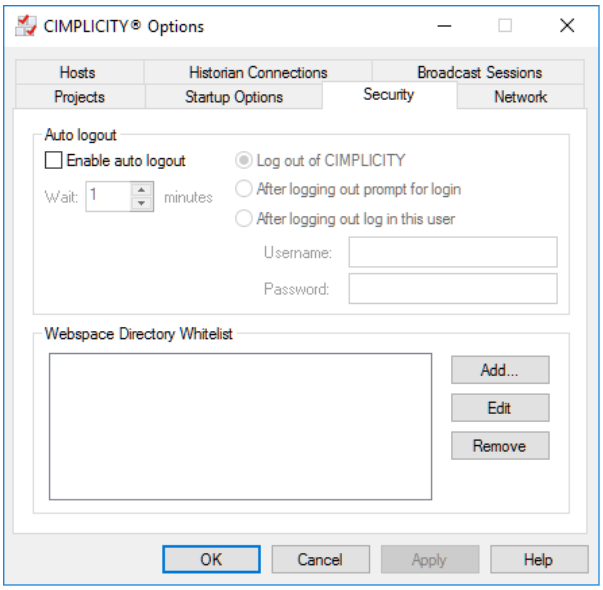


Figure 8 Auto Logout Feature, Security Tab

Configure connections to the Historian Server in the *Historian Connections* tab in *CIMPLICITY Options* (see Figure 9). This is where the user name and password provided by the Historian Administrator are entered to allow the CIMPLICITY Server to log in to Historian. The password must meet the password policy of the organization.

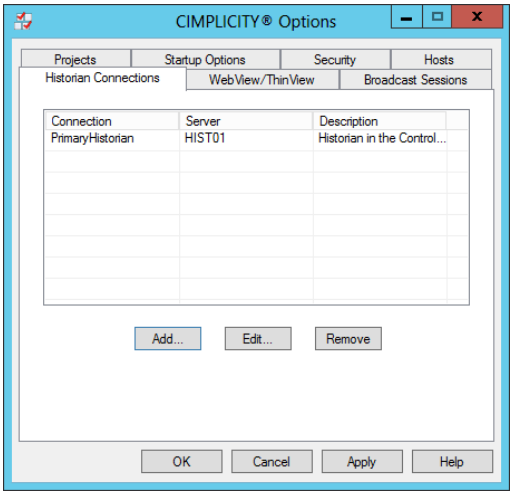


Figure 9 CIMPLICITY Options, Historian Connections Tab

3.5 Project

The CIMPLICITY operation is based upon Projects. A Project contains the configuration for the monitoring and control of an entire ICS or a subset of an ICS. CIMPLICITY supports multiple Projects to enable an owner/operator to decide whether to include the entire control system in a single Project or to divide it into multiple Projects based on the environment and system management approach.

The Workbench application in CIMPLICITY creates, modifies, and runs Projects. There are a few important security decisions to make when a Project is created in Workbench. Most of these selections can be changed after creating a Project through the settings in *Project Properties*.

The files in a CIMPLICITY project define how the project interacts with other ICS components and how the project itself behaves. To secure the system, the Windows permissions on each project folder and CIMPLICITY installation folder must be reviewed and updated. The System Administrator can change file permissions so that those Windows users who need to configure or access the different folders and files in the projects and the CIMPLICITY installation directory have the minimum access they need to perform their duties. Different users will require different levels of access to various files.

At a basic level, these users can be put into the following categories.

- **Admin:** users who change the system level configuration in CIMPLICITY and require administrator privileges on the local machine.
- **Configuration**: users who configure projects.
- **Operators**: users who use the CimView screens, and other CIMPLICITY runtime tools to view and interact with the plant process.
- **Runtime**: functional user under whom the CIMPLICITY services (see Table 2) should be configured to run as. This will also cause all the processes that execute for a CIMPLICITY project to run under this account user. This user needs to a direct member of the administrator's group.

Service name	Executable
CIMPLICITY	CIMPLICITY.exe
CIMPLICITY Advanced View	ptopc.exe
CIMPLICITY Broadcast Service	CIMBroadcastService.exe
CIMPLICITY Configuration Microservice	cim_config_service.exe

CIMPLICITY HTTPD Service	httpd.exe
CIMPLICITY OPC UA Browser Microservice	opcua_browse_service.exe

Table 2 list of CIMPLICITY services

See the appendix for a sample powershell script to set up the installation directory folder permissions and the projects' folder permissions.

Folder	**Require Read permissions**	**Require Modify permissions**
<project>\alarm_help	admin, configuration, runtime	admin, configuration, runtime
<project>\arc	admin, configuration, runtime	admin, configuration, runtime
<project>\data	admin, configuration, runtime	admin, configuration, runtime
<project>\lock	admin, configuration, runtime	admin, configuration, runtime
<project>\log	admin, configuration, runtime, operators	admin, configuration, runtime, operators
<project>\master	admin, configuration, runtime	admin, configuration, runtime
<project>\pki	admin, configuration, runtime	admin, configuration, runtime
<project>\RCO	admin, configuration, runtime	admin, configuration, runtime

Folder	Require Read permissions	Require Modify permissions
<project>\Recipes	admin, configuration, runtime	admin, configuration, runtime
<project>\screens	admin, configuration, operators	admin, configuration
<project>\scripts	admin, configuration, runtime	admin, configuration
<project>\SPC	admin, configuration, runtime	admin, configuration
<project>	admin, configuration, runtime, operators	admin, configuration
<project>\<project_name>.gef	admin, configuration, runtime, operators	admin, configuration, runtime
<CIMPLICITY install>\admin_data	admin, configuration, runtime, operators	admin
<CIMPLICITY install>\AEOPC	admin	admin
<CIMPLICITY install>\ALARMCAST	admin, configuration, runtime,	admin, configuration, runtime,
<CIMPLICITY install>\api	admin, configuration	admin,
<CIMPLICITY install>\arc	admin, configuration, runtime, operators	admin, configuration, runtime,
<CIMPLICITY install>\bsm_data	admin, configuration	admin, configuration

Folder	Require Read permissions	Require Modify permissions
<CIMPLICITY install>\cimpole	admin	admin
<CIMPLICITY install>\classes	admin, configuration	admin,
<CIMPLICITY install>\data	admin, configuration, runtime, operators	admin, Configuration, runtime
<CIMPLICITY install>\dc (and sub folders)	admin	admin
<CIMPLICITY install>\docs	admin, configuration	admin
<CIMPLICITY install>\Drivers (and sub folders)	admin	admin
<CIMPLICITY install>\etc	admin, configuration, runtime	admin, configuration
<CIMPLICITY install>\exe	admin, configuration, runtime, operators	admin
<CIMPLICITY install>\extras	admin, configuration	admin
<CIMPLICITY install>\firewall	admin, configuration	admin
<CIMPLICITY install>\fonts	admin	admin
<CIMPLICITY install>\GefVCR	admin	admin
<CIMPLICITY install>\lock	admin, configuration, runtime	admin, configuration, runtime
<CIMPLICITY install>\log	admin, configuration, runtime, operators	admin, configuration, runtime, operators

Folder	Require Read permissions	Require Modify permissions
<CIMPLICITY install>\mdac	admin, configuration, runtime, operators	admin
<CIMPLICITY install>\OpenSSL	admin, configuration, runtime	admin
<CIMPLICITY install>\perfserv	admin, configuration, runtime, operators	admin
<CIMPLICITY install>\projects (and sub folders)	admin	admin
<CIMPLICITY install>\PublishSubscribeDelivery (and sub folders)	admin	admin
<CIMPLICITY install>\report	admin	admin
<CIMPLICITY install>\ScadaConfigPki	admin, runtime	admin
<CIMPLICITY install>\scripts	admin, configuration, runtime	admin, configuration
<CIMPLICITY install>\Series90	admin, configuration, operators	admin, configuration
<CIMPLICITY install>\symbols	admin, configuration, operators	admin, configuration
<CIMPLICITY install>\SystemSentry	admin, configuration, operators	admin
<CIMPLICITY install>\uninstall	admin	admin

Folder	Require Read permissions	Require Modify permissions
<CIMPLICITY install>\WebPages	admin, configuration, runtime	admin, configuration
<CIMPLICITY install>\Web	admin, runtime	admin, runtime
<CIMPLICITY install> (this directory only)	admin, configuration	Admin
<CIMPLICITY install>\webspace-session-manager	admin, configuration, runtime, operators	admin. configuration

3.5.1 General Settings

The *General Settings* tab (see Figure 10) determines which optional application components (Options) and which protocols are enabled. If the Project uses a redundant CIMPLICITY Server for increased availability, check the **Server Redundancy check box** under *Options*.

The decision about protocols is often made before the deployment of the CIMPLICITY Server. The protocol selection is based on which protocols are required to communicate with PLCs, controllers, and other devices for monitoring and control. The CIMPLICITY Server does support the secure OPC UA protocol, as opposed to the less secure OPC classic protocol.

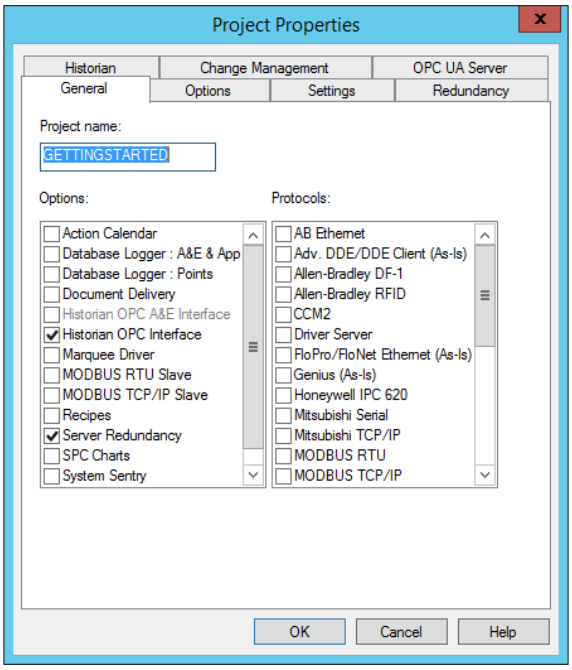


Figure 10 Selecting Server Redundancy and Protocols

3.5.2 Options

The most critical security settings for a CIMPLICITY Project are set in the *Options* tab (see Figure 11) of *Project Properties*, which appear during Project creation. Always check the **Configuration security** and **Start stop security** check boxes unless certain they are unneeded. By selecting these options, they become available during Project configuration.

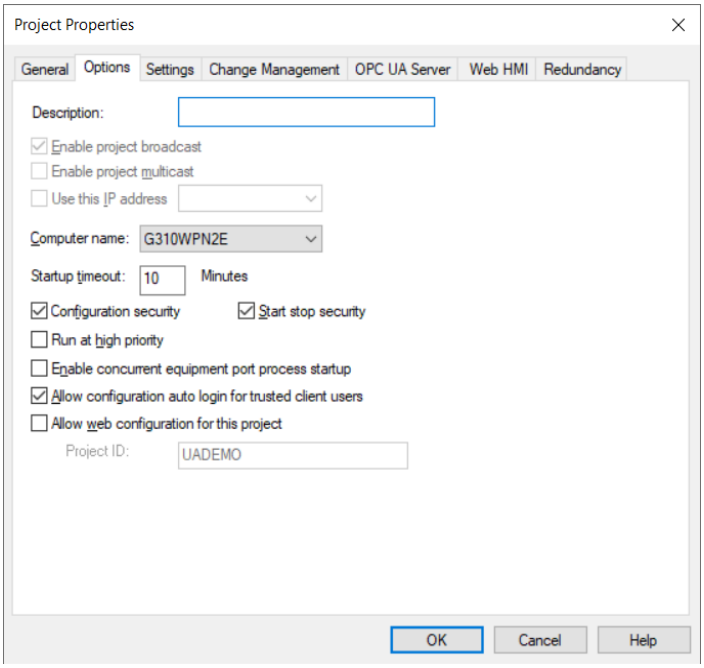


Figure 11 Project Configuration Security and Start Stop Security

Selecting the **Configuration security** check box opens the *Configuration* tab in *Role Properties* (see section Roles). Project administrators can select the privileges assigned to each role. For example, privileges such as running the Workbench and modifying users, roles, and resources are set through Configuration security.

Selecting the **Start stop security** check box activates the Start Project and Stop Project capability in the *Privileges* tab in *Role Properties* (see Figure 12). As the name indicates, this allows an Administrator to configure the roles allowed to start and stop a project.

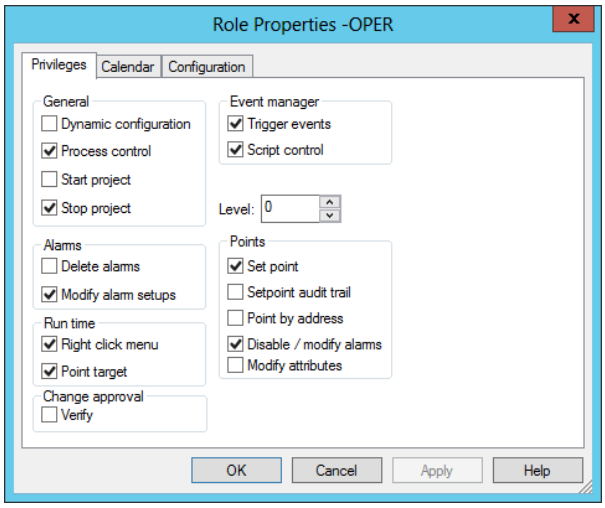


Figure 12 Start Project/Stop Project Privileges Assigned to a Role

After the options are selected, the person creating the Project is required to log in as a user with the SYSMGR role or a role created with the required privileges.

If a Project was created with an older version of CIMPLICITY and requires upgrading, review the Project for the Administrator account and check that the password meets current password complexity requirements or remove the password. Also, verify that the account password is not set to None.

CIMPLICITY has the capability to ensure only authorized users are making configuration changes. Review the configuration and diagnostic tools output for adherence to the Project specifications to ensure the configuration is valid.

Want to Know More?

Search "Configuration Security for a Project" in the CIMPLICITY Help Guide.

3.5.3 Settings

One of the most important security settings in the *Settings* tab is related to *User Setup* (see Figure 13). By default, new Projects have a password complexity that requires a minimum of 8 characters with an upper and lower-case letter plus a special character. Password length is configurable. This functionality is important in the event users have not originated from Active Directory.

The allowed number of unsuccessful login attempts before disabling the user account can be set on *User Setup*. The exact value of this setting is less important than setting it to some number - even a high number like 100. If there is no limit to the number of failed login attempts, an attacker can run a password cracking script or tool to attempt an unlimited number of potential passwords.

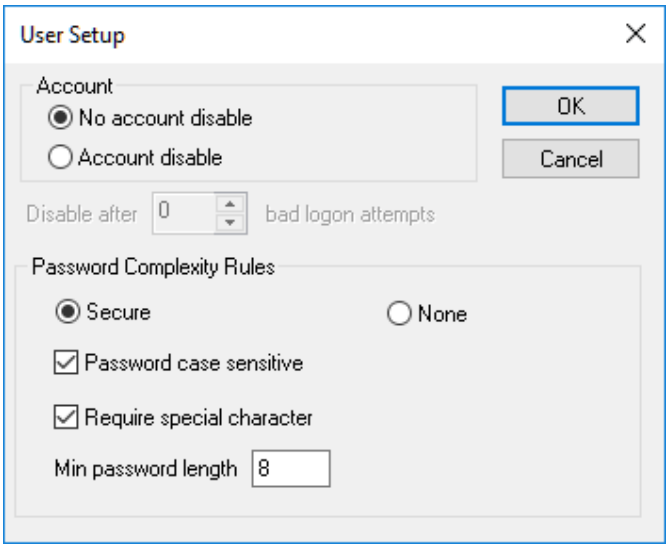


Figure 13 User Passwords and Allowed Login Attempts

If the CIMPLICITY system uses the Active Directory for authentication and an account lockout setting is implemented in the Active Directory, the **Account disable** option may not have a practical impact. However, as a precaution, configure the **Account disable** option in the CIMPLICITY Server.

The CIMPLICITY services (see Table 2) should be configured as a Windows domain account or as a local user with sufficient privilege to the projects configuration files and other CIMPLICITY configuration files, if using the powershell script in appendix A, this user should be a member of the `'CIM_RUNTIME_USERS'` group. The account must have lockout disabled to ensure that CIMPLICITY is always available. Windows domain accounts used by critical control room operators must verify that the account lockout is disabled and that it never expires so they can always log in to CIMPLICITY and avoid loss of control.

Want to Know More?

Search “Windows Authentication Configuration” and “User Runtime Properties” in the *CIMPLICITY User Guide*.

The security point settings on the *Point Setup* window (see Figure 14) has significant security implications. Access, privileges, and authentication can be restricted at the resource level by enabling these security point settings:

- **Enable Resource Set Point Security**

  In the *User Properties* configuration, a user can be configured with the ability to perform set points for selected resources in a Project. This is done by selecting the **Enable resource set point security** check box for the Project for a user. It is a good security practice to select this option in all cases, making all resources available in *User Properties* to all users if Resource Set Point Security is not being used in the initial installation.

- **Enable Level Set Point Security**

  This is a different type of access control that restricts the ability to perform set points by roles and points. Each role can be assigned a numerical level, and assign each point a numerical level. A user can perform set points when the level in the user role is greater than or equal to the level of the point that is set. This is a very granular, down-to-the-point level, access control feature. It also requires solid planning and attention to detail to implement properly.

- **Enable Set Point Password**

  A single password can be set for users to perform set points. This password is shared with all users who require the ability to perform set points and does not provide significant security protection. The Resource Set Point Security and the Level Set Point Security are much better security controls.

- **Allow Set Point for Read-Only Manual Mode Points**

  In some situations, this is considered a security setting. A user in a role with modify attributes privileges (see section Roles) can configure a point to manual mode. The point then uses and keeps whatever value the user sets, regardless of the actual value, until manual mode is disabled. Selecting this check box allows the user with the manual mode privileges to change the value of a read-only point. If the read-only points are for safety or high impact reasons, this setting can enable an attacker to compromise a user account with modify attribute privileges, placing a system in a high-risk state. Consider the benefits and risks of this option before making a configuration decision.

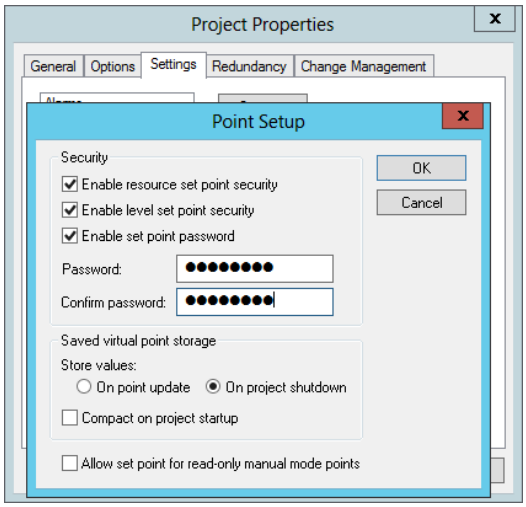


Figure 14 Point Setup Security Settings

Want to Know More?

Search "Set Point Security" in the *CIMPLICITY User Guide.*

3.5.4 Change Management

The *Change Management* tab in *Project Properties* (see Figure 15) is where change management is enabled for Project settings. This security control helps with after-incident analysis.

If **Project Change Management is enabled**, then the Change Management Server must be entered and the connection tested. Decisions on when and how to log in to the Change Management Server are available as check box options. An additional user login for change management may not be necessary if users and roles are set up properly (see sections Roles and Users).

The **Require checkout before changes** and **Allow changes when the server is not available** check boxes have potential availability issues for the CIMPLICITY Server. If either of these boxes is selected, no Project changes are possible if the Change Management Server is unavailable. Owners/operators must decide if the benefits of the technical controls that force the use of change management outweigh the risk of prohibiting Project changes because the Change Management Server is unavailable.

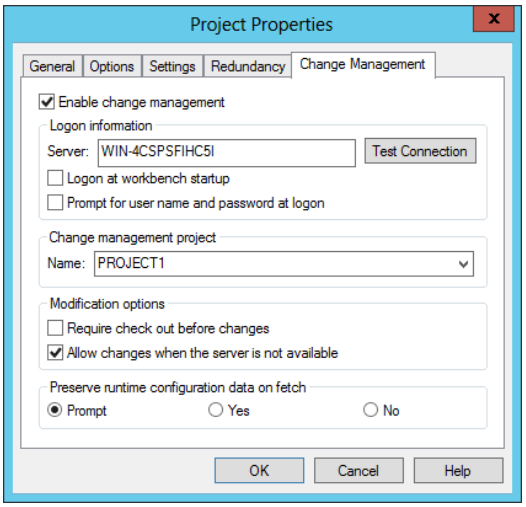


Figure 15 Change Management Security Settings

3.5.5 OPC UA Server

The OPC UA tab in Project Properties (Figure 16) allows users to enable and configure the OPC UA server. This allows OPC UA clients to retrieve data and alarms from the OPC UA server. Web HMI connects to CIMPLICITY via CIMPLICITY'S OPC UA server.

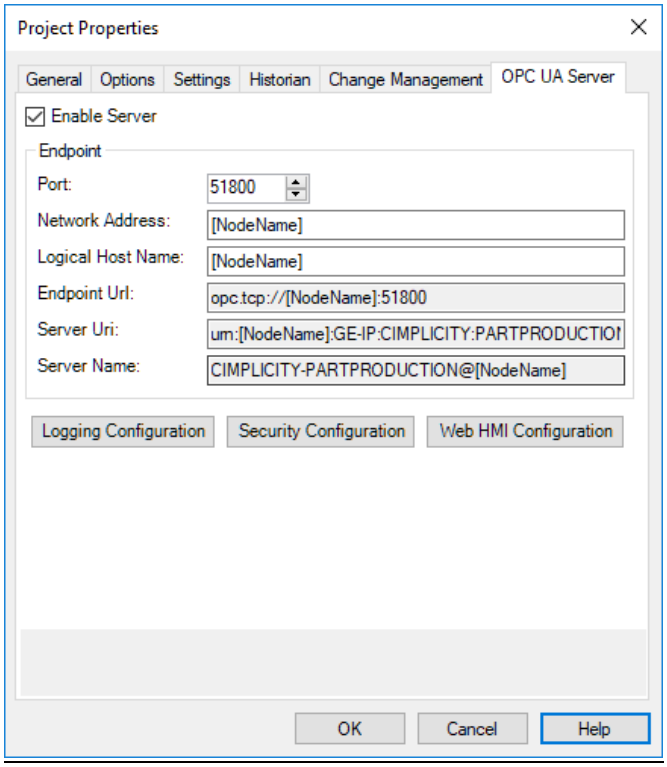


Figure 16 OPC UA Server Settings

Click Security Configuration to configure the security settings for the OPC UA server.

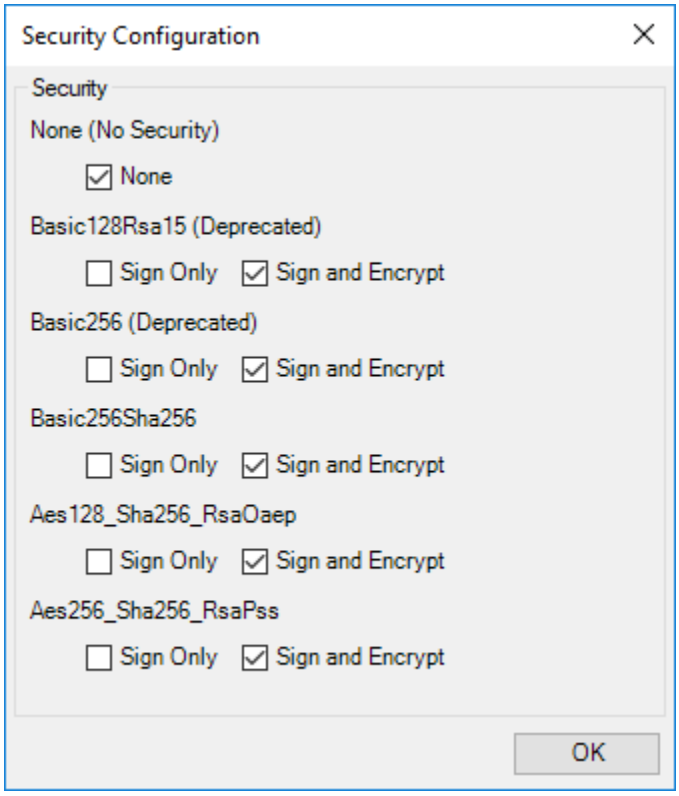


Figure 17 OPC UA Security Configuration Settings

Click Web HMI Configuration to set up and test the connection to the GE Web HMI server.

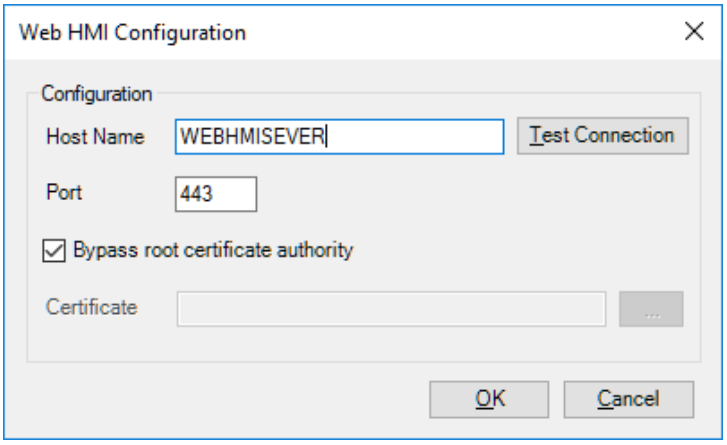


Figure 18 GE Web HMI Configuration for the OPC UA Server

Launch the OPC UA Security Configuration tool from the CIMPLICITY Workbench.

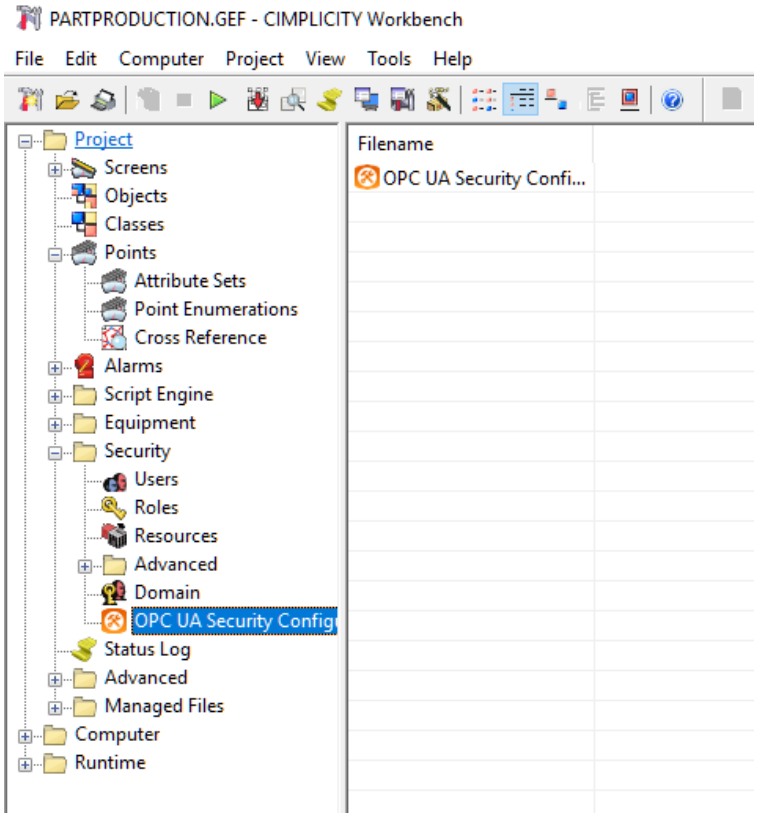


Figure 19 CIMPLICITY Workbench screen to launch the OPC UA Security Configuration tool

Launch the OPC UA Security Configuration tool to create the certificate required for the OPC UA server and OPC UA client.

To use self-signed certificates, uncheck the **Use GDS** check box and then click the **Enable Security** button. By default this certificate has a validity period of 5 years. If you wish a different expiration time period the advanced button may be used. There is no warning available for when this expiration will occur.

To use certificates signed by the Global Discovery Server (GDS), click the **Use GDS** check box and then click the **Enable Security** button. Any client that already trusts the GDS will automatically trust the certificate for a project when the GDS signs the certificates. Note that GDS must already be installed and configured to sign certificates. GDS simplifies the management of certificates when using a substantial number of clients and servers. For more information, search for "Configure a GDS-signed Certificate" in the CIMPLICITY help.

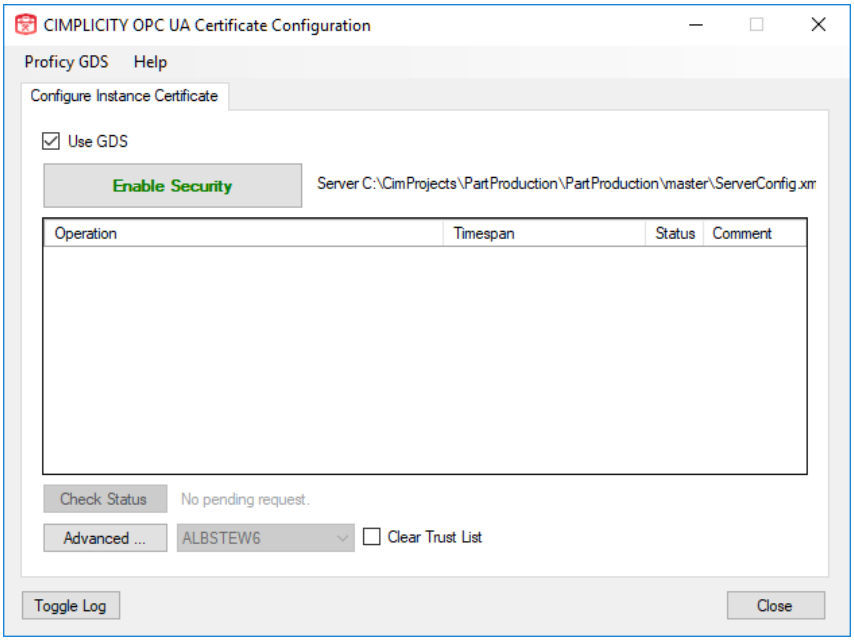


Figure 20 CIMPLICITY OPC UA Certificate Configuration/Creation tool

Want to Know More?

Search "Enable/Disable the OPC UA Server" in the *CIMPLICITY User Guide.*

3.6Allow Projects configuration

As of CIMPLICITY 2022 (aka v11.5) the CIMPLICITY system provides configuration option to define file paths from which projects are allowed to be started. This configuration is managed by editing the %BSM_ROOT%\admin_data\AllowProjects.json. The default installation allows project in any path to start.

```
"allow_all": true, // When true all projects can run, regardless
of directory
```

It is recommended that the allow_all parameter to be changed to 'false' and that the allowed_projects array be modified to include only valid project paths. The full path to each individual project folder that is allowed to start must be included in the allowed_projects array. It is important that only authorized users have write permissions to these project folders to secure the project configuration.

E.g.

```
"allowed_projects":["c:\\test_project1\\", "c:\\dev_project1\\"]
```

3.7 Resources

Resources are the physical or conceptual units that comprise the facility. They can be devices, machines or stations where work is performed. Resources can also be areas where several tasks are carried out. The organization and definition of resources play a large part in determining the view a user has in CIMPLICITY.

As discussed in section Settings, a user is typically assigned resources in the *Resources* tab of the *User Properties* window during user creation. Users can also be assigned to a resource in the *Resource Definition* window (see Figure 21).

The *Resource Definition* window shows the current users assigned to the resource. The following actions can be performed;

- Verify the user against the resource definition for troubleshooting and audit
- Add a user to a resource
- Assign users to a new resource in a deployed CIMPLICITY System

A CIMPLICITY administrator can add resources to each user but it is easier to add all required users in one step in the *Resource Definition* window.

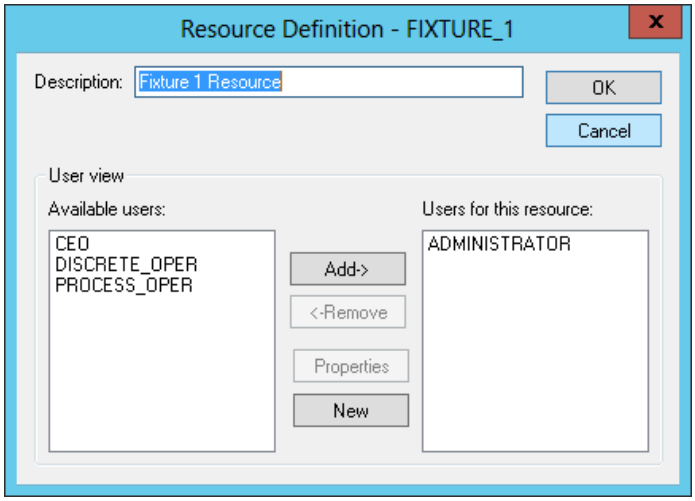


Figure 21 View and Modify User Resource Assignments

3.8 Roles

Role-based access control can make user administration simple and potentially less prone to errors with a security impact. When privileges are assigned to roles, users placed in these roles inherit those privileges. Role-based access control is used in most ICS applications, including the CIMPLICITY Server.

Each CIMPLICITY Project has three default roles for all Projects and two additional default roles if Process Systems are enabled.

These are the main default roles:

- SYSMGR (System Manager)
- USER
- OPER (Operator)

These roles appear when Process Systems are enabled:

- ENGINEER
- GUEST

As part of the security design for a Project, owners/operators should review all role settings and determine if additional roles are needed.

The *Role Properties* window is where roles are configured and the tabs on this window are determined by Project settings.

The creation of user accounts, activation, de-activation and removal of user accounts are logged into the event log as `$DYN_CFG` events.

Want to Know More?

Search "Dynamic Configuration Changes" in the *CIMPLICITY User Guide*.

3.8.1 Privileges

All roles have the *Privileges* tab (see Figure 22). The Start Project and Stop Project privileges are configurable only if they are selected in *Project Properties* (see section Options). The ability to start and stop Projects has operational and security ramifications that must be considered for each role. For all roles, the Start Project/Stop Project setting is unselected.

The other important security control on the *Privileges* tab is the **Level** setting. If a Project is set with **Enable Level Set Point Security** (see section Settings), this setting can be used. The Level setting is a role-based access control method where the level of a user role is compared to the level assigned to a point. A user can set points or change other writeable attributes if the user role level is greater than or equal to the point level.

Using the role-based Level Set Point Security feature requires planning in the design phase as levels for points and roles must be considered and set. The primary benefit of using this feature is allowing a user to view resources but restricting actions on the points based on the user role. The default level is zero for all roles.

Several check box options are not strictly security related when in the Level setting, but control whether a user in a role can perform some important actions, such as:

Alarms

If a user in a role can modify and delete alarms, it may impact the integrity of the audit trail and after-incident analysis.

Change Approval

Select this check box if electronic signatures are required for both the set point performer and the verifier.

Points

Security-related check boxes pertaining to points are:

- Role can perform set points on resources in the users view (Set Point)
- Set point audit trail is sent to the event log (Set point Audit Trail)
- Role can disable or modify alarms (Disable/Modify Alarms)

- Role can change a point to MANUAL_MODE or QUALITY.DISABLE_WRITE (Modify Attributes)

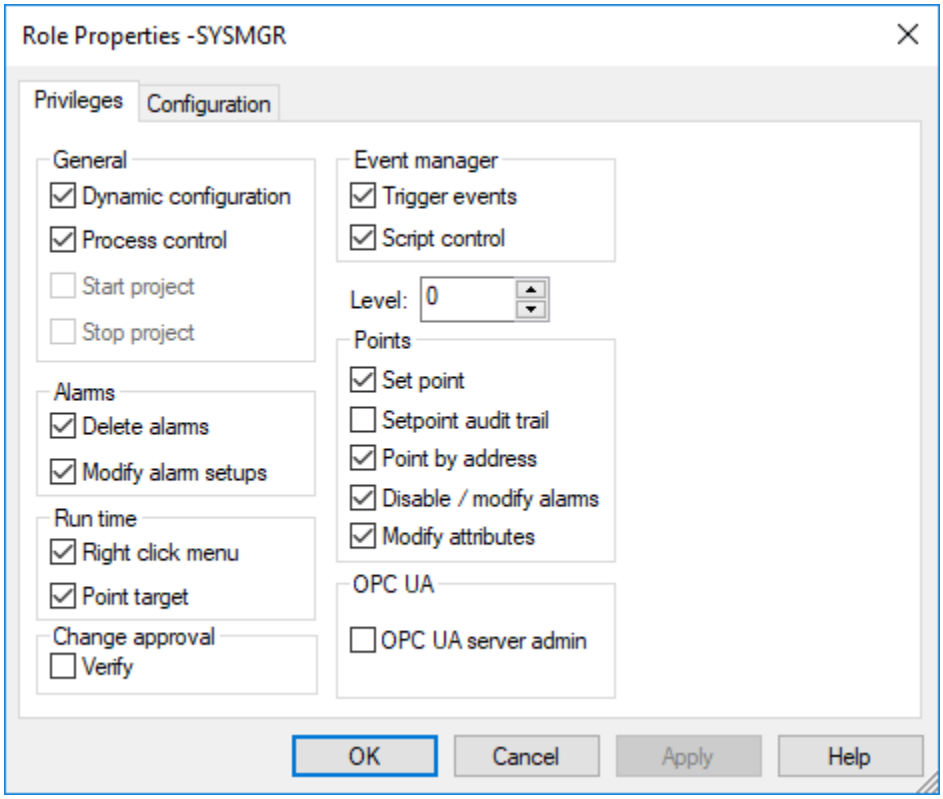


Figure 22 Configure Privileges in Role Properties

3.8.2 Configuration

The *Configuration* tab appears in the *Role Properties* window if configuration security is set in *Project Properties* (see section Options). The configuration settings for *Role Properties* determine what a user in a role can configure in the CIMPLICITY Server (see Figure 18), such as add, delete, or modify user accounts, open the Workbench application, and access remote Projects.

The default settings for the ENGINEER, OPER, and SYSMGR roles are automatically selected. The default setting for the GUEST role has no check boxes selected. The USER Role is the only role with some check boxes selected and others not selected (see Figure 23). If role-based access control is part of the control system design principle, then the configuration settings of the default roles and any newly created roles must be carefully considered and set accordingly.

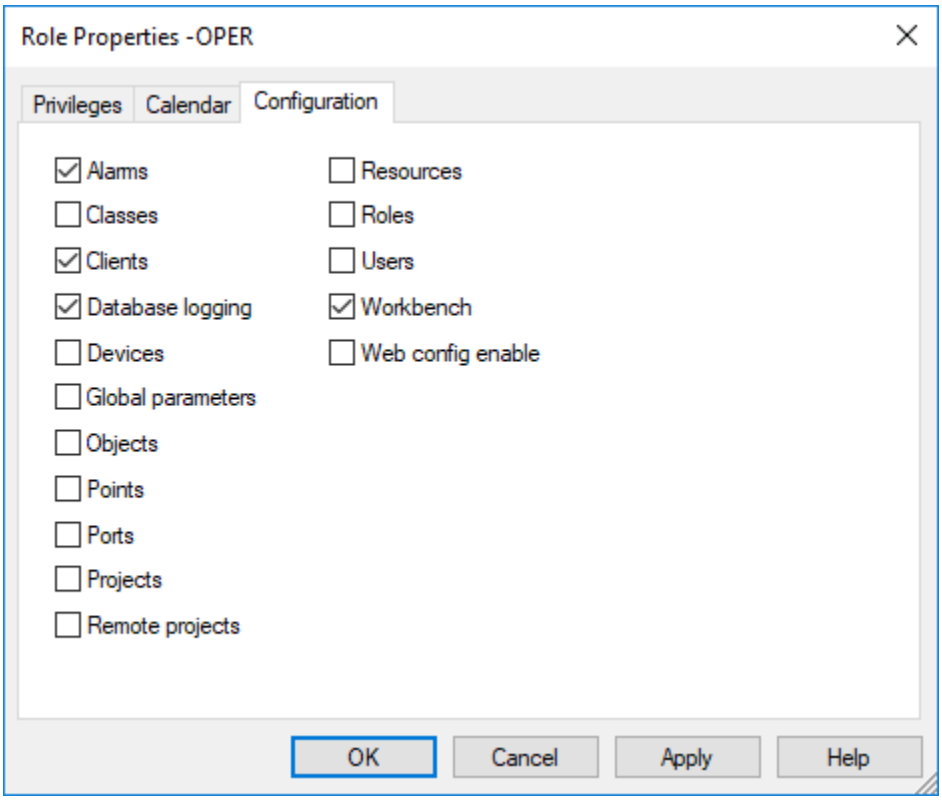


Figure 23 Default Configuration Rights for User Role in Role Properties

3.8.3 Calendar

The *Calendar* tab in *Role Properties* (see Figure 24) appears if the Action Calendar was enabled in *Project Properties*. Area Resource Security is another access control method to restrict user viewing and point operations. This is similar to Resource Set Point Security but adds the time element (see section Settings).

When the **Area Resource Security** check box is selected and areas are created and mapped to a Resource ID, then the Action Calendar can be used to determine when the users with access to an area can view and operate points related to the Resource ID assigned to the area. Area Resource Security must be considered when the staffing, operation and management of the control system varies by day or shift.

The **Configuration** check box determines if the role can create or modify a schedule in areas they can see. Limit the ability to modify a schedule to only those users who require this privilege.

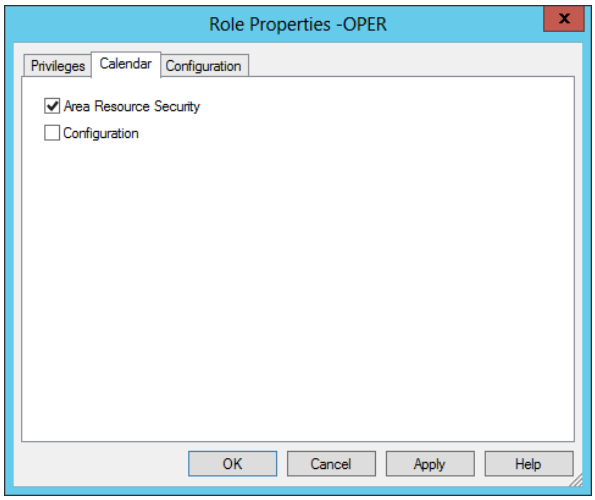


Figure 24 Calendar Tab in Role Properties

3.8.4 Additional Role Properties

These additional *Role Properties* tabs appear with configurable options if the CIMPLICITY Server Tracker or Order Execution Management options are selected.

- Role Broadcast privileges can be set if the CIMPLICITY Server has the Order Execution Management Broadcast option enabled.
- Role Tracker Query Engine (TQE) privileges can be set if the CIMPLICITY Server has the Order Execution Mgt. TQE option enabled.
- Role Tracker Attribute Database (TADB) privileges can be set if the CIMPLICITY Server has the Order Execution Mgt. TADB option enabled.
- Role Tracker User Interface (UI) privileges can be set if the CIMPLICITY Server has the Tracker option enabled.

- Role Routing and Control Objects (RCO) User Interface (UI) privileges can be set if the CIMPLICITY Server has the Tracker RCO UI option enabled.

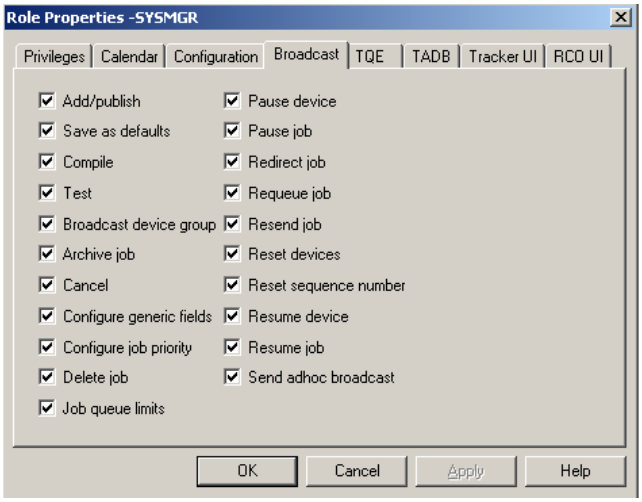


Figure 25 All Possible Role Properties

3.9 Users

When a new CIMPLICITY Project is created in a CIMPLICITY Server, the user is prompted to provide a user name and password that is assigned the SYSMGR role. There are no user default accounts. Passwords are subject to complex password rules.

One best security practice is to create and assign a unique user account to each person requiring a CIMPLICITY Server login. This allows any action recorded during login to be attributed to the specific owner of the account performing the action. Shared accounts make this attribution through logs impossible, and it is very common for shared account credentials to be widely known in the Operations Group over time.

This security practice of unique user accounts is often violated by ICS owners/operators, particularly with operators in a control room for a variety of reasons. Issuing unique user accounts to individuals is most important for:

- Highly-privileged accounts, such as accounts with the SYSMGR role
- Accounts used in a physically insecure site or a site that is not manned 24x7

If a shared user account is part of the security design, then another security control should be implemented by policy or other means to hold an individual responsible for the action taken with the shared user account. For example, operators using a positional shared user account, for use by any operator on a specific HMI, could be held accountable for all actions taken on that HMI while an operator is on shift.

One of the important security decisions to be made during the security design phase is the type of user authentication to use. While it is possible to assign an authentication method by user, it is better to keep it simple and select a single method for all authentication unless there is a compelling reason to make authentication more complicated.

3.9.1 Windows Authentication

Microsoft has developed robust user authentication and authorization capabilities in their Active Directory/Domain services, which are well understood by most owners and operators. The CIMPLICITY Server can leverage these capabilities and provide some helpful benefits, such as:

- **Single Sign On**

  CIMPLICITY can be configured so a user who logged in to the Windows OS does not need to log in to the CIMPLICITY Server.

- **Centralized User Management for Operations Technology**

  As the size and complexity of the control system grows, this feature becomes more significant. Users are added, deleted, and modified in the Active Directory rather than in multiple application servers.

- **Password Policy**

  Active Directory can enforce a full-featured password policy.

- **Centralized User Security Logging**

  Log-on failures, account changes, and other user related security events are stored and available centrally on the Active Directory Server.

  If Windows authentication is used, owners/operators should deploy a separate domain structure for the Control System/Operations Technology users who are not part of the same domain forest or tree as the corporate domain (see section Sample Reference Architectures). This prevents any attacks on the corporate Active Directory from affecting user management on CIMPLICITY.

Windows Authentication is enabled by selecting the **Enable Windows Authentication** check box in the *Windows Authentication* window, which is accessed through Domain Properties in Project>Security (see Figure 26).

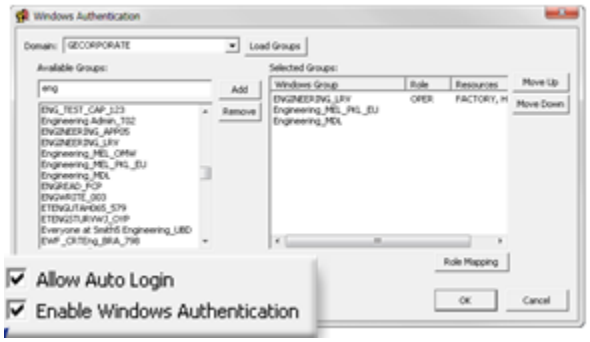


Figure 26 Enable Windows Authentication

The next step is to select the Windows domain to use for authentication from a list of available domains. One authentication or authorization deployment approach is to stop integration at this point. The Windows Active Directory can authenticate one or more users but all privileges are determined by how users are configured to roles and resources in the CIMPLICITY Server.

However, another deeper level of Windows and CIMPLICITY integration is possible by mapping Windows groups to CIMPLICITY roles. These are the benefits to such an integration:

- No need to add users in CIMPLICITY. When a Windows user is a member of a Windows group mapped to a CIMPLICITY role, then the user is automatically assigned to the CIMPLICITY Server.
- No need to assign roles to users in CIMPLICITY. A user's Windows group membership determines the role assignment to the user.
- No need to assign resources to users in CIMPLICITY. A user's Windows group membership identifies the resources a role can access.
- The mapping of a role and resources to a Windows group provides another method of implementing granular authorization privileges. For example, a site with two plants, Plant A and Plant B, has two Windows groups for each role, such as OPER_A and OPER_B. The mapping for Windows group OPER_A is the OPER role and the resources in Plant A. Similarly, the Windows group OPER_B is mapped to the OPER role and the resources in Plant B.

The first step in using Active Directory groups for selecting a CIMPLICITY role and resources is to create the Active Directory groups. Before creating a unique group, evaluate each unique role and resource case.

Next, click the **Load Groups** button (see Figure 27). This loads all available groups in the selected Windows Domain. Select the groups created or planned for use with CIMPLICITY. They appear as selected groups.

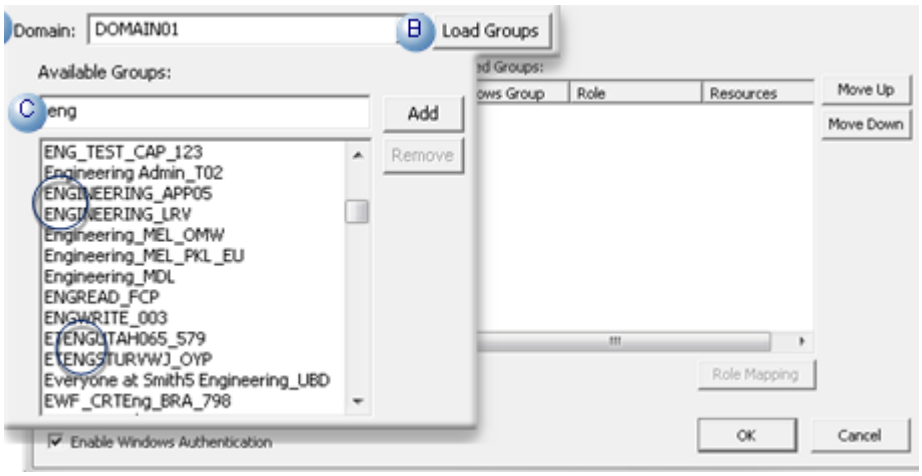


Figure 27 Load Groups for Role and Resource Mapping

Highlight each selected group and click the **Role Mapping** button. For each selected group, assign one role and the appropriate resources from the list of available roles and resources that appear (see Figure 28). This mapping is unique to the Project and can be set differently for each Project.

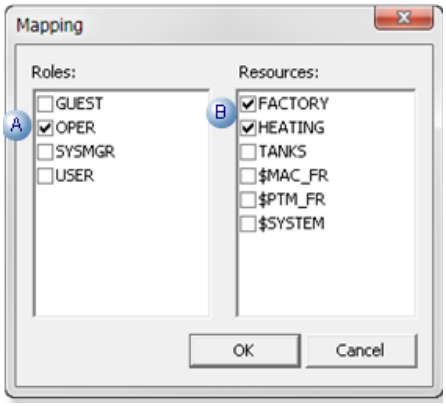


Figure 28 Role and Resource Mapping to a Windows Group

An important step is to place the selected groups in priority order. If each user is only in one selected group, then the priority order does not matter. If a user is in more than one selected group, the user is assigned with the role and resources of the highest priority selected group.

The priority order of selected groups tends to be important in larger and more complex CIMPLICITY deployments. If the CIMPLICITY Server has multiple Projects, the proper assignment of a role and resources may differ by Project and require a different set of selected groups and a different priority order.

The last step is to determine if single sign-on authentication is allowed. If the Allow Auto Login check box (see Figure 26) is selected, the Windows user name is used and the Active Directory is queried for group membership. The selected Windows groups and corresponding role and resources are applied. If this check box is not selected, the user is presented with another means of logging on for authentication.

The main security benefit of the second authentication to a CIMPLICITY application is when the CIMPLICITY client is left unattended and unlocked. An adversary with physical access to this computer can use an existing login to gain access to CIMPLICITY applications. Consider single sign-on authentication when the ease of operation is important for users in a physically secure area or when clients have short idle time outs.

Want to Know More?

Search “Windows Authentication Configuration" in the *CIMPLICITY User Guide*.

3.9.2 Proficy Authentication

Proficy Authentication (PA) provides identity-based security for Proficy based applications and APIs. It supports open standards for authentication and authorization, including Oauth2.

In addition to CIMPLICITY, Several Proficy products use Proficy Authentication, including Historian, IFIX, Plant Applications, and Operations Hub. To use Proficy Authentication, you must install one of these products. Each product can install an independent instance of Proficy Authentication, or it can reuse an existing instance of Proficy Authentication which was previously installed by another Proficy product. When more than one product uses the same instance of Proficy Authentication, this is called a shared or common Proficy Authentication.

Shared Proficy Authentication means that if you have a Proficy product installed that uses Proficy Authentication, additional Proficy products installed after that initial product can also share that existing, already configured Proficy Authentication Server. **This is the recommended model as this would allow user management across multiple products from single place.**

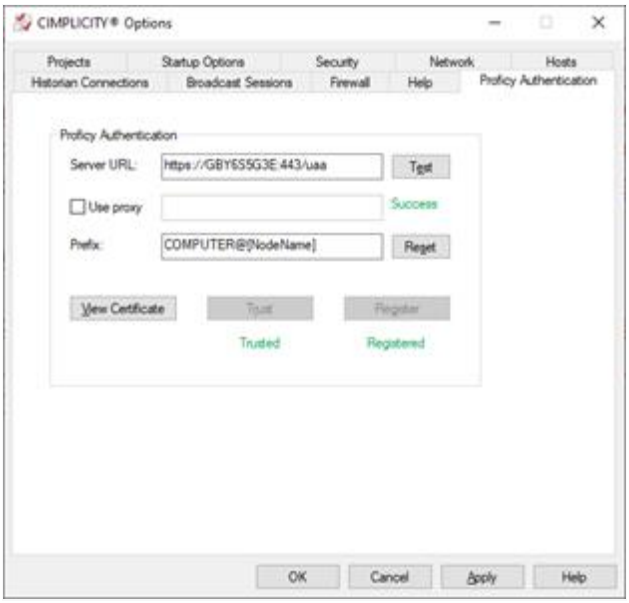
Proficy Authentication can additionally be configured to use an external identity provider. This includes identity providers which use Lightweight Directory Access Protocol (LDAP) or Security Assertion Markup Language (SAML). When you integrate Proficy Authentication with an external identity provider, you can provide the users and groups from that identity provider with access to Proficy products and their features.

Proficy Authentication support can be layered into your existing CIMPLICITY projects while still fully supporting its existing native authentication and authorization capabilities. CIMPLICITY integrates its Roles and Resources into a new identity called "Security Groups" which then synchronize with Proficy Authentication Groups to provide appropriate permissions to users.

To set up Proficy Authentication, you need to follow a two-phase configuration process. Initially, you configure the Proficy Authentication server information at the computer level. Afterward, each project on the computer can independently decide whether to utilize Proficy Authentication or not.

Computer level configuration:

You can configure the details of the Proficy Authentication Server through the CIMPLICITY Options Dialog. The page looks as follows:

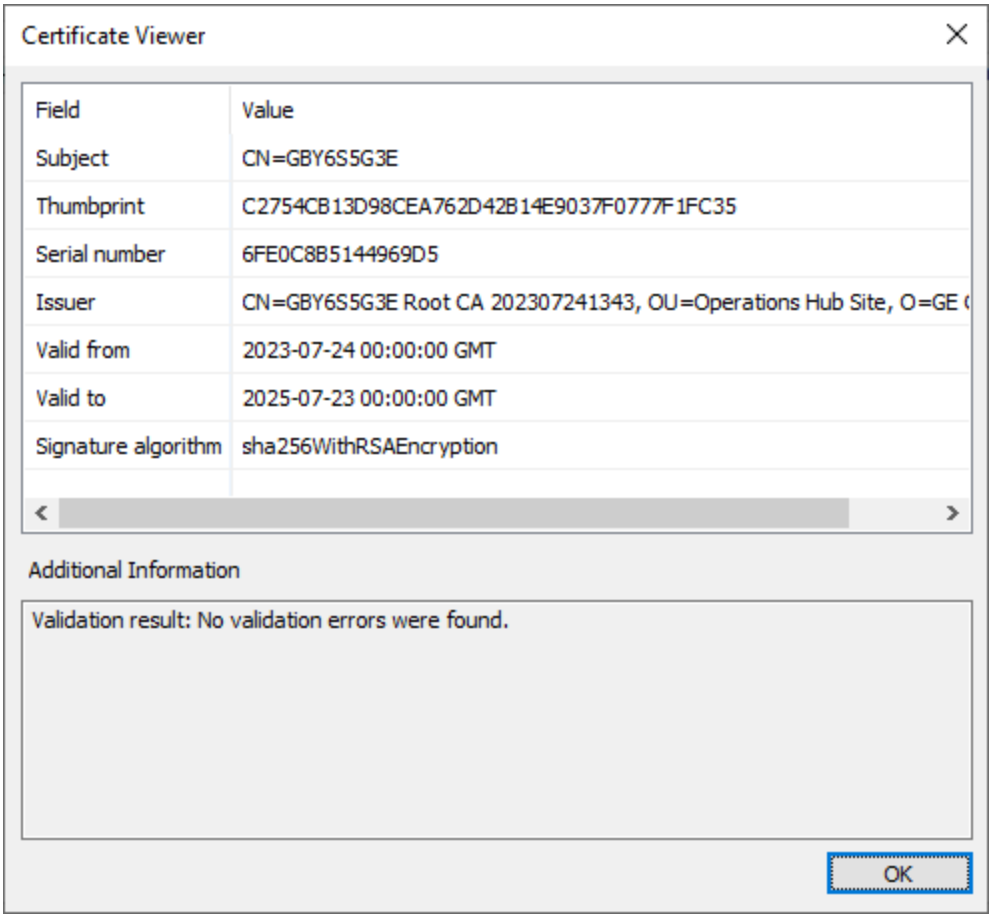


The steps for configuration are outlined below.

1.Enter Proficy Authentication url in the Server URL edit box.

2.Click on Test button to ensure connection is successful.

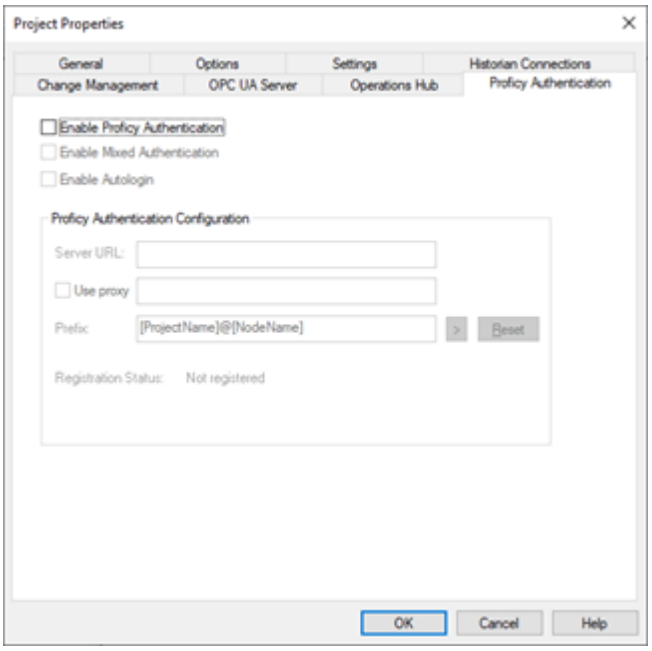
3.Click on View Certificate button. If url is properly configured root certificate of Proficy Authentication server will be shown as below



4.Ensure that it is correct certificate by cross checking Thumbprint.

5.Then clicking on Trust button will import the above root certificate into Trusted Root Certification Authorities.

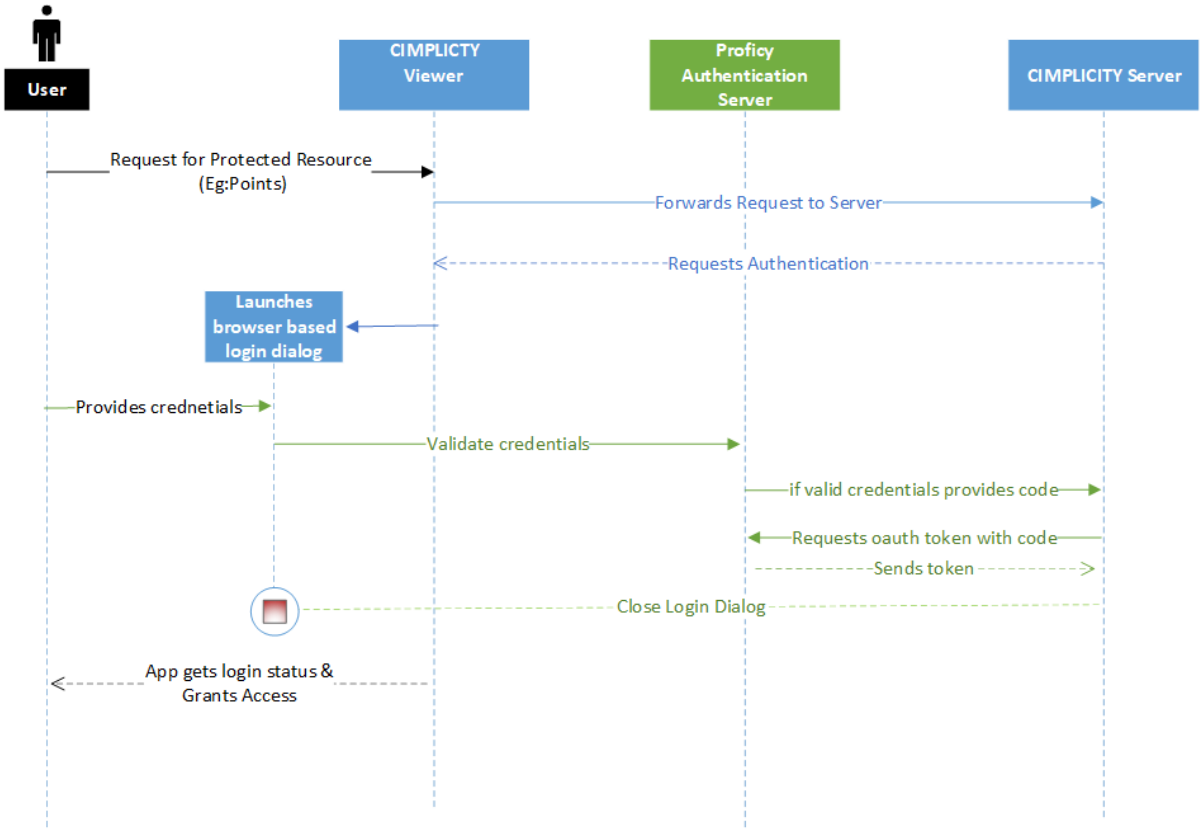
Project Level Proficy Authentication Configuration:



Enable Proficy Authentication:

This option displays the Proficy Authentication Login Dialog and employs the Authorization Code Grant flow. It utilizes the browser to accept user credentials as input and supports multi-factor authentication. The diagram below illustrates the high-level flow of data in the authentication process.

CIMPLICITY communicates with Proficy Authentication using REST calls, which is a web-based architectural style. This communication requires proper configuration of certificates and ports, and the subsequent sections provide details about these configurations.



Root Certificates:

In the flow diagram above, the green-colored arrows represent REST communication between different nodes. From the diagram, it is evident that the Viewer must communicate with both the Proficy Authentication server and the CIMPLICTY server via REST (HTTPS). Therefore, it is necessary to install and trust the root certificates of both the Proficy Authentication Server and the CIMPLICTY Server on all the Viewer nodes.

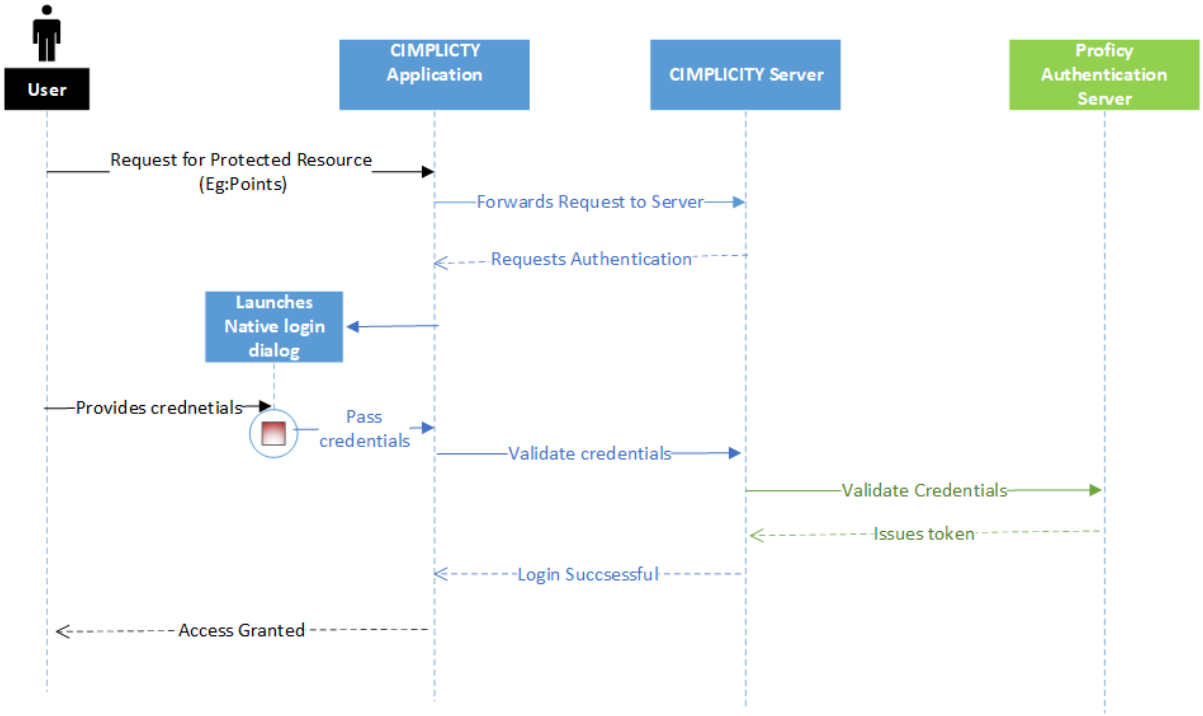
Firewall ports:

This firewall rule supports this communication:

Source IP	Destination IP	Destination Port
CIMPLICITY Server	Proficy Authentication Server	TCP/443
CIMPLICITY Viewer	Proficy Authentication Server	TCP/443
CIMPLICITY Viewer	CIMPLICITY Server	TCP/9443

Enable Mixed Authentication:

This option utilizes the classic Login Dialog to collect user credentials. However, this mode does not support multi-factor authentication.



Root Certificates:

In the flow diagram above, the green-colored arrows represent REST communication between different nodes. From the diagram, it is evident that only the CIMPLICTY Server needs to communicate with the Proficy Authentication server via REST (HTTPS). As a result, it is necessary to install and trust the root certificates of the Proficy Authentication Server solely on the CIMPLICTY server node.

Firewall ports:

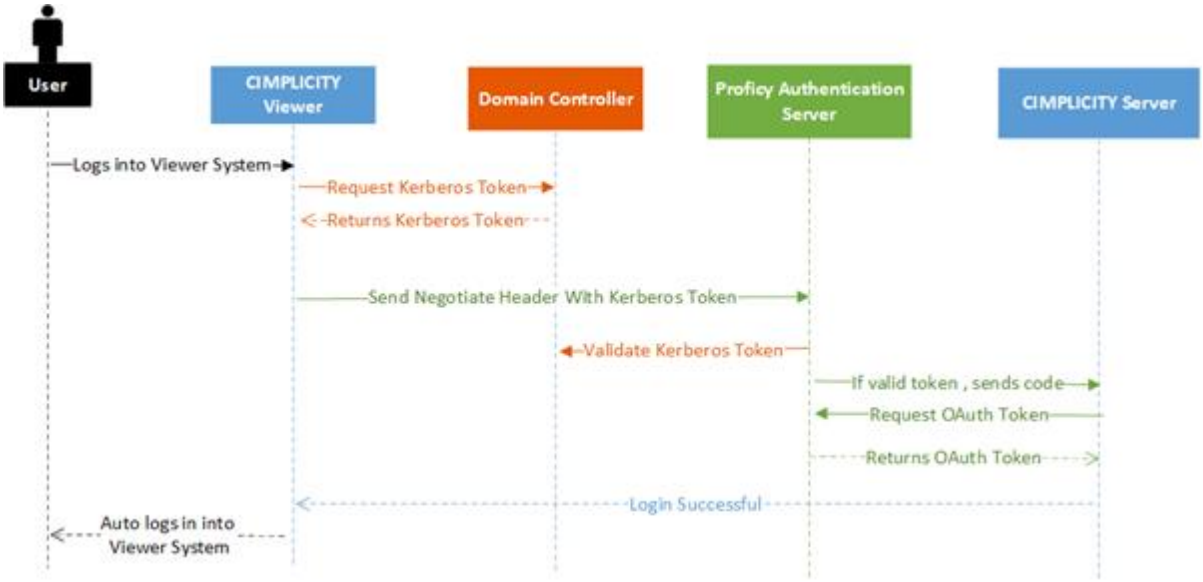
This firewall rule supports this communication:

Source IP	Destination IP	Destination Port
CIMPLICITY Server	Proficy Authentication Server	TCP/443

CIMPLICITY Viewer	CIMPLICITY Server	TCP/9443

Autologin:

This option enables users to automatically log in to CIMPLICITY applications after logging into the Windows system using Kerberos authentication. It's important to note that Kerberos authentication is supported only in domain controller systems.



The root certificates and firewall requirements for this option are identical to those needed for the Authorization grant (Enabling Proficy Authentication).

Want to Know More?

Search “Proficy Authentication Configuration" in the *CIMPLICITY User Guide*.

3.9.3 Managing Users in CIMPLICITY

CIMPLICITY

If Windows Authentication is not the desired approach, the following authentication and authorization methods can be implemented per user (see Figure 29):

Users can be entered in the CIMPLICITY Server, authenticated through the CIMPLICITY Server, and assigned a role and resources through the CIMPLICITY Server. This authentication type does not require a Windows Domain Controller. This is best suited to smaller environments with a limited number of users, roles and resources, or by companies where employees may not have the skill set to deploy and maintain the Windows Active Directory.

Windows Domain

Users are authenticated using the Windows Active Directory but the role and resource assignments in the User Properties window override any selected group mappings.

This is the case where Active Directory is used for authentication, but authorization is configured for the User in CIMPLICITY.

Windows Domain with Group Mapping

Active Directory authenticates the User and Windows Group membership of the User and determines the User's Role and access to Resources. This Authentication Type leverages Windows Active Directory to a greater extent, and requires a more skilled Windows Domain Administrator.

The *General* tab of *User Properties* has several security related settings that apply, depending on the authentication type selected.

- The role entered on this tab applies to the CIMPLICITY and Windows Domain authentication types.
- The Password setting only applies to the CIMPLICITY authentication type.
- The Password Expires setting only applies to the CIMPLICITY authentication type. When this value is set to zero, a password never expires.

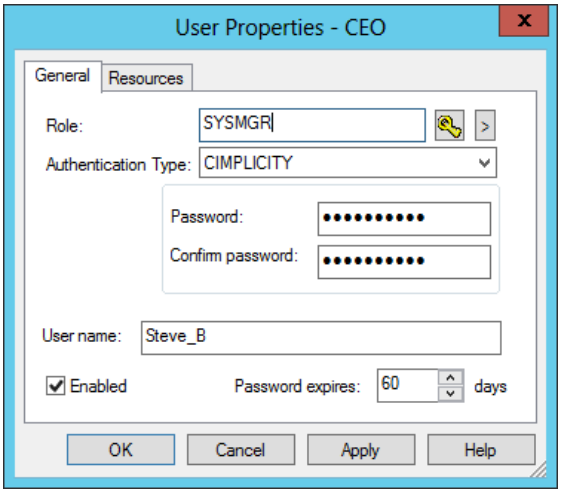


Figure 29 User Properties

The *Resources* tab allows resources to be assigned to a user. This applies to the CIMPLICITY and Windows Domain authentication types.

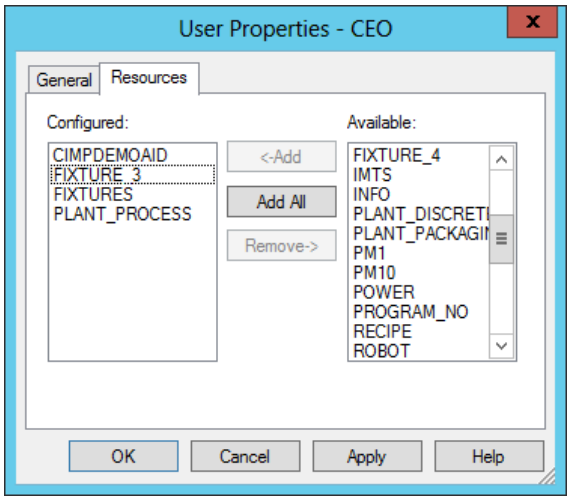


Figure 30 Assign Resources to a User

Proficy Authentication

Proficy Authentication can be used for enforcing security by following below steps,

1. Create security groups in CIMPLICITY.
2. Publish them to Proficy Authentication server.
3. Assign appropriate security groups to the Proficy users.

Create Security Groups in CIMPLICITY:

The security group is a new concept created to group Proficy Authentication users together and assign them common roles and resources. For further clarification, please refer to the example provided below.

Example:

Let us say we have three category of user groups, Administrators, Operators and Users we could create corresponding three security groups in CIMPLICITY.

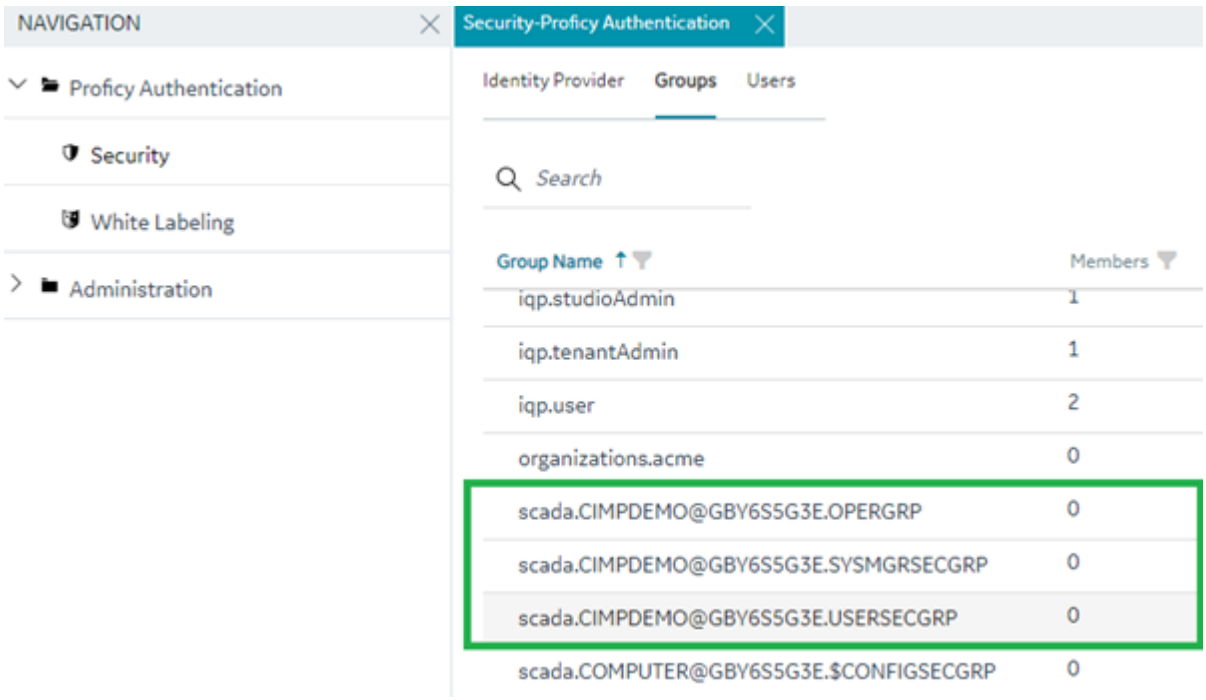
SYSMGRSECGRP: security group for administrators.

OPERSECGRP: security group for operators.

USERSECGRP: security group for users.

Name	Role ID	Rank	Description
OPERGRP	OPER	997	Security group for operators
USERSECGRP	USER	998	Security group for users
SYSMGRSECGRP	SYSMGR	999	Security group for administrators
$CONFIGSECGRP	$CONFIG	0	Configuration privileges security group

After publishing these security groups, they will be incorporated as groups in the Proficy Authentication server, appearing as follows:



Group names in PA will be based on below naming convention:

scada.<project_prefix>.<security_group_name >

By default, for a single CIMPLICITY server system, the project prefix is set as [ProjectName]@[NodeName]. However, this configuration can be adjusted from the project-level Proficy Authentication page. For redundant systems, the project prefix is only [ProjectName].

To grant Proficy Authentication users access to the CIMPLICITY project, it is necessary to assign the aforementioned security groups within Proficy Authentication Server.

For e.g.: let us say there are three Proficy users

1. PlantAdmin

2.PlantOperator

3.PlantUser

We can assign Proficy Authentication Groups in the following ways:

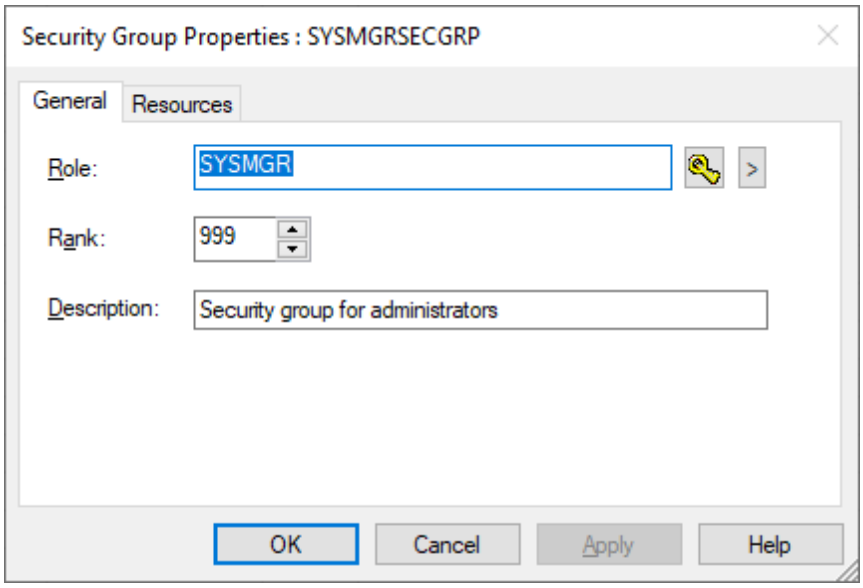
Assign one group to each user:

We can configure one to one Group mapping for users as mentioned below

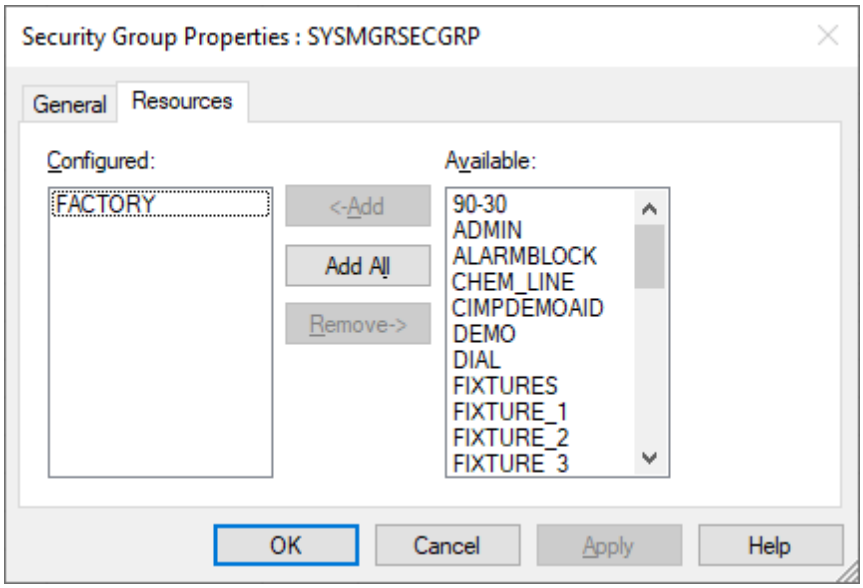
S.No	Username	Groups assigned in PA
1	PlantAdmin	scada.CIMPDEMO@GBY6S5G3E.SYSMGRSECGRP
2	PlantOperator	scada.CIMPDEMO@GBY6S5G3E.OPERGRP
3	PlantUser	scada.CIMPDEMO@GBY6S5G3E.USERSECGRP

With this mapping when user “PlantAdmin” logs into CIMPDEMO project on node GBY6S5G3E, he will be getting role and resources configured for security group SYSMGRSECGRP.

So if we configured SYSMGRSECGRP as shown below:



The user "PlantAdmin" will be assigned the role of "SYSMGR."



The user PlantAdmin would get role as SYSMGR with access to resource FACTORY.

Assign multiple groups to the same user:

Proficy Authentication also supports assigning multiple groups to the same user. For example, it could be configured as demonstrated in the table below:

S.No	Username	Groups assigned
1	PlantAdmin	scada.CIMPDEMO@GBY6S5G3E.SYSMGRSECGRP scada.CIMPDEMO@GBY6S5G3E.OPERGRP
2	PlantOperator	scada.CIMPDEMO@GBY6S5G3E.OPERGRP
3	PlantUser	scada.CIMPDEMO@GBY6S5G3E.USERSECGRP

In this scenario, we have assigned two groups, namely "scada.CIMPDEMO@GBY6S5G3E.SYSMGRSECGRP" and "scada.CIMPDEMO@GBY6S5G3E.OPERGRP," to the user "PlantAdmin." The resolution of role and resources is outlined as follows:

Role:

When user is assigned multiple groups, role is resolved based on the rank of security groups, for e,g: if we have following configuration

S.No	Security Group Name	Rank
1	SYSMGRSECGRP	999
2	OPERGRP	998
3	USERSECGRP	997

PlantAdmin is assigned two groups, SYSMGRSECGRP and OPERGRP. Since SYSMGRSECGRP has a higher rank among the assigned groups, the configuration from SYSMGRSECGRP would be applied to the PlantAdmin user, granting him the SYSMGR role.

Resources:

When a user is assigned multiple groups, the resources available to the user are the cumulative sum of the resources present in all the assigned groups.

S.No	Security Group Name	Resources
1	SYSMGRSECGRP	SYSRES1, SYSRES2
2	OPERGRP	OPERRES1, OPERRES2,
3	USERSECGRP	USERRES1

PlantAdmin is assigned two groups, SYSMGRSECGRP and OPERGRP, PlantAdmin will have access to the resources SYSRES1, SYSRES2, OPERRES1, and OPERRES2.

Integrating Proficy Authentication with external active directory(LDAP):

any existing security provider based on Microsoft Active Directory (LDAP Server), can be integrated with Proficy Authentication Server, by mapping LDAP groups with CIMPLICTY security groups published to PA Server. This can save considerable time by avoiding the need to replicate the user database. Refer to Proficy Authentication Server documentation for more help.

4. Client Connections

The primary security settings for client connections are set and enforced in the CIMPLICITY Server. Section Computer explains the Secure Sockets setting that encrypts client-to-server communications. Section Users covers the various CIMPLICITY Server user authentication options and how to configure them.

4.1 Client Configuration

The CIMPLICITY Server can determine the authentication requirements for a computer acting as a CIMPLICITY Client. Create and configure a CIMPLICITY Client in Project>Advanced>Client. A new client is given the computer name and its properties set in the *Client Properties* window (see Figure 31).

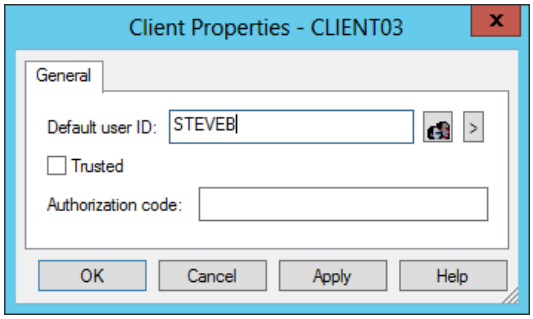


Figure 31 Client Properties

The *Client Properties* window helps to determine the required authentication (see Figure 32).

Option	In the Default User ID Field	Trusted Check Box	Client Access
1	Enter a User ID from the list of users available for the project.	Cleared	Users from the Client computer with the selected User ID are automatically logged in.
2	Leave User ID blank.	Selected	Users whose Windows Logon Username matches any CIMPLICITY User ID in the project are automatically logged in. All other users must enter a User ID and Password (if required) in the CIMPLICITY Login dialog box.
3	Enter a User ID from the list of users available for the project.	Selected	Users whose Windows Logon Username matches the specified CIMPLICITY User ID in the project are automatically logged in with that User ID. All other users must enter a User ID and Password (if required) in the CIMPLICITY Login dialog box.
4	Leave User ID blank.	Cleared	All users from the Client computer must manually log into CIMPLICITY.

Figure 32 Authentication Options in Client Properties

Always leave the **User ID** blank and the **Trusted** check box cleared to ensure that all users must log in to that computer/client. Many organizations choose to lessen login requirements for clients that are in a physically secure and 24x7x365 manned location, or for clients that have limited privileges such as view only. The automation and login requirements needs to be considered during the design phase of a project.

If automated login is set in the *Client Properties* window, an attacker can spoof the client connection from another computer – that is, gain unauthorized access by pretending to be the user. Setting and requiring an authorization code reduces this risk.

The authorization code is generated on the CIMPLICITY Client computer using the Genauthcode command in a *cmd* window. Enter the authorization code in Client Properties on the CIMPLICITY Server. Part of the input for this authorization code is data specific to the client computer for each computer to generate a unique authorization code. The authorization code feature is considered a station-based access control feature.

The default *CIMPLICITY Login* dialog box (see Figure 33) has a **Save User ID + Password** check box. This feature makes the user experience easier, but it also introduces some risk to computers with CIMPLICITY Clients. The check box can be removed by adding the LOGIN_NOSAVE function to the Global Parameters file in a CIMPLICITY Client computer. This is a good security practice for all CIMPLICITY Client computers, and it is more important in CIMPLICITY Client computers that are in a physically insecure location or that are accessible by users with different privileges. Never save user IDs and passwords on a CIMPLICITY Server computer.

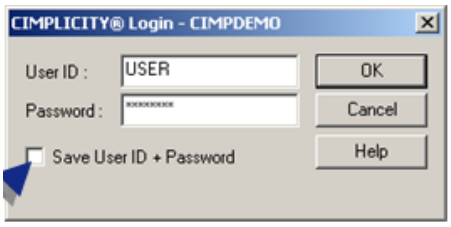


Figure 33 CIMPLICITY Login Dialog Box

4.2 CimView

CimView is the runtime client application used by personnel who monitor and control a process through the CIMPLICITY Server. It is commonly referred to as a Human Machine Interface or Operator Station in ICS terminology.

The CIMPLICITY System Administrator controls which CimView Projects and screens that CimView can open, and has access to both the computer and the user logged in to CimView. The screen files, `.cim` files, are distributed to each CimView. Typically, CimView automatically retrieves these files from a shared folder on the CIMPLICITY Server.

This automated method introduces risk as the Microsoft protocols required for file and folder sharing are high value targets and are the subject of automated attacks when vulnerabilities are identified. Organizations should consider manually distributing the CIMPLICITY screens, particularly to CimView stations that are in a less trusted zone such as DMZ. This eliminates the need to allow highly targeted Microsoft protocols through the firewall forming the cyber security perimeter. Manually distributing the screens to less trusted CimView clients also allows an organization to provide a restricted set of screens.

CimView can be started from the command line. Command line arguments can be reviewed to understand their security ramifications when using Cimview:

- `/loadpassword`

  This argument is followed by a file name that stores the Project Name|User ID|Password in plain text, which is often a security risk.

- `/noopen`

  This argument restricts users to opening CimView screens that are explicitly listed in Open Screen and Overlay Screen actions. Use this argument for stations requiring restricted views and commands.

- `/nosetpoints`

  This argument prevents and fails all set point requests. Consider this argument for an automated start up of a view-only CimView.

Screen Security: CimView screens can be digitally signed using a valid X509 signing certificate with a private key to protect them. Tampering becomes detectable, and CimView can be configured to either warn that the signature is not valid, or it can prevent opening displays that do not match their signature. In addition, it validates that the signature was performed by a trusted certificate. Screen security configuration must be performed by a system administrator and is not intended for a regular CimView user. Every time a user opens a signed screen, the CimView application checks for the certificate that was used to sign. If the certificate is not available along with the screen, a relevant warning is displayed based on the settings. See the CIMPLICITY help topic “About Screen Security” for more information. https://www.ge.com/digital/documentation/cimplicity/version2023/oxy_ex-2/screens/topics/g_cimplicity_screens_about_screen_security.html .

Configure e-mail servers to filter out documents with the following extensions: .CIM, .CIMRT, .CTX, .CMS, .BCL, .BCLRT.

Ensure that any locations used to store CIMPLICITY project configuration files for all lifecycle phases have access restrictions so that only those responsible for performing configuration, testing, and production have access to these files.

Ensure that any documents to be put into these secure locations have a secure chain of custody before their transfer to the secure location.

Screen Version Control: A best practice is to manage screens as you would source code and store them in an access-controlled version control system such as git or svn. You can store them in the text CTX format to make it easier to see what changes were made to a screen file.

Want to Know More?

Search the "DisableSetpoints" method in the *CIMPLICITY User Guide*. This Cimview method allows an application to determine if a Cimview application session can perform setpoints.

4.3 CimEdit

CimEdit includes the capabilities of CimView and adds the ability to configure the CimView screens. CimEdit is often referred to as an Engineering workstation while CimView is an HMI.

A screen can be saved as a runtime-only screen (.cimrt) that cannot be edited in CimEdit. This prevents an attacker with access to CimEdit from changing the screen or objects on the screen through CimEdit. It is a good security practice to provide runtime-only screens to users that are performing monitoring and control but are not changing screens.

Save the same screen as an editable Cim screen that is not distributed to operators and view-only users. Engineers and administrators can then change this screen as needed and use it to update the corresponding runtime-only screen (.cimrt).

4.4 CIMPLICITY Plug-in for Configuration Hub

Configuration Hub:

Configuration Hub is a new centralized platform to configure all your Proficy products conveniently, offering access and configuration from any location. Within Configuration Hub, you can simultaneously view multiple Proficy applications, including Proficy Authentication, CIMPLICITY, iFIX, Historian, and Operations Hub, among others. This unified hub streamlines the management of various Proficy products and facilitates seamless monitoring and administration from a single interface.

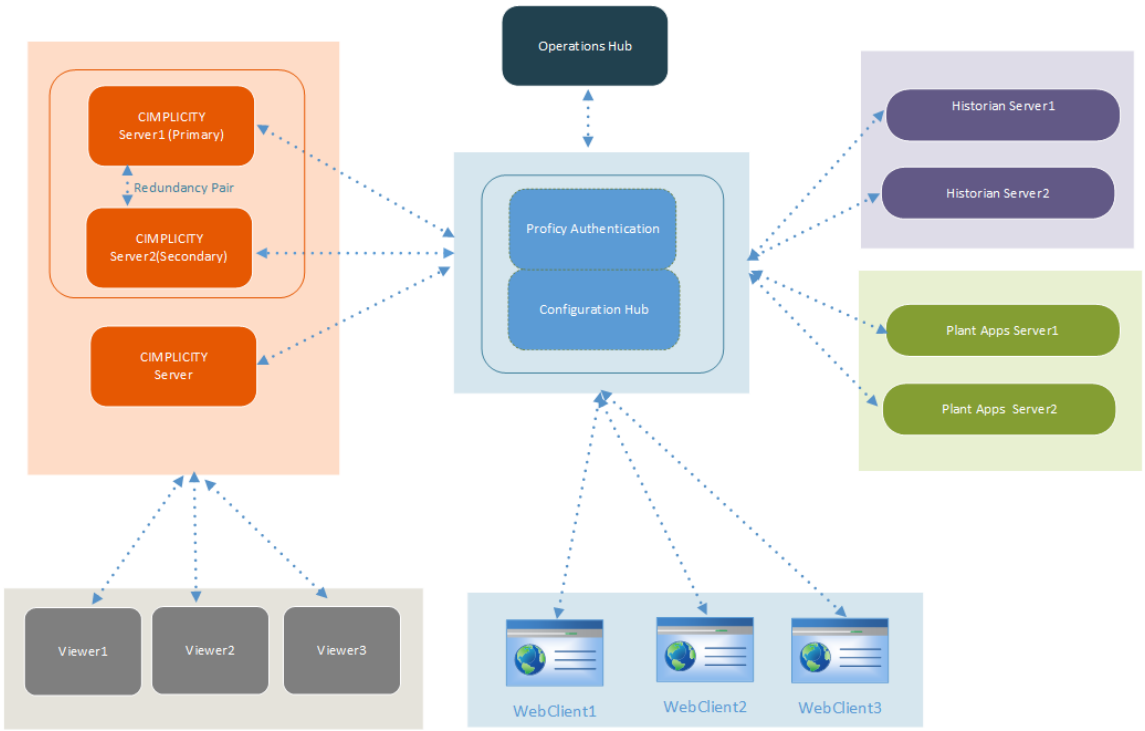
To enable a product's integration with Configuration Hub, it must first undergo registration. When multiple products complete the registration process with Configuration Hub, they become accessible for configuration through the hub. This means that once registered, these products can be conveniently configured and managed directly from the Configuration Hub interface.

Refer to CIMPLICTY documentation for registering CIMPLICITY-Plugin with Configuration-Hub .

4.4.1 Sample deployment Architectures:

Distributed Proficy Architecture:

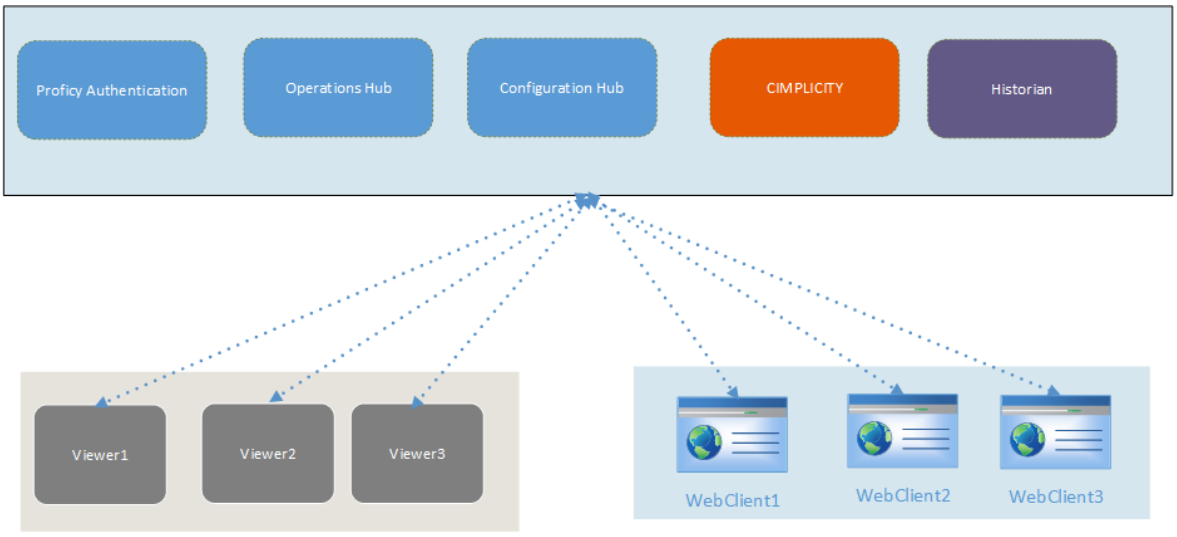
The recommended architecture for accessing Proficy Products from the web involves installing Proficy Authentication Server and Configuration Hub on a central node. By configuring all other Proficy products to work with this central node, users gain the ability to access Proficy products through a web interface. This centralized setup streamlines the security management and configuration access to Proficy applications, offering a more unified and user-friendly experience on the web.



Single Node Proficy Architecture:

Smaller applications that do not require redundancy can have CIMPLICTY installed on the same node alongside Configuration Hub, Proficy Authentication Server, and Operations Hub.

The Architecture looks like below:



Want to Know More?

Search “Configuration Hub” in the *CIMPLICITY User Guide*.

4.5 WebSpace

WebSpace is a server-based, thin client solution that is optimized for reliable, secure, and scalable remote CimView screen monitoring and control. Users access the WebSpace Web Server, part of a CIMPLICITY Server, using a web browser. This web client to web server communication can be protected using the encryption and authentication features available in SSL/TLS.

WebSpace must be installed and configured on the CIMPLICITY Server. The *Proficy WebSpace* tab in the *CIMPLICITY Options* window (see Figure 34) has a **Start Proficy WebSpace Server at boot time** check box under Configuration. Select this if using WebSpace. You can also set Webspace to automatically start via the Windows Services settings.

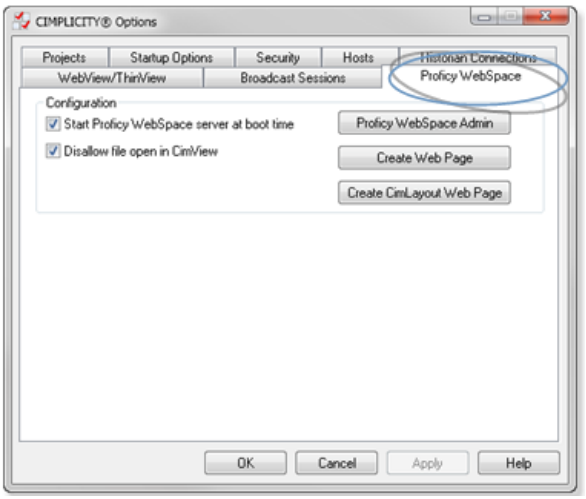


Figure 34 Configure WebSpace in CIMPLICITY Server

The **Disallow file open in CimView** check box prevents all WebSpace clients from viewing or controlling CimView screens. If selected, WebSpace cannot work. This setting allows for quickly stopping WebSpace in an emergency.

The **Create Web Page** button (see Figure 34) creates the login page for WebSpace and select the CimView screen to appear for WebSpace user login. Other screen options can also be set as part of web page creation (see Figure 35).

Most options are related to the look and feel of the WebSpace environment but there are two security control options to consider in the design phase. These options are:

- **Restrict** screen opening

  Users can only open CimView screens that are explicitly listed in the Open Screen and Overlay Screen actions. This provides another way to restrict what a WebSpace user can see and control.

- **Disable setpoints**

  Prevents a WebSpace user from having control capability. This is specifically useful for view-only WebSpace implementations.

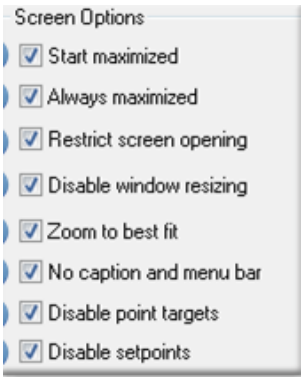


Figure 35 Select WebSpace Screen Options

Administering User Accounts

To access applications on a WebSpace server, clients must sign in to the server machine. When users start a WebSpace client, they are prompted for their user name and password. This information is optionally encrypted and passed to the Application Publishing Service running on the WebSpace server. The Application Publishing Service then performs the login operation using the standard multi-user features of Windows.

When a user signs in to a host and a domain is not specified, the service first attempts to authenticate the account on the local machine, followed by the machine's domain, and lastly the trusted domains. Users can override this default behavior and specify a domain by typing the domain name followed by a backslash (\) and their network user name in the User name box of the Sign In dialog, such as NORTH\johng. When a local user name on the WebSpace server is the same user name as a domain account, each with a different password, WebSpace treats them as two separate accounts.

Once a user is signed in, WebSpace relies on the server's operating system to provide the security necessary to run applications safely in a multi-user environment. Applications run in the security context of the client user to ensure private sessions. Access to all machines and network resources is governed by the operating system and the rights granted to individual user sessions.

Users must be able to log in interactively (locally) on the WebSpace server. Users must have local login rights in Local Security Policy, Domain Security Policy, and Domain Controller Security Policy.

4.6 Terminal Services

Microsoft's Terminal Services can run the CIMPLICITY CimView or CimEdit applications in a DMZ to provide a more secure environment and make deployment easier.

The primary security benefit is that an organization can focus on securing a small number of computers running terminal services rather than every client computer. These Terminal Servers, typically located in a DMZ, can be scheduled for prioritized security patching and enhanced security monitoring.

The CimView or CimEdit CIMPLICITY Clients need only be installed and maintained on the Terminal Servers rather than on each user computer in the Corporate Zone. The same security controls in the CIMPLICITY Server and CIMPLICITY Client described in earlier sections can be applied to CimView or CimEdit installed as terminal services applications in a DMZ.

There are a small number of additional security features in the Global Parameters that can affect the security of the Terminal Server CIMPLICITY Client connections. The most significant one is the TERMSERV_ALLOW_SETPOINTS parameter if its value is false. This prevents a set point action (control) from any Terminal Server connection. Organizations wanting to make screens viewable from the Corporate Zone but still restrict control to the Control System Zone can benefit from this feature.

The GSM_TERMSERV_CACHE_SIZE Global parameter restricts the number of screens that are cached in CimView. While being a performance issue, it also restricts the immediately available information if the Terminal Server or associated DMZ are compromised.

The reference architecture, in section Emergency Remote Access for Control and Administration, shows a Terminal Server being used for a remote control capability from an untrusted zone in the case of emergencies. Organizations must examine the need for remote control and then consider the risk of remote control; determining if it is prohibited beyond emergency use or allowed for some regularly occurring remote control. If remote control is allowed, the Terminal Server architecture represents the lowest risk method of providing this remote control.

There are numerous resources for deploying and securing Terminal Services and there is nothing unique about using Terminal Services in CIMPLICITY that alters this guidance.

Here are some of the main considerations:

- **RDP Full Connection vs. RDP Web Connection**

  RDP Full Connection offers encryption but is vulnerable to a man-in-the-middle attack if certificates are not deployed. Most organizations find more security and ease of use with an RDP web connection (if it is https), in conjunction with a web site certificate and good web server security practices.

- **Changing the Default RDP/Terminal Services Port**

  Changing the default Microsoft Terminal Services Port (TCP/3389) can prevent automated attacks from identifying the Terminal Server but may not stop a skilled attacker.

4.7 Webspace Plug-in for Operations Hub

The Webspace Plug-in for Operations Hub enables you to monitor and control production equipment and processes though a web browser based human machine interface (HMI) that is securely communicating to your SCADA system via an on-premise web server.

Refer to the Operations Hub documentation for information about securely deploying and configuring Operations Hub.

Refer to this guide and the CIMPLICITY documentation for information about securely deploying and configuring Webspace and the Webspace Plug-in for Operations Hub.

The Webspace Plug-in for Operations Hub consists of two additional components beyond the traditional CIMPLICITY and Webspace deployments:

- The Webspace Session Manager, running on the Webspace server, creates the CimView sessions running in Webspace and displayed by the plug-in. It also allows the plug-in to navigate to different CimView screens, according to the user's permissions.

- The Apache httpd server, shared with CIMPLICITY SCADA Web configuration, provides the external endpoints to access the Webspace Session Manager. httpd server is functioning purely as a reverse proxy server in this case.

Httpd server and the Webspace Session Manager communicate through an internal socket (as show in the **Data Flow Connection Descriptions** table) that does not need to be open in the firewall.

Security considerations during configuration in CIMPLICITY Options:

- When configuring the Windows Server Credentials, this is the Windows user under whose account all the CimView sessions will run. This should be a non-privileged account configured with the same permissions required for operator accounts. If using the recommendations in **Appendix A: Access Control List**, this would be a user in the CIM_OPER_USERS group.

Want to Know More?

Go to GE Operations Hub documentation at
https://www.ge.com/digital/documentation/opshub/windows/index.html

5. Server Connections

5.1 Remote Projects

A CIMPLICITY Server can retrieve, or pull, Project data from another CIMPLICITY Server by implementing a Remote Project. In the Control System Zone, this can be used to collect data from Projects that run on two or more CIMPLICITY Servers to a central CIMPLICITY Server. Selected points can be retrieved from a related ICS that is monitored and controlled as a Project on another CIMPLICITY Server.

The CIMPLICITY Remote Project capability is very important if users on a less trusted zone require access to a CIMPLICITY Server. One example of this might involve a WebSpace Server running on a CIMPLICITY Server in the Control System DMZ that provides ICS data and screens to Corporate Zone users. This example is outlined in the reference architecture described in section Remote Access to CIMPLICITY Screens Using WebSpace. In this example, the CIMPLICITY Server in the Control System DMZ accesses the data in the Control System Zone as a Remote Project.

The Remote Project requires that the Remote Registry Service runs on the CIMPLICITY Server that is the source of the data. This increases the attack surface and can provide an attacker with credentials or a working exploit with significant rights. The risk of this setting is based on the trust level of the zone that is allowed to access the remote registry, and it is an example of why the reference architecture, in section Remote Access to CIMPLICITY Screens Using WebSpace, has the WebSpace/CIMPLICITY Server in the Control System DMZ rather than in the Corporate Zone.

The CIMPLICITY Server that accesses the Remote Project requires the credentials for the *Remote Project* (see Figure 36). If the **Resident process use only** check box is selected on the *General* tab, the CIMPLICITY Server logs on to the Remote Project, but users must still log in to the Remote Project, and the user rights are based on this user login. Select this check box for most deployments.

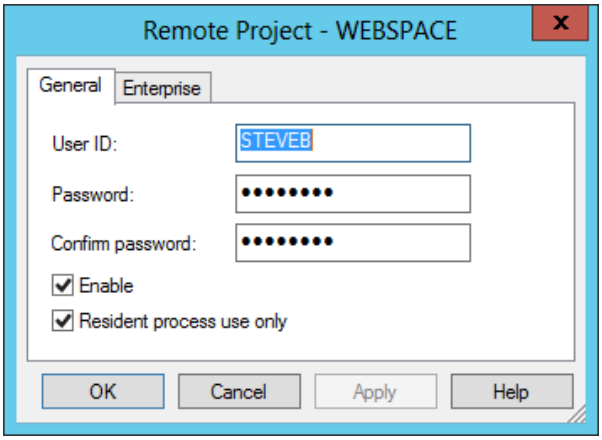


Figure 36 Remote Project Properties

CIMPLICITY Server to CIMPLICITY Server communications between security zones must use the CIMPLICITY Point Bridge feature. The source of data is a CIMPLICITY Server in the Control System Zone that obtains the point data from a PLC, RTU, instrument or other part of the process being monitored and controlled. The destination, the CIMPLICITY Server getting the data from the source CIMPLICITY Server, runs the Point Bridge process. The destination is in the less trusted zone if a Remote Project is used for ICS data export.

Point Bridge requires setting up a port and then a device in a Project on the destination CIMPLICITY Server. Points can then be created on the Project through *Point Properties* (see Figure 37). The configuration parameters on the *General* tab are the same as for local Projects; however, the **Read only** check box behaves slightly differently.

If the corresponding point on the source CIMPLICITY Server is set to read only, then the **Read only** check box for the point on the destination CIMPLICITY Server has no effect. A point on a Remote Project can be changed if the **Read only** check box on both the source and destination CIMPLICITY Servers are not selected. This can put the ICS and controlled process at risk if the destination CIMPLICITY Server is accessible from a less trusted zone.

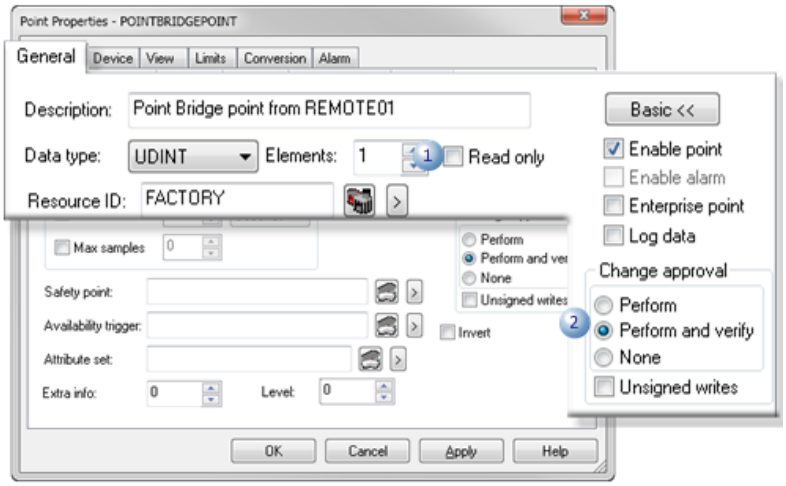


Figure 37 Set a Point to Read Only

Figure 38 shows where the device created for the Point Bridge is entered under the *Device* tab in *Point Properties*.

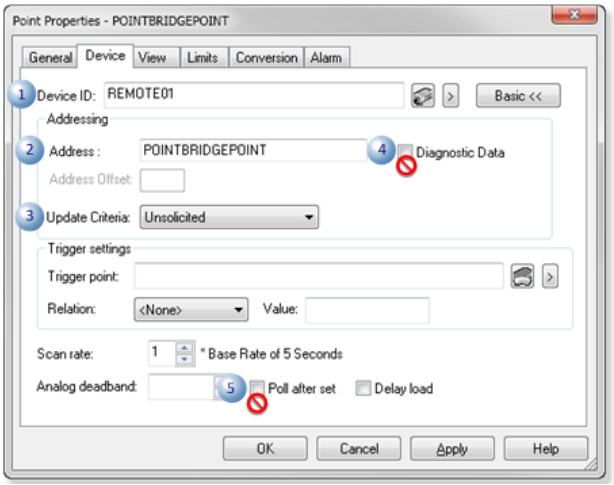


Figure 38 Configure a Point to Use the Point Bridge Device

5.2 CIMPLICITY Server to Historian

GE Historian provides historical ICS data to users in any zone without providing these users access to the CIMPLICITY Server and its control capability. One security practice is to push ICS historical data out to a DMZ. From there it can be made available to users and applications on the Corporate Zone or other less trusted zones without providing direct access to the Control System Zone.

The connection from the CIMPLICITY Server to Historian is set in the *Historian Connections* tab of the *CIMPLICITY Options* window (see Figure 39). The user name and password entered must be valid on Historian. The user name/password credentials are encrypted and stored in the CIMPLICITY Server but are not encrypted or hashed when sent over the network. They must not be used in an untrusted zone, such as the Corporate Network Zone or any other external zone, without additional security controls.

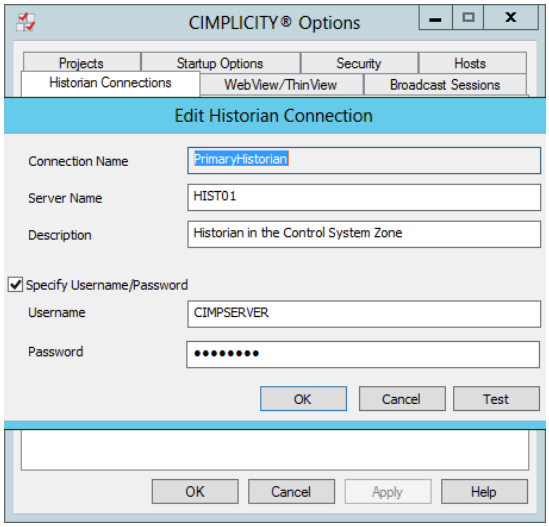


Figure 39 Configure a Historian Connection

The CIMPLICITY Server establishes a TCP session to Historian on port 14000. If the CIMPLICITY Server and Historian are in different zones, appropriate firewall rules must be applied.

5.3 CIMPLICITY Server to Alarm Cast Server

CIMPLICITY Alarm Cast is a high-volume message processing engine that can deliver CIMPLICITY Server alarms and other messages to a variety of devices and applications. A common use of Alarm Cast is to deliver alarms to mobile phones, an e-mail address, and other devices for support purposes. Alarm Cast supports common messaging protocols such as SMTP, SMTPS, ODBC, MS-SPEECH, SNPP, TAP, and UCP.

The security requirements for delivery of Alarm Cast messages in the Control System Zone are minimal because this is a trusted zone. This section assumes that Alarm Cast messages are sent to a less trusted network, typically a mobile data network or Internet, and a DMZ is used as described in the sample reference architecture, in section Historical Data and Alarms on Semi-Trusted Control System DMZ.

Alarm Cast Rules related to a Project's resources are configured in the CIMPLICITY Server in the Control System Zone. When a rule is met, the Alarm Cast Gateway forwards the message and any configured alarms and point values to the Alarm Cast Server in the Control System DMZ.

The Alarm Cast Gateway on the CIMPLICITY Server in the Control System Zone is a client to the Alarm Cast Server in the Control System DMZ. An Alarm Cast Gateway client must be created on the CIMPLICITY Server (see Figure 40). The user ID must match an account on the Alarm Cast Server, and it must be an account created for this remote connection and purpose. Do not use the default Administrator account.

Select the **Trusted** check box on *Client Properties* because there is no opportunity for an interactive login. Use the Authorization Code feature (see section Client Configuration) to prevent spoofing of the default user ID.

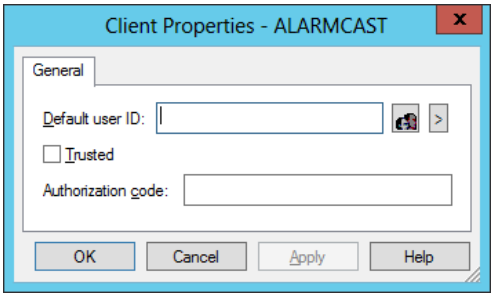


Figure 40 Client Properties for the Alarm Cast Gateway

The Alarm Cast Gateway is configured for each Project in Project>Equipment>Alarm Cast Gateway>User ID. This is the User ID set in Figure 40. Double clicking the User ID opens the *Alarm Cast Gateway* window. The *Settings* tab (see Figure 41) is where the Alarm Cast Alarm Server location is set by Host Name and the CP port that is listening on the Alarm Cast Server. These configuration parameters are required to configure the firewall that forms the cyber security perimeter.

NOTE: Each project has a unique listening TCP port on the Alarm Cast Server.

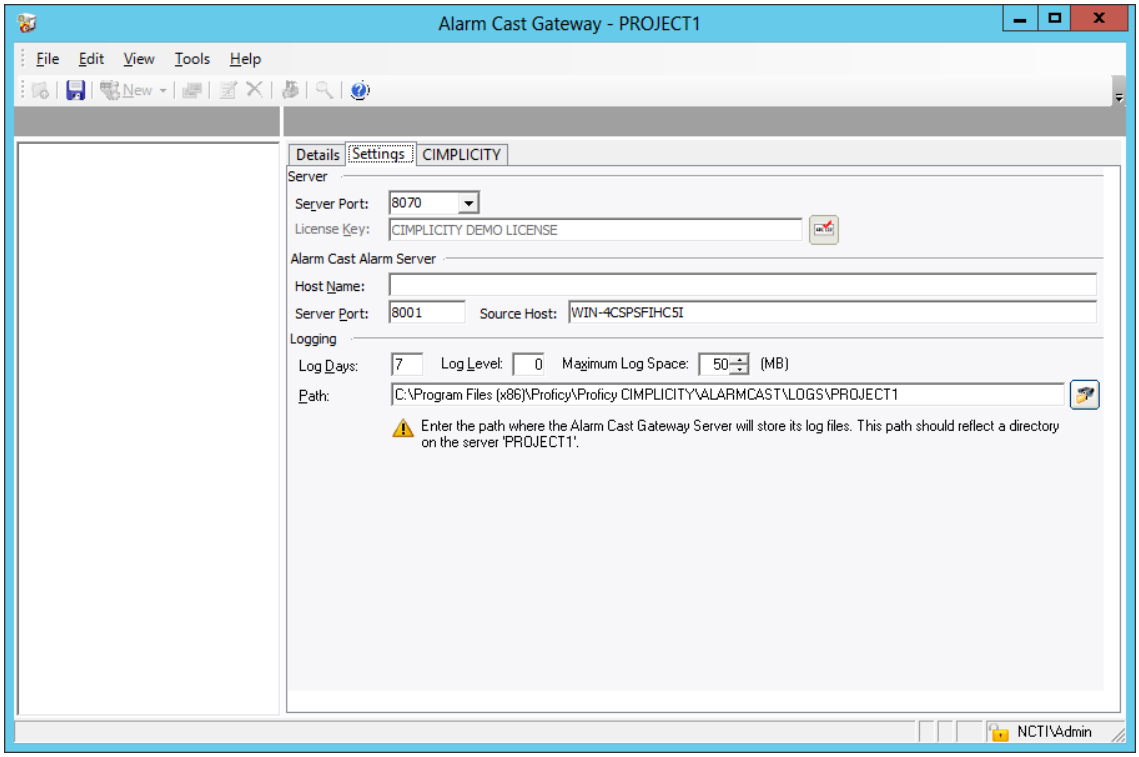


Figure 41 Client for the Alarm Cast Gateway

The authentication mode for the CIMPLICITY Server carries over to the Alarm Cast Gateway.

- If CIMPLICITY authentication is deployed, a set of CIMPLICITY Server credentials must be entered in the *CIMPLICITY* tab of the *Alarm Cast Server* window (see Figure 41).
- If Windows authentication is deployed, a Tools tree with a Users folder is added to the left pane of the Alarm Cast Gateway window. This also creates a *Security* tab in the *Alarm Cast Server* window. The users who require access to the Alarm Gateway must be added. Users must log in when they access the Alarm Gateway.
- If Windows Trusted is deployed, the process is similar to Windows authentication except that logging in is not required when an authenticated Windows user accesses the Alarm Gateway.

The biggest risk reduction comes from the architecture rather than any configuration parameter. By pushing the messages from the CIMPLICITY Server in the Control System Zone to the Alarm Cast Server in the Control System DMZ, the need for a less trusted zone to access the Control System Zone for alarm messages is eliminated.

NOTE: Consider the security consequences of sending ICS messages through less trusted zones and configure the Alarm Cast Server in the Control System DMZ appropriately.

Want to Know More?

Search "Alarm Cast Administrator - Key Features" in the *CIMPLICITY User Guide*.

5.4 Change Management

Change management is an important part of maintaining a secure and reliable ICS. The CIMPLICITY solution works with the Change Management (PCM) application to automate change management for CIMPLICITY Computers and Projects.

PCM supports the necessary features in a change management program, such as check out and check actions, comparing a deployed Project with a Project in PCM, and tracking changes after-incident investigation. Use the CIMPLICITY Server user, role, client, resource, and point security controls to define who can make a change and from where. PCM is designed to enforce a change management structure for authorized users.

The CIMPLICITY Server is a client that must log in to the PCM. The default credentials listed in the PCM manual must have been changed and replaced by unique credentials on the PCM for CIMPLICITY Server to PCM login (see Figure 42).

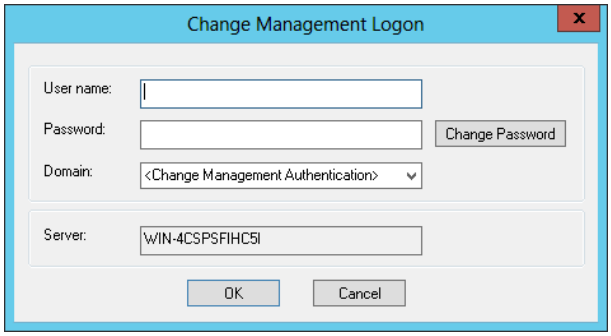


Figure 42 Login Credentials to Change Management

The *Change Management* tab on the *Computer Properties* and *Project Properties* windows has some security features (see Figure 43). The key settings are related to the login options. Selecting the **Prompt for user name and password at login** check box requires logging on to CIMPLICITY when Change Management is started even when the CIMPLICITY Server login is automated. This is useful for users in the control room who do not log in for operational activities but need to be identified when making changes to a CIMPLICITY Computer or Project.

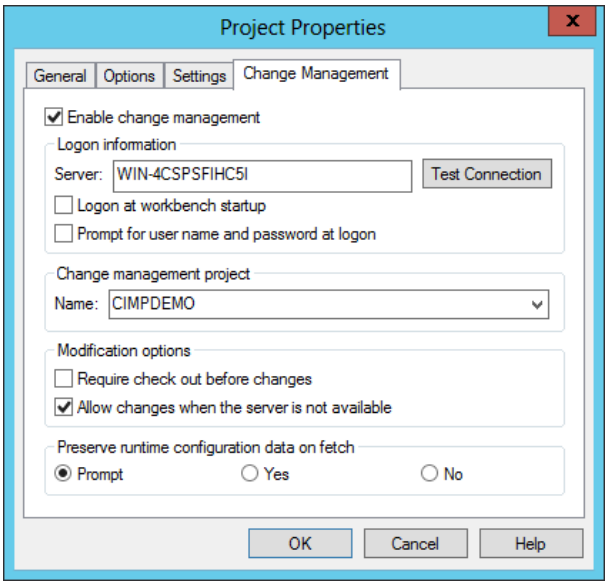


Figure 43 Change Management Settings in CIMPLICITY Server Backup

6. Cyber Maintenance

The CIMPLICITY HMI/SCADA system and associated products, applications, and networks comprising ICS require maintenance just as physical equipment that is monitored and controlled in a physical process requires maintenance.

If CIMPLICITY is installed and not maintained, it is operating in a “run to fail” maintenance plan. This maintenance approach is rarely recommended or used due to the failure unpredictability, increased outage times, and cost after failure. Without a cyber maintenance plan, any cyber system degrades over time into a less secure and more fragile system. Therefore, it is essential to implement a cyber maintenance plan for a CIMPLICITY HMI/SCADA system.

This section covers some of the key elements of a cyber maintenance plan. A risk management team must determine the specific requirements for each of these elements, particularly requirements related to frequency and time.

6.1 Backup and Recovery

ICS has traditionally relied on redundancy, such as redundant servers, networks, and control rooms, to prevent a cyber incident from causing an ICS outage. Redundancy is typically not an effective control against a cyber attack because the redundant system is identical to the primary system and is vulnerable to the same attack. Assume that a cyber attack always takes out the primary and any redundant systems, and these systems must be completely rebuilt.

The appropriate level of management must set a Recovery Time Objective (RTO) for the CIMPLICITY HMI/SCADA system. The RTO is based on a capability rather than on the entire set of computers, applications, and networks, and an RTO may be different for different components in ICS. For example, an organization may have an RTO of six hours to recover the ability to monitor and control a process using CIMPLICITY, and an RTO of 48 hours to recover the ability to share historical data with the Corporate Zone.

The RTO may not require all systems of a specific type to be recovered. For example, a Control System Zone with redundant CIMPLICITY Servers, 15 CIMPLICITY Clients and redundant local area networks (LANs) may have an RTO that requires a single CIMPLICITY Server, two CIMPLICITY Clients, and a single LAN to provide the required monitoring and control capability.

In the Control Zone, the data on Historian must have a backup plan to back up the SQL server for the Alarms and Events and data archives.

Want to Know More?

Search “Backing up an Archive” and “Backing Up Alarms”, “Alarm Backup” and “Back up a selected archive” in the *Historian User Guide.*

Once management has set one or more RTOs, then the recovery capability should be designed, implemented and periodically tested. Very short RTOs are achievable, but in general, the cost of recovery increases as an RTO is decreased.

The first step in a recovery program is to make sure the necessary software and hardware is available. For CIMPLICITY, the software is needed to rebuild the platform/OS, the software to install the CIMPLICITY and associated GE applications, and the CIMPLICITY Project specific data. Implement a backup process and schedule and periodically check this process. The frequency of the backup is determined by a Recovery Point Objective (RPO) set by the appropriate level of management.

The RPO determines the amount of historical data that management is prepared to lose. The RPO in an ICS is often less than the RPO on a Corporate Zone computer because an ICS configuration typically does not change often, and important historical data is often exported from the CIMPLICITY Server to the Historian or a database.

The RTO guides the decision on how to recover the CIMPLICITY Server and other computer platforms. For recovery, back-up material can be used, such as media, image, or a virtual machine, or connect a cold standby server for a very short RTO. Always update the back-up material whenever the operating system or applications are updated.

Back up the CIMPLICITY Project files and other installation-specific information at least as often as the RPO.

CIMPLICITY configuration data that applies to CIMPLICITY data as a system outside the scope of a project is stored in this directory:

```
C:\Program Files (x86)\Proficy\Proficy CIMPLICITY\data
```

Copy this directory and all its contents along with the Project directories and all their contents, to a backup location. A CIMPLICITY Project folder contains a file with the *<project name>*.gef structure. Always perform a backup on the entire contents of the Project folder, including subdirectories. Multiple Projects can exist on a computer and it must be understand which of these Projects comprise the solution.

If a Project is stopped, use the Windows mechanisms to copy all Project directories to a backup location. In this case, select the file menu on the workbench titled “Copy to Project” and select a destination in another directory. A copy is then made in the selected destination. This ensures files that are generally locked are handled correctly. Note that backing up a Project does not require that it be stopped first.

The Historian Alarm backup can occur while the system is in operation. However, by performing this backup during off hours when alarms are minimal, any delays in logging alarms is reduced to a minimum.

Want to Know More?

Search "Copy to Project" in the *CIMPLICITY User Guide.*

6.1.1 Backup system

To minimize downtime, perform full backups of each machine. Consider a backup software solution that provides encryption, verification, incremental backups, audit logging, and secure offsite storage.

Update the backups when patches are installed and when configuration changes are performed. Consider the availability of offline spare hardware as part of the backup solution, and the use of virtualized systems for an automation solution. Many hardware virtualization platforms have their own backup issues to evaluate.

Consider performing back up operations at the host layer instead of at the guest OS layer. Review best practices for backups in virtualization systems in an automation solution. Virtualization provides the maximum flexibility for restoring machine images. In many cases, CIMPLICITY server redundancy can provide continued operation while a lost server is restored.

6.1.2 Restoration from Backup

The backup and restore solution must restore a full system or a specific subset of files. Restoration requirements may need to only recover a CIMPLICITY Project directory.

Restoring a back up of a CIMPLICITY Project is as simple as restoring the Project directory, as explained in section Backup and Recovery,

Restore the CIMPLICITY global configuration by restoring the contents of this backup directory:

```
C:\Program Files (x86)\Proficy\Proficy CIMPLICITY\data
```

During a restore, moving the suspect Project directory to another location may be required. Retaining this directory for comparison with the backup is necessary to identify any changes that were not preserved in the backup.

When restoring a system with CIMPLICITY components or just a Project, note that saved points contain values from the time of the backup. Make sure there is a procedure in place to review and correct these values as desired.

Use a visual difference tool to compare the restored backup folder to the current Project folder in use. This can display unexpected differences, such as missing files or configuration changes. Expect files in a Project's log directory to frequently change as the Project continues to run.

6.1.3 Data Retention and Encryption of Data

Encryption of Data at Rest

Whether in SQL, Historian or another location, encrypting data at rest is recommended.

SQL supports native encryption of a database.

For Historian information, consider encrypting whole hard drives. The recommendation is to place archives on drives with Bitlocker drive encryption enabled.

Always consult the Corporate IT policy on drive encryption standards and procedures as well as data retention plans.

Older historical data is often archived to a different database. The ICS environment is only responsible for maintaining information for the required scope of time for operations.

Want to Know More?

- For information on Transparent Data Encryption (TDE) for SQL database files, go to https://msdn.microsoft.com/en-us/library/bb934049(v=sql.120).aspx
- For information on Bitlocker drive encryption, go to https://msdn.microsoft.com/en-us/windows/hardware/commercialize/manufacture/desktop/bitlocker-drive-encryption
- For information on maintaining CIMPLICITY in SQL, search “Configure the Logging Maintenance Actions” in the CIMPLICITY User Guide.
- Search “Using ihBackupAlarms.exe to Backup Alarms from the Command Line” and “Purging Alarms”, “Using ihPurgeAlarms.exe to Purge Alarms from the Command Line” and “Adding, Backing Up, or Restoring an Archive” and “Data Store Maintenance Screen” in *Historian User Guide.*

6.2 Security Patching and Software Updates

Cyber maintenance includes updating software to apply security patches and ensure the software is on a supported version. Create and maintain software inventory to assist with this aspect of cyber maintenance.

All software that runs on an ICS must be supported by the vendor. GE, Microsoft, and third-party application vendors who typically provide years of advance notice before declaring a version end of life/out of support. Annually review the end of life/out of support status of all software. Develop and implement a plan to update the OS, GE application, and all required third-party applications before reaching end of life/out of support status.

The frequency of applying security patches and updating software is a business and risk management decision. When making this decision, answer the following questions:

- Is the computer or device that is being patched accessible from a less trusted zone? The sample reference architectures (see Section Sample Reference Architectures) first focus on security patching and particularly on computers and applications in DMZ, and then to the CIMPLICITY Servers in the Control System Zone sending data to applications in the Control System DMZ.
- Does the installation have a test system where the security patches are tested before deployment?
- Does the ICS have redundancy so that one instance of a computer or application can be patched while leaving the other instance as-is for a set time to verify that the security patch does not affect operations? Leveraging redundancy and applying security patches in phases significantly reduces the time of an outage in the rare case of a security patch problem.

Due to the testing and phased rollout required to prevent outages caused by security patch incompatibility, security patches cannot be applied once a month to the Control System Zone like the Corporate Zone. Consider different security patching frequencies for systems based on where they are accessed, but make sure all software is patched periodically.

6.3 Periodic Project, User, Role and Resource Auditing

Sections Securing the CIMPLICITY Server and Client Connections discuss the security-related configuration decisions made for CIMPLICITY Server Projects, users, roles and resources. The configuration of these items determines the security controls in the CIMPLICITY Server and the privileges of each user in the CIMPLICITY Server.

The security posture of a system can degrade over time, particularly in user privileges. Users leave an organization, change roles, or require temporary privileges and other status changes that often are not addressed in a CIMPLICITY Server or Active Directory user management. More troubling are instances where a user is granted privileges without following the approved process.

A good security practice is to periodically verify, typically once a year, that all security settings have the correct controls and the user management settings are up to date. If there are significant variances between the actual settings and privileges and the expected settings and privileges, perform an investigation to determine how this gap occurred and determine which processes to enforce or change to prevent this in the future.

6.4 Log Aggregation and Security Monitoring

Cyber maintenance of security logs has two important facets. First, aggregate and store security logs on a system not performing the logging so the security logs are available for an after-incident investigation. There are a variety of log aggregation tools and the CIMPLICITY Server supports a variety of methods to send security logs to a log aggregation server. Design and implement a method for aggregating and archiving security logs. Periodically review this method to verify all logs are available when needed.

The second cyber maintenance activity related to security logging is monitoring to detect intrusion attempts, compromises, and other unauthorized or unexpected activity in the ICS. Security log files are generated by CIMPLICITY, the OS, routers, switches, firewalls, anti-virus, IDS sensors, and other applications and devices. Many organizations have deployed a Security Incident and Event Management (SIEM) service in the Corporate Zone to centralize security monitoring. Selecting a SIEM with reporting interfaces that match preferred notification of intrusion mechanisms (such as, email and text and text-to-speech) is important. Separate the duties of the administrators of the core system from the SIEM administrator duties.

Consider whether to forward security logs from the Control System Zone and any DMZ to the SIEM service for monitoring. A SIEM system can detect security compromises when configured to do so. For example, a SIEM system can be configured to aggregate event logs. CIMPLICITY event logs for $LOGIN_FAILURE and $LOGIN and $LOGOUT are events of interest that can be propagated to a SIEM system. Determine if the events listed in the section “CIMPLICITY Event Alarms” in the *CIMPLICITY User Guide* should be sent to the SIEM for analysis of unusual patterns.

Given that the Control System Zone is a special purpose zone, without Internet browsing, e-mail, and other typical user application-related communication, typically the alarm thresholds are set for ICS-related security events in the SIEM service to lower thresholds than the thresholds for Corporate Zone security events.

The CIMPLICITY Server has a set of System Sentry Power Tools that can log an alarm on Windows Performance Counters, Remote Access Servers, SQL Server, and an IIS Web Server. System Sentry points can be configured to identify performance issues, security related or other, before they become an issue that affects operations. An example is a point and corresponding alarm that can be set to monitor the percent of free space on a drive or the CPU utilization. This type of performance monitoring is important to detect the impact of cyber incidents on an ICS.

The Excel add-in for Historian mechanism is another method to provide a simple way to review and interactively explore the alarms and events logged to Historian. Queries can be conducted to find specific security related events.

Want to Know More?

Search these topics in the *CIMPLICITY User Guide:*

- Security Audit Trail Options
- CIMPLICITY Event Alarms
- Configure Point Alarms
- Set Alarm Options
- About CIMPLICITY Integration with Historian
- Select the Historian Logging Option(s)
- Define the Historian Connection

6.5 Root Certificate Authorities

A process is recommended for a periodic review of all new trusted root certificate authorities on the operating system. If unknown certificates appear, investigate and verify whether they are trusted. Such a process ensures only authorized certificates are installed. Remove any certificates that are from an unknown source.

Appendix A Access Control List Power Shell Script

The access control list power shell script can be used to set up secure access to your CIMPLICITY project.

Create a file named **SetUpCIMPLICITYACLs.ps1** at the following location:
`c:\tools\`

From an administrator powershell prompt, enter the following

- to adjust the install ACLs:
  `c:\tools\SetUpCIMPLICITYACLs.ps1`
- to adjust the ACLs for a new project:
  `c:\tools\SetUpCIMPLICITYACLs.ps1 “c:\cimprojects\a_project_folder\” the_project_name`

Enter the following script into **SetUpCIMPLICITYACLs.ps1**:

```
Param(
   [string]$project_dir,
   [string]$project_name
 )

function RemoveAllAccessRulesForUser([string]$file_name, [string]$arg_user)
{
   $dir_exist = Test-Path -Path $file_name -PathType Any
   if ($dir_exist)
   {
      $file_acl = Get-Acl $file_name
      $file_acl.SetAccessRuleProtection($true,$true)
      Set-Acl $file_name $file_acl

      $file_rule_w = New-Object
system.security.accesscontrol.filesystemaccessrule($arg_user,"Modify", "Allow")
      $file_acl.RemoveAccessRuleAll($file_rule_w)

      Write-Host "RemoveAllAccessRulesForUser " $file_name
      Set-Acl $file_name $file_acl
   }
   else
   {
      Write-Host "RemoveAllAccessRulesForUser No file:" $file_name
   }
}

function MakeReadOnlyFileForUser([string]$file_name, [string]$arg_user)
{
   $dir_exist = Test-Path -Path $file_name -PathType Any
   if ($dir_exist)
   {
      # first make a clean slate of no access rulls then add the read access
      RemoveAllAccessRulesForUser $file_name $arg_user
```

```
      $file_acl = Get-Acl $file_name
      $file_rule_r = New-Object
system.security.accesscontrol.filesystemaccessrule($arg_user,"Read", "Allow")
      $file_acl.SetAccessRule($file_rule_r)

      Write-Host "MakeReadOnlyFileForUserNoSubs " $file_name

      Set-Acl $file_name $file_acl
   }
   else
   {
      Write-Host "MakeReadOnlyFileForUserNoSubs No file: " $file_name
   }
}

function MakeReadOnlyFolderForUser([string]$file_name, [string]$arg_user)
{
   $dir_exist = Test-Path -Path $file_name -PathType Any
   if ($dir_exist)
   {
      # first make a clean slate of no access rulls then add the read access
      RemoveAllAccessRulesForUser $file_name $arg_user

      $file_acl = Get-Acl $file_name
      $file_rule_r = New-Object
system.security.accesscontrol.filesystemaccessrule($arg_user,"Read,
ListDirectory","ContainerInherit,ObjectInherit", "None", "Allow")
      $file_acl.SetAccessRule($file_rule_r)

      Write-Host "MakeReadOnlyFolderForUser " $file_name

      Set-Acl $file_name $file_acl
   }
   else
   {
      Write-Host "MakeReadOnlyFolderForUser No file: " $file_name
   }
}

function MakeModifyFolderForUser([string]$file_name, [string]$arg_user)
{
   $dir_exist = Test-Path -Path $file_name -PathType Any
   if ($dir_exist)
   {
      $file_acl = Get-Acl $file_name
      $file_rule_w = New-Object
system.security.accesscontrol.filesystemaccessrule($arg_user,"Modify",
"ContainerInherit,ObjectInherit", "None", "Allow")
      $file_acl.SetAccessRule($file_rule_w)
      Write-Host "MakeModifyFolderForUser " $file_name

      Set-Acl $file_name $file_acl
   }
   else
   {
      Write-Host "MakeModifyFolderForUser No file: " $file_name
   }
}
```

```
function MakeModifyFileForUser([string]$file_name, [string]$arg_user)
{
   $dir_exist = Test-Path -Path $file_name -PathType Any
   if ($dir_exist)
   {
      $file_acl = Get-Acl $file_name
      $file_rule_w = New-Object
system.security.accesscontrol.filesystemaccessrule($arg_user,"Modify", "Allow")
      $file_acl.SetAccessRule($file_rule_w)
      Write-Host "MakeModifyFileForUser " $file_name

      Set-Acl $file_name $file_acl
   }
   else
   {
      Write-Host "MakeModifyFileForUser No file: " $file_name
   }
}

function SetUserFoldersACLS([string]$root_dir, [string]$user_arg, [string[]]
$no_access_folders, [string[]] $readonly_access, [string[]] $read_write_access)
{
   foreach($folder in $no_access_folders)
   {
      $full_path = $root_dir + $folder
      RemoveAllAccessRulesForUser $full_path $user_arg
   }

   foreach($folder in $readonly_access)
   {
      $full_path = $root_dir + $folder
      MakeReadOnlyFolderForUser $full_path $user_arg
   }

   foreach($folder in $read_write_access)
   {
      $full_path = $root_dir + $folder
      MakeModifyFolderForUser $full_path $user_arg
   }
}

function SetInstallDirPermisions()
{
   $install_root = ($env:CIMPATH).Substring(0,$env:CIMPATH.LastIndexOf('\')+1)

   Write-Host "SetInstallDirPermisions install_root = " $install_root

   [string[]] $users_no_access_install_folders = "data", "ALARMCAST", "arc",
"data", "lock", "log", "etc", "mdac", "perfserv", "scripts", "Web", "WebPages",
"AEOPC", "api", "bsm_data", "cimpole", "classes", "dc", "docs", "drivers",
"extras", "firewall", "fonts", "GefVCR", "OpenSSL", "projects",
"PublishSubscribeDelivery", "report", "ScadaConfigPki",  "symbols", "Series90",
"SystemSentry", "uninstall"
```

```
   [string[]] $runtime_no_access_install_folders = "AEOPC", "api", "bsm_data",
"cimpole", "classes", "dc", "docs", "drivers", "extras", "firewall", "fonts",
"GefVCR", "projects", "PublishSubscribeDelivery", "report", "symbols", "Series90",
"SystemSentry", "uninstall"
   [string[]] $runtime_read_only_install_folders = "etc", "OpenSSL", "mdac",
"perfserv", "scripts", "WebPages", "ScadaConfigPki"
   [string[]] $runtime_read_write_install_folders = "data", "ALARMCAST", "arc",
"data", "lock", "log", "Web"

   [string[]] $config_no_access_install_folders = "AEOPC", "cimpole", "dc",
"drivers", "fonts", "GefVCR", "projects", "PublishSubscribeDelivery", "report",
"ScadaConfigPki", "uninstall", "Web"
   [string[]] $config_read_only_install_folders = "api", "classes", "docs",
"extras", "firewall", "mdac", "OpenSSL", "perfserv", "SystemSentry"
   [string[]] $config_read_write_install_folders = "arc", "bsm_data", "etc",
"data", "ALARMCAST", "data", "lock", "log", "scripts", "WebPages", "symbols",
"Series90"

   [string[]] $operators_no_access_install_folders = "ALARMCAST", "lock", "etc",
"scripts", "Web", "WebPages", "AEOPC", "api", "bsm_data", "cimpole", "classes",
"dc", "docs", "drivers", "extras", "firewall", "fonts", "GefVCR", "OpenSSL",
"projects", "PublishSubscribeDelivery", "report", "ScadaConfigPki", "uninstall"
   [string[]] $operators_read_only_install_folders = "arc", "data", "mdac",
"perfserv", "symbols", "SystemSentry", "Series90"
   [string[]] $operators_read_write_install_folders = "log"

   [string[]] $admin_no_access_install_folders
   [string[]] $admin_read_only_install_folders
   [string[]] $admin_read_write_install_folders = "AEOPC", "ALARMCAST", "api",
"arc", "bsm_data", "cimpole", "classes", "data", "dc", "docs", "etc", "extras",
"firewall", "fonts", "GefVCR", "lock", "log", "mdac", "OpenSSL", "perfserv",
"projects", "PublishSubscribeDelivery", "report", "Series90", "symbols",
"SystemSentry", "uninstall", "Web", "WebPages", "Drivers", "Scripts",
"ScadaConfigPki"


   foreach($folder in $users_no_access_install_folders)
   {
      $full_path = $install_root + $folder
      RemoveAllAccessRulesForUser $full_path 'users'
   }

   SetUserFoldersACLS $install_root 'CIM_RUNTIME_USERS'
$runtime_no_access_install_folders $runtime_read_only_install_folders
$runtime_read_write_install_folders

   SetUserFoldersACLS $install_root 'CIM_OPER_USERS'
$operators_no_access_install_folders $operators_read_only_install_folders
$operators_read_write_install_folders

   SetUserFoldersACLS $install_root 'CIM_CONFIG_USERS'
$config_no_access_install_folders $config_read_only_install_folders
$config_read_write_install_folders

   SetUserFoldersACLS $install_root 'CIM_ADMIN_USERS'
$admin_no_access_install_folders $admin_read_only_install_folders
$admin_read_write_install_folders
}
```

```
function SetProjectDirPermisions([string]$site_root, [string] $project_name)
{
   Write-Host "SetProjectDirPermisions site_root = " $site_root


   $users_no_access_project_folders ="RCO", "alarm_help", "arc", "data", "lock",
"log", "pki", "Recipes", "master", "scripts", "SPC", "screens"

   $runtime_no_access_project_folders = "screens"
   $runtime_read_only_project_folders = "scripts", "SPC"
   $runtime_read_write_project_folders = "RCO", "alarm_help", "arc", "data",
"lock", "log", "pki", "Recipes", "master"

   $operators_no_access_project_folders = "scripts", "SPC", "RCO", "alarm_help",
"arc", "data", "lock",  "pki", "Recipes", "master"
   $operators_read_only_project_folders = "screens"
   $operators_read_write_project_folders = "log"

   $config_no_access_project_folders
   $config_read_only_project_folders
   $config_read_write_project_folders = "screens", "scripts", "SPC", "RCO",
"alarm_help", "arc", "data", "lock", "log", "pki", "Recipes", "master"

   $admin_no_access_project_folders
   $admin_read_only_project_folders
   $admin_read_write_project_folders = "screens", "scripts", "SPC", "RCO",
"alarm_help", "arc", "data", "lock", "log", "pki", "Recipes", "master"


   $gef_file_name = $site_root + $project_name + ".gef"

   Write-Host "SetProjectDirPermisions project file = " $gef_file_name


   foreach($folder in $users_no_access_project_folders)
   {
      $full_path = $site_root + $folder
      RemoveAllAccessRulesForUser $full_path 'users'
   }

   MakeModifyFileForUser $gef_file_name 'CIM_RUNTIME_USERS'
   MakeModifyFileForUser $gef_file_name 'CIM_CONFIG_USERS'
   MakeModifyFileForUser $gef_file_name 'CIM_ADMIN_USERS'

   MakeReadOnlyFileForUser $gef_file_name 'CIM_OPER_USERS'


   SetUserFoldersACLS $site_root 'CIM_RUNTIME_USERS'
$runtime_no_access_project_folders $runtime_read_only_project_folders
$runtime_read_write_project_folders

   SetUserFoldersACLS $site_root 'CIM_OPER_USERS'
$operators_no_access_project_folders $operators_read_only_project_folders
$operators_read_write_project_folders
```

```
   SetUserFoldersACLS $site_root 'CIM_CONFIG_USERS'
$config_no_access_project_folders $config_read_only_project_folders
$config_read_write_project_folders

   SetUserFoldersACLS $site_root 'CIM_ADMIN_USERS' $admin_no_access_project_folders
$admin_read_only_project_folders $admin_read_write_project_folders
}

function ReadDirPermissions($directory, $state)
{
    If ($directory -eq $project_dir)
    {
        $fileName = "_Project"
    }
    Else
    {
        $fileName = "_Install"
    }
    $fileName = "C:\Permissions" + $fileName + $state + ".CSV"

    Get-ChildItem $directory -recurse | Get-Acl | Format-List > $fileName
}

function CreateCIMPLICITYLocalGroups()
{
   $Computer = $env:COMPUTERNAME
   $adsi = [ADSI]("WinNT://$Computer")

   $adminGroup = $adsi.Children.Find('administrators', 'group')

   try
   {
      $groupCimAdmin = $adsi.Children.Find('CIM_ADMIN_USERS', 'group')
   }
   catch
   {
     $groupCimAdmin = $null
   }

   if(!$groupCimAdmin)
   {
      $groupCimAdmin = $adsi.Create('Group', 'CIM_ADMIN_USERS')
      $groupCimAdmin.setinfo()
      $groupCimAdmin.description = 'Users that administer the CIMPLICITY system'
      $groupCimAdmin.setinfo()
      # The CIMPLICITY administrators, and runtime users need to be in the
administrators group
      $adminGroup.Add(("WinNT://$Computer/CIM_ADMIN_USERS"))
   }

   try
   {
      $groupConfig = $adsi.Children.Find('CIM_CONFIG_USERS', 'group')
   }
   catch
   {
     $groupConfig = $null
   }
```

```
   if(!$groupConfig)
   {
      $groupConfig = $adsi.Create('Group','CIM_CONFIG_USERS')
      $groupConfig.setinfo()
      $groupConfig.description = 'Users that configure CIMPLICITY projects'
      $groupConfig.setinfo()
   }

   try
   {
      $groupOper = $adsi.Children.Find('CIM_OPER_USERS', 'group')
   }
   catch
   {
     $groupOper = $null
   }

   if(!$groupOper)
   {
      $groupOper = $adsi.Create('Group','CIM_OPER_USERS')
      $groupOper.setinfo()
      $groupOper.description = 'Users that run CimView, and other operator
applications'
      $groupOper.setinfo()
   }

   try
   {
      $groupRuntime = $adsi.Children.Find('CIM_RUNTIME_USERS', 'group')
   }
   catch
   {
     $groupRuntime = $null
   }

   if(!$groupRuntime)
   {
      $groupRuntime = $adsi.Create('Group','CIM_RUNTIME_USERS')
      $groupRuntime.setinfo()
      $groupRuntime.description = 'Users that all the CIMPLICITY project processes
can run as, including w32rtr.exe'
      $groupRuntime.setinfo()
      # The CIMPLICITY administrators, and runtime users need to be in the
administrators group
      $adminGroup.Add(("WinNT://$Computer/CIM_RUNTIME_USERS"))
   }
}

CreateCIMPLICITYLocalGroups

if(($project_dir).length -gt 0)
{
   SetProjectDirPermisions $project_dir $project_name
}
else
{
 SetInstallDirPermisions

 }
```