These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and GE makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that GE may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the GE products referenced herein.

GE may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

Public Information – This document contains non-sensitive information approved for public disclosure.

GE provides the following document and the information included therein as is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for particular purpose.

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

Revised: Jan 2019
Issued: March 2017


* Indicates a trademark of General Electric Company and/or its subsidiaries. All other trademarks are the property of their respective owners.

We would appreciate your feedback about our documentation. Please send comments or suggestions to controls.doc@ge.com
## Document Updates

<table>
<thead>
<tr>
<th>Revision</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>C</strong></td>
<td>Create and Deploy SDI Certificates for WorkstationST Features</td>
<td>Added this section to provide the procedure to create and deploy certificates for clients that send SDI commands to the controller.</td>
</tr>
<tr>
<td><strong>B</strong></td>
<td>Reset Network Switch SNMP Security Parameters</td>
<td>Added this section to provide the procedure to reset the network switch SNMP security parameters.</td>
</tr>
<tr>
<td></td>
<td>Common Procedures, Update ControlST Feature-level SNMP Security Parameters</td>
<td>Added this section to provide the procedures to update ControlST feature-level SNMP security parameters.</td>
</tr>
<tr>
<td></td>
<td>Common Procedures, Update ControlST Switch-level SNMP Parameter Overrides</td>
<td>Added this section to provide the procedures to update ControlST switch-level SNMP parameter override settings.</td>
</tr>
<tr>
<td></td>
<td>Common Procedures, View/Update Cisco Switch SNMP Security Parameters</td>
<td>Added this section to provide the procedures to update view and/or update Cisco switch SNMP security parameters.</td>
</tr>
<tr>
<td></td>
<td>Common Procedures, Enable SNMP V3 Support in Cisco Switch not Configured for SNMP V3 Support</td>
<td>Added this section to provide the procedures to enable SNMP V3 support in a Cisco switch that is not configured for SNMP V3 support.</td>
</tr>
<tr>
<td></td>
<td>Common Procedures, Connect to Switch in Enable Mode using PuTTy Application</td>
<td>Added this section to provide the procedure to connect to the switch in Enable mode using the PuTTy application.</td>
</tr>
<tr>
<td></td>
<td>Common Procedures, View ControlST Configured Switch SNMP Settings</td>
<td>Added this section to provide the procedure to view the SNMP mode and security parameters.</td>
</tr>
<tr>
<td><strong>A</strong></td>
<td>Change Database Password in Proficy Vision</td>
<td>Added this section containing the procedure to change the Database password in Proficy Vision.</td>
</tr>
</tbody>
</table>
Acronyms and Abbreviations

CA Certificate Authority
DNS Domain Name System
EAP Electronic Access Point
ESP Electronic Security Perimeter
HMI Human-machine Interface
HTTPS HyperText Transfer Protocol Secure
IP Internet Protocol
MDH Monitoring Data Highway
NERC North American Electrical Reliability Corporation
NTP Network Time Protocol
OU organizational unit
OSM On Site Monitor
PDH Plant Data Highway
RADIUS Remote Authentication Dial-In User Service
RBAC Role Based Access Control
RSG Remote Services Gateway
SIEM Security Information and Event Management
SSH Secure Shell
TCP/IP Transmission Control Protocol/Internet Protocol
UDH Unit Data Highway
UDP/IP User Datagram Protocol/Internet Protocol
URL Uniform Resource Locator
UTM Unified Threat Management

Related Documents

<table>
<thead>
<tr>
<th>Doc #</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEH-6700</td>
<td>ToolboxST User Guide for Mark Controls Platform</td>
</tr>
<tr>
<td>GEH-6846</td>
<td>Control Server Installation and Startup Guide</td>
</tr>
<tr>
<td>GEH-6848</td>
<td>Control Server Hand-over Guide</td>
</tr>
</tbody>
</table>
Safety Symbol Legend

**Warning**

Indicates a procedure or condition that, if not strictly observed, could result in personal injury or death.

**Caution**

Indicates a procedure or condition that, if not strictly observed, could result in damage to or destruction of equipment.

**Attention**

Indicates a procedure or condition that should be strictly followed to improve these applications.
Control System Warnings

Warning

To prevent personal injury or damage to equipment, follow all equipment safety procedures, Lockout Tagout (LOTO), and site safety procedures as indicated by Employee Health and Safety (EHS) guidelines.

Warning

This equipment contains a potential hazard of electric shock, burn, or death. Only personnel who are adequately trained and thoroughly familiar with the equipment and the instructions should install, operate, or maintain this equipment.

Warning

Isolation of test equipment from the equipment under test presents potential electrical hazards. If the test equipment cannot be grounded to the equipment under test, the test equipment’s case must be shielded to prevent contact by personnel.

To minimize hazard of electrical shock or burn, approved grounding practices and procedures must be strictly followed.

Warning

To prevent personal injury or equipment damage caused by equipment malfunction, only adequately trained personnel should modify any programmable machine.

Warning

Always ensure that applicable standards and regulations are followed and only properly certified equipment is used as a critical component of a safety system. Never assume that the Human-machine Interface (HMI) or the operator will close a safety critical control loop.
The procedures and methods described in this document apply to the standard Control Server product as originally designed by GE. However, there may be deviations from the standard feature set installed and configured at the time of shipment. Please reference plant-specific documentation provided by your GE representative at the time of installation and commissioning for alternative or supplemental maintenance instructions for your application.

Note

1. Disconnect the equipment from the power supply by removing the plug from the socket-outlet, which is installed near the equipment and easily accessible.

2. There are no serviceable parts. Replace faulty sub-assembly and return defective material to GE Automation & Controls.

Waste Disposal: This mark or symbol on any electrical or electronic product indicates that this product cannot be disposed of in a trash bin. Such products must be returned to the original vendor or to a properly authorized collection point. The black bar under the waste bin symbol shows that the product was placed on the market after 13 August 2005.

Batteries are not meant to be replaced by an operator. A coin cell battery is included in the servers and in the firewall device, and the original manufacturer documentation should be referenced for any applicable end-of-life removal instructions.
Contents

1 Overview .............................................................................................................................................. 11
  1.1 Control Server Core ....................................................................................................................... 11
    1.1.1 Simplex Core ....................................................................................................................... 11
    1.1.2 High Availability (HA) Core ............................................................................................... 12
  1.2 Control Server Modules ............................................................................................................... 12
    1.2.1 Domain Services Module .................................................................................................... 12
    1.2.2 Thin Client HMI Module ...................................................................................................... 13
    1.2.3 Virtual Field Agent Module ............................................................................................... 14

2 Theory of Operations .................................................................................................................... 15
  2.1 Defense-in-Depth Concept ........................................................................................................... 15
  2.2 Role Based Access Control ........................................................................................................... 16
    2.2.1 Active Directory .................................................................................................................. 16
    2.2.2 Active Directory Organizational Units .................................................................................. 16
    2.2.3 Active Directory Users ......................................................................................................... 18
    2.2.4 Active Directory Groups ..................................................................................................... 19
    2.2.5 Active Directory Group Policy ............................................................................................ 21
    2.2.6 RADIUS Servers ................................................................................................................ 24
    2.2.7 Certificate Authority ............................................................................................................ 24
  2.3 IP Address Management ............................................................................................................... 26
    2.3.1 DNS Server .......................................................................................................................... 26
    2.3.2 DHCP Server ....................................................................................................................... 27
  2.4 Hardening ....................................................................................................................................... 28
    2.4.1 Controller Hardening .......................................................................................................... 28
    2.4.2 Computer Hardening .......................................................................................................... 29
    2.4.3 Switch Hardening .............................................................................................................. 29
  2.5 Network Switches ......................................................................................................................... 30
  2.6 Time Management ......................................................................................................................... 31
  2.7 Redundancy Concepts .................................................................................................................... 32
  2.8 Availability Concepts ..................................................................................................................... 33
  2.9 Security Concepts .......................................................................................................................... 34
  2.10 CA1 Sharenames .......................................................................................................................... 35

3 Ongoing Operations ............................................................................................................................. 37
  3.1 Account Overview .......................................................................................................................... 37
  3.2 Access Management and Permissions ........................................................................................... 38
    3.2.1 User Access Control ............................................................................................................ 38
    3.2.2 Domain Updates .................................................................................................................. 38
    3.2.3 Group Policy Updates ......................................................................................................... 39
    3.2.4 Reset System Account Passwords ...................................................................................... 41
    3.2.5 Reset DSRM Administrator Password .............................................................................. 48
    3.2.6 Reset Switch Passwords ...................................................................................................... 49
    3.2.7 Reset Network Switch SNOP Security Parameters ............................................................ 54
    3.2.8 Reset HMI Local Account Passwords .................................................................................. 54
    3.2.9 Change Passwords Associated with Proficy Historian Analysis .......................................... 55
    3.2.10 Password Maintenance for VMware ................................................................................... 61
4 Common Procedures ........................................................................................................................................... 97

4.1 New User Setup .............................................................................................................................................. 97

4.1.1 Example Group Assignments Based on Function .................................................................................. 98

4.1.2 Add New User .......................................................................................................................................... 99

4.2 Add HMI to System ....................................................................................................................................... 104

4.2.1 Add HMI to Domain ............................................................................................................................. 104

4.2.2 Configure DNS Server Addresses ...................................................................................................... 106

4.2.3 Add HMI to Domain ............................................................................................................................. 109

4.3 Add Computer to MDH .............................................................................................................................. 110

4.4 Add Switch ..................................................................................................................................................... 111

4.5 Change User’s Assigned Role .................................................................................................................... 113

4.6 Suspend or Delete User .............................................................................................................................. 115

4.7 Add Website to Internet Explorer Trusted Sites List .................................................................................. 116

4.8 Restart Default Website in IIS Manager ..................................................................................................... 117

4.9 Update ControlST Feature-level SNMP Security Parameters ................................................................ 118

4.9.1 Modify SNMP V1 Mode Security Parameters .................................................................................. 120

4.9.2 Modify SNMP V3 Mode Security Parameters .................................................................................. 121

4.10 Update ControlST Switch-level SNMP Parameter Overrides .................................................................. 123

4.10.1 Determine SNMP Parameter Override State .................................................................................... 123

4.10.2 Modify SNMP V1 Parameter Override Settings .............................................................................. 124

4.10.3 Modify SNMP V3 Parameter Override Settings .............................................................................. 125

4.11 View/Update Cisco Switch SNMP Security Parameters ............................................................................ 127

4.11.1 View Current Switch SNMP Settings ............................................................................................... 127

4.11.2 Modify SNMP V1 Community Name ............................................................................................... 127

4.11.3 Modify SNMP V3 Security Parameters ........................................................................................... 128

4.12 Enable SNMP V3 Support in Cisco Switch not Configured for SNMP V3 Support ........................................ 129

4.13 Connect to Switch in Enable Mode using PuTTy Application .................................................................... 130
4.14 View ControlST Configured Switch SNMP Settings ................................................................. 132
4.15 Create and Deploy SDI Certificates for WorkstationST Features ........................................ 133

Appendix A Reference ......................................................................................................................... 135
  Default Address Information .......................................................................................................... 135
  Default Credentials ....................................................................................................................... 135
  Expected Local and Domain Accounts ......................................................................................... 135

Glossary ............................................................................................................................................... 137

Index .................................................................................................................................................. 139
1 Overview

The Control Server consists of a product line that can be combined in different configurations to meet the needs of individual sites. The basic architecture consists of one or more server class computers each running a hypervisor. The Virtual Machines (VMs) that run on the hypervisor(s) perform the site functions.

The Control Server product architecture consists of two layers: Control Server Core and Control Server Module. Within each layer, multiple products are available to meet a site's feature, redundancy, size, and workload requirements.

The Control Server Core is the lower architectural layer. It includes the server hardware and the hypervisor software that runs on the server to provide the platform for hosting virtual machines. Various core architectures and options are available to meet a site's redundancy and performance requirements.

The Control Server Module is the upper architecture layer. Various modules supply different types of VMs to meet the site's application requirements, and multiple modules can be supported at the same time. Within each module there are typically options for the number and size of VMs supplied, such as the number of HMI VMs supplied, the number of Virtual Field Agent VMs supplied, or the number of Thin Client Terminals that must be supported.

The following sections provide additional information on the Control Server Cores and Control Server Modules that are available.

1.1 Control Server Core

The Control Server Core is the lower architectural layer. It includes the server hardware and the hypervisor software that runs on the server to provide the platform for hosting VMs.

The following Control Server Core architectures are available:

- **Simplex Core**: This core supplies a single server where all the VMs run. Various options are available controlling the size of this server. This core is typically used when the functions that it provides do not need to be redundant.
- **High Availability (HA) Core**: This core supplies a pair of redundant servers and a high-speed interconnection between them to support both manual and automatic fail-over capability. VMs can be migrated between the servers, and if one server fails or is shut down then the VMs will run on the remaining server.

A site's redundancy requirements tend to drive the Core selection (Simplex or HA), and its anticipated workloads tend to drive the selection of Platform and Options within the selected Core.

The following sections provide additional information about the Control Server Core products.

1.1.1 Simplex Core

The Simplex Core provides a single server class computer upon which to run VMs. The VMware ESXi hypervisor is used to host one or more VMs to meet the site's application needs.

The Simplex Core product is further subdivided into the Platform and Options available:

- **The Platform** selects the base type of server used. The Platform selection tends to focus on the features and expandability that is available in the platform. Low end platforms may not supply redundant power supplies, and may be more limited in their expandability. Higher end platforms tend to include redundant power supplies and have greater flexibility and range with respect to the CPU power, memory, and disk drive capacities available.
- **Various Options** are available within any one Platform selection. These options control items such as the CPU power, memory, and disk drive capacities available. The site's anticipated workload (number and types of VMs) typically drive the sizing option selection.
1.1.2 High Availability (HA) Core

High Availability (HA) Core supplies a pair of redundant servers and a high-speed interconnection between them to support both manual and automatic failover capability. The VMware ESXi hypervisor is used to host one or more VMs to meet the site's application needs.

Various Options are available to control items such as the CPU power, memory, and disk drive capacities available. The site's anticipated workload (number and types of VMs) typically drive the sizing option selection. Both physical machines must have the same options selected to support the failover options.

The VMware Virtual SAN product is used with the high-speed interconnection between the servers to mirror the virtual hard drives used in each VM on each server and provide failover capability. VMs can be migrated from one host to another without clients even recognizing that a transfer has taken place. In case of a sudden server failure preventing graceful migration, the client may need to reconnect to the VM after it restarts itself on the remaining host - a process that typically takes 15-30 seconds for a typical HMI. Depending upon the platform sizing options selected, a single server running all the VMs may exhibit reduced performance over the normal case of both servers in operation and the site load distributed between them.

1.2 Control Server Modules

The Control Server Module is the upper architecture layer. Various modules supply different types of virtual machines to meet the site's application requirements. Multiple Modules and/or multiple instances of a single Module are supported, with the platform sizing and performance requirements being the limiting factor. There are three basic modules available: Domain Services Module, Thin Client HMI Module, and Virtual Field Agent Module. There are options on the number and type of VMs supplied within each module.

1.2.1 Domain Services Module

The Domain Services Module provides a pair of redundant Domain Controller VMs and a Certificate Authority VM to establish a Microsoft Active Directory domain at the site. The domain provides for centralized management of users and roles and typically all Windows based VMs are joined to this domain. Computer Hardening is accomplished by joining computers (or VMs) to the domain and using domain Group Policies to apply the hardening policies. Services in the Domain Controllers and Certificate Authority are also used by devices outside of the domain for user identity management and access control.

The Domain Services Module supplies the following VMs:

- DC1: This is the primary domain controller. It provides the domain services listed below.
- DC2: This is the backup domain controller. It provides the same features as the primary domain controller.
- CA1: This is the Certificate Authority. It provides the Certificate and Public Key Infrastructure (PKI) services listed below.

The Domain Controllers supply the following domain functions:

- Microsoft Active Directory Domain Services
- Microsoft RADIUS Server
- Microsoft DNS Server
- Microsoft DHCP Server

The Certificate Authority supports the following domain functions:

- Microsoft Active Directory Certificate Authority
- Microsoft Network Device Enrollment Service

The Domain Services Module does not have options for the number and type of VMs supplied, a pair of redundant Domain Controllers and the Certificate Authority (3 VMs total) are always supplied.

The Domain Services Module does not have any other core or module dependencies, although using this module in a Simplex Core environment prevents splitting the redundant Domain Controllers across multiple servers.
### 1.2.2 Thin Client HMI Module

The **Thin Client HMI Module** provides one or more Virtual Machines typically used for supervisory level control. This includes the HMI, Historian, and Gateway VMs used to configure, monitor, and operate the control system. The VMs in this module are normally accessed by using Thin Client Terminals as the user interface.

The Thin Client HMI Module supplies the following types of VMs:

- **Engineering Workstation (EWS):** This VM type supplies the programming tools and typically acts as the master repository for the control configuration information. (See below for more details)

- **HMI:** This VM type is used for the Operator Interface. In addition to the Operator Interface software it also has the full programming and communication capability. There are typically multiple HMI VMs at a site for redundancy or to segment the operator displays for handling separate plant areas.

- **Historian (HST):** This VM type supplies the Proficy Historian with the Proficy Historian Analysis package. If required, there is typically only one VM of this type at a site.

- **Gateway:** This VM type is used as an interface between control systems or DCS layers. It provides the communication interface between control systems using an agreed upon standard protocol, such as Modbus, GSM, OPC DA, OPC AE, or OPC UA. If required, there are typically two of these VMs supplied for redundancy.

- **Application Server (AppServ):** This VM type is used as a host for control applications, such as a Configuration Management System or an Alarm Server. This VM comes with the communication layers needed to exchange control information, but not the Operator Interface tools or Configuration Tools.

- **Windows Server (WinServ):** This VM type is essentially a Windows Server VM with antivirus software. It has no additional control software on it for communications and is available for loading any site specific applications.

The Engineering Workstation (EWS) VM type is unique in that this VM includes software that is typically only installed on one VM at a site. This VM also has a special IP address that, in conjunction with the NetworkST 4.x access control lists, allows it to communicate with and configure network equipment that other VMs cannot reach. The functions that are typically supplied only on this VM type include:

- **CMS Server:** This provides the central repository for the Configuration Management System (CMS) and the CMS Server that clients use to access it.

- **Proficy Licensing Server:** This provides the licensing server that coordinates the GE Proficy licenses across all other VMs.

- **Microsoft Terminal Services License Server:** This (optional) component is used to coordinate licenses across all instances of Terminal Services across all other VMs. This is only required in Many-to-One configurations (see definition below).

- **Thin Client Configuration Server:** This provides the programming tools, services, and files needed to configure Thin Client Terminals. This includes the Thin Client Terminals firmware and configurations. For some Thin Client Terminal types this information is pushed from this VM to the Thin Client Terminals, in others the Thin Client Terminals are configured to pull the information from this VM.

- **Thin Client Module Information:** This VM holds a set of sharenames that provide scripts and online documentation for the Thin Client Module.

There are typically two schemes used for connecting Thin Client Terminals to the Thin Client HMI VMs. The selection is typically made based upon the site size, cost targets, redundancy requirements, and the desired relationship between the number of Thin Client Terminals and the number of VMs:

- **One-to-One:** This scheme supports a single Thin Client Terminal logged into a VM at any one time. Multiple Thin Client Terminals are supported, but each VM can only support one logged in user at a time.

- **Many-to-One:** This scheme supports multiple Thin Client Terminals to be logged into a single VM concurrently. The maximum number of Thin Client Terminals that can be logged in is determined by performance and the sizing of the VM, and enforced by the Terminal Services Licensing.

The Thin Client HMI Module supports many options for defining the number and type of VMs to be supplied. The options to select are based upon each site’s requirement as to the number and type of VMs along with its One-to-One or Many-to-One configuration. In the Many-to-One configurations, the CPU power and memory to be allocated to each VM may be adjusted within the total limits imposed by the Platform Options selected. This balancing can be done after the initial creation of the VMs and is not required at the time of placing the order. Verify that the Platform Options supply sufficient resources, and those resources can be reallocated or balanced between VMs at any time.
The Thin Client HMI Module requires that the Domain Services Module be installed as it makes extensive use of the Domain Services that it provides. All VMs in this module must be joined to the Domain Services domain.

### 1.2.3 Virtual Field Agent Module

The Virtual Field Agent (VFA) Module provides one or more VMs used for hosting Predix applications. The VMs in this module primarily interact with the control system, but applications may also provide an interface (such as a Web Server) for direct access. Various network connectivity options are available to meet the needs of site applications and to address site security policies.

The VFA Module supports the creation of multiple VMs, each running their own Predix applications. This split may be done for performance reasons, or the applications may be split among multiple VMs due to the data that they are dealing with, segmenting different plant areas into their own VMs. The maximum number of VMs is defined by the resource demands of the applications that are run within the VM versus the platform options and the site's performance requirements.

The base VFA Module does not have any other core or module dependencies, but individual Predix applications may add their own dependencies. These may include items such as additional security capability through the Domain Module, or a user interface accessed through the Thin Client Module.
2 Theory of Operations

The Domain Services Module has a number of subsystems. This chapter describes some of the major concepts of these subsystems, and how they work together to provide a defense-in-depth solution.

2.1 Defense-in-Depth Concept

Defense-in-depth is a security concept where multiple layers of security are in place so that if one layer allows something through, another layer is available to defend against attack. The concept of multiple security layers presents itself in many ways. In some cases, multiple layers exist looking for the same thing, or providing recovery procedures in case something does get through. In the case of protection against malware, the various levels include:

In some cases, the different layers support different levels of access control, such as:

- **Fine Control** where the ControlST* software suite applies Users and Roles and privileges to allow or block user actions based on customizable settings in the ToolboxST* application.

- **Coarse Control** where the Mark VIe controllers in Secure State make use of user certificates to provide a non-configurable capability that allows or blocks user actions based on membership in a fixed set of Controller Role groups.

Note Refer to the section Controller Hardening for more information.
2.2 Role Based Access Control

The Role Based Access Control (RBAC) concept is that users are granted the minimum rights and privileges that they must have to perform in their role (do their jobs). By limiting the privileges to the minimum required, user impact on the system is lessened, either through actions or through inadvertently triggered malware.

For example, a user with administrative privileges can change the system configuration (add users, services, and such), but if the user does not have administrative privileges, they would not be able to impact the system to such a degree.

Concepts include:

• Each user has an individual identifiable account.
• Each user account grants the rights and privileges needed to do the job (and no more).
• Users can have more than one account if they perform more than one role.
• Event logs can trace actions back to the (unique, identifiable) user who initiated the action.

2.2.1 Active Directory

Microsoft Active Directory is used to create a domain for all computers and users in the system. Active Directory holds the list of users, rights and privileges granted to each user, and the list of computers allowed to join the domain. Active Directory is run on the Domain Controllers, and its database is queried by all computers in the domain. Non-domain based elements (such as network switches) can access Active Directory information through RADIUS servers running in the Domain Controllers, and use the results to allow or disallow access to individual users.

Active Directory uses the concepts of Organizational Units, Users, Groups, and Group Policy to implement the security strategy. The following sections outline each of these concepts, and how they are applied.

2.2.2 Active Directory Organizational Units

Microsoft Active Directory is designed to handle large organizations, and be able to distribute the management functions to each group to handle their own special requirements. To accomplish these tasks, it allows for building an Organizational Unit (OU) tree where the main domain is at the top level, and each level down can represent various groups in an organization. Each level in the organization provides for the addition of users and computers, and each level can define the required settings (group policies) applied to users and groups defined at that level.

The Domain Services systems are designed to be a simple single domain with a limited set of OUs. Different OUs are supplied for the domain controllers, application servers, HMIs, Historians, and Thin Client terminals as follows:
HMI.local is the standard OU of the HMI domain supplied and managed by the Domain Services.

BuiltIn is the Microsoft-standard OU that defines a number of standard groups.

Computers is the Microsoft-standard OU that contains all the computers that were joined to the domain with no prior indication of what OU the computer should be in. If you join a computer to the domain without first defining the computer in an OU, it displays in this group. You can then drag-and-drop the computer from that group to the proper OU (typically, GE Controls\HMI\Computers).

Domain Controllers is a Microsoft-standard OU where all domain controllers are placed. In the Domain Services configuration, the DC1 and DC2 computers display in this OU.

ForeignSecurityPrincipals is a Microsoft-standard OU that holds accounts defined in other domains so that they can then become members of groups in this domain. Domain Services does not use this OU.

GE Controls is the main OU where the Domain Services-specific items are defined. This OU contains the definition of groups supplied by GE, along with child OUs for the Application Servers and HMIs.

- **GE Controls\Application Servers** holds accounts pertaining directly to the Application Servers.
  - **GE Controls\Application Servers\Computers** holds the computer accounts associated with the Domain Services Application Servers (such as CA1).

- **GE Controls\HMI** is the main OU where the accounts pertaining to HMI and Historian computers and users are based.
  - **GE Controls\HMI-HST\Computers** holds the HMI Computer accounts. When an HMI is added to the domain, the computer account should be created in or moved to this OU. If sites wish to further divide the HMI groups, child OUs can be created here.
  - **GE Controls\HMI\Users** holds the HMI users defined at this site. When an HMI user account is added to the domain, it should be added here. If sites wish to further divide the HMI user groups, child OUs can be created here.
  - **GE Controls\HMI\Users\GE Accounts** holds defined GE user accounts. This special OU exists only prior to commissioning the system. This OU, and all accounts defined within it, are deleted prior to turning the system over to the site to manage.

- **GE Controls\HST** is the main OU where the accounts pertaining to the Historian computers and users are based.
  - **GE Controls\HST\Computers** holds the Historian Computer accounts. When a Historian is added to the domain, the computer account should be created in or moved to this OU. If sites wish to further divide the Historian groups, child OUs can be created here.

**Note** By default, users of Historians are assumed to be users of the HMI and therefore their accounts would be created as HMI users, not HST users. If sites wish to have a separate location for historian only users then a Users OU can be created parallel to the Computers OU here.

- **GE Controls\Thin Clients** is the main OU where thin client computers are defined at this site.
  - **GE Controls\Thin Clients\WES7** holds the Windows Embedded Standard 7 (WES7) thin clients. This OU applies specific hardening policies to the Windows 7 thin clients.

**Note** By default, users of Windows 7 thin clients do not log onto the thin clients using domain accounts. A local, common, non-privileged account is used for the thin client and then the user's domain account is used for connecting to an HMI or Historian VM. If sites wish to have a separate location for thin client accounts then a WES7-Users OU can be created parallel to the "WES7" OU here. In general users should not be logging onto WES7 thin clients using anything other than the non-privileged local account unless site security procedures dictate otherwise.

Managed Service Accounts is a Microsoft-standard OU that supports automatic password management at the domain level for services or applications running in individual computers. Domain Services does not use this OU.

Users is a Microsoft-standard OU that holds domain users outside of any other OU. Domain Services puts agent, administration, and other accounts used domain-wide in this OU.
The OU structure creates a hierarchy where user and computer accounts are created and managed, but it does not imply or enforce that users may only log on to devices that are in its OU or its child OUs. A user created in any OU is allowed to log on to any computer in the domain.

*Note* Logon limitations could be implemented using special security rules or group membership, but it is not enforced by the OU structure itself.

### 2.2.3 Active Directory Users

Active Directory Users (or User Accounts) are the entries that define who is allowed to log on to computers in the domain, as well as the rights and privileges that should be granted each individual user. When a user account is created, it is assigned a unique user name and a password. In addition, when defining the account, the rights and privileges that the user will have are defined, mainly by adding the user as a member of one or more groups.

Users that perform more than one role should be given more than one user account. This practice allows the user to run with the minimum privileges required to perform a particular function and then increase their privilege level when needed. This practice is very common with domain administrators. They use a normal day-to-day account for normal activity, but switch to using their domain administrator account when performing domain administration tasks. The same is true with HMI administration accounts. Users may be provided Maintenance-level accounts to use for normal activity, reserving their Administrator-level account for software installation and computer administration purposes. This practice helps limit the impact of a user inadvertently triggering malware.

In addition to normal user accounts, Domain Services includes additional user accounts for use by background programs: agent accounts and application accounts

**Agent Account** is a user account that supplies access credentials and rights for a background program. Agent accounts are typically used on client computers to access both local and remote resources. Agent Accounts are also used to access non-computer devices, such as the Network Agent account being used to access network switches to retrieve their configuration.

- **Limitations:** The agent accounts are intended for background usage, and are typically denied the ability to log on interactively or through Remote Desktop by the hardening security policies. You cannot test an agent account password by logging into a computer using the agent account; however, many subsystems (such as Remote Desktop Services) send one error message if the password is wrong (*The logon attempt failed*), and another if the password was right but logon was denied (*To log on to this remote computer, you must be granted the Allow log on through Terminal Services right*).

- **Password Management:** The agent accounts are configured initially with the *Password does not expire* option. This setting indicates that background communication will not cease suddenly when a password expires. Sites may establish that the agent account passwords be changed periodically or based upon an event. When changing an agent account password, the password must be changed in Active Directory and in all the agent programs that use that password. Active Directory follows the normal rules for changing (resetting) a user password, but the procedures for changing the password in the agent program are different for each agent. (Refer to the section *Reset System Account Passwords*.)

**Application Account** is a user account that supplies access credentials and rights to run as a program on an application server. Application accounts are created when the account needs special access rights or rights to cross from one computer to another, such as the Certificate Application account requiring special impersonation rights.

- **Password Management:** Like agent accounts, application accounts are initially set to *Password does not expire*, but when the password is changed, that password must be changed in both Active Directory (the account) and the application using the account. (Refer to the section *Access Management and Permissions*.)

**GE Generic Accounts** exist prior to commissioning and turning control of the system over to the site. These accounts are used in the initial setup and configuration of the domain and to add site-specific accounts for users. These GE accounts are created in the *GE Controls\HMI\Users\GE Accounts* OU and are removed as part of the hand-over processes.
**Local Accounts** are used by the HMIs when users are not in a domain, and as the last fallback in case of long-term domain controller failure. Users in a domain are not expected to use these accounts (or even know the passwords) unless the site is operating long-term without access to the Domain Controllers. Procedures are supplied to list the local accounts that exist, as well as procedures to reset the passwords of these accounts. At hand-over, both these procedures are run to identify local accounts and reset their passwords. (Refer to section *Expected Local and Domain Accounts*.)

### 2.2.4 Active Directory Groups

Microsoft Active Directory has the concept of security groups, typically just called groups. Each function or resource is configured to allow access by members of certain groups. The goal is to never need to change the security settings on objects or files, but instead to simply add or remove users from the groups that control access.

When adding a new user to the system, you must define the expected role of the user, then make the user a member of the appropriate groups to allow them access to functions and files they require. The primary implementation of role-based access control is adding user accounts to only the groups they require to perform their roles. Adding users to groups grants them rights and privileges, and understanding those rights and privileges is key to implementing role-based access control.

Microsoft defines a number of standard groups, called *built-in groups*, at both the domain and the local computer level. In addition, GE has created a number of groups for the special functions that it provides. Microsoft provides documentation on the groups that they provide and the rights that membership in those groups provides. The multitude of groups provides for a very flexible environment suitable for very large organizations with distributed control at each OU level. The Domain Services domain structure does not prevent any of those features from being used, but due to the smaller size and reduced requirements, it tends not to use all the features that Microsoft provides.

A user can be a member of a group, but so can another group. If a group (A) is a member of another group (B), all rights and privileges granted to members of group (B) are granted to members of group (A). For example, the Remote Desktop Users group grants users the ability to log on using a Remote Desktop Client. The Administrators group is (by default) added to the Remote Desktop Users group so that all administrators can log on using Remote Desktop Clients. It is usually a best practice to structure groups so that this group-in-a-group is limited to the final group that grants permissions (meaning only two levels of group memberships) instead of allowing it to become a more complicated three-or-more layer structure.

Following is a brief summary of some of the more useful groups for small system management.

**Microsoft-supplied Groups (partial listing):**

- **Administrators**: A user added to the Administrators group of a single computer is granted complete configuration control of that computer. A user added to the Administrators group on a Domain Controller has complete configuration control of the domain. Membership in this group at the domain level should be limited to the users in charge of maintaining the domain configuration. (Domain Administrators should be added to the Domain Admins group, which adds them to the Administrators group on all computers in the domain instead of adding them individually to the Administrators group of the computer.)

- **Domain Admins**: A user added to this group is granted administrator rights on all computers in the domain, including the Domain Controllers. Membership in this domain should be limited to the users in charge of maintaining the domain configuration.

- **Remote Desktop Users**: A user added to this group is allowed to log on to the computer using a Remote Desktop Client. The Microsoft default setting is to include the local Administrators group so that all administrators also have this right.

- **Users**: A user added to this group has normal user rights (not administrative rights) to the computer. By default, all users created are included in this group.

**GE adds the following groups to perform specific GE-related functions:**

- **Controller Role-Base, Controller Role-Download, Controller Role-Force, Controller Role-Set**: Members in these groups are granted certificates with the specified level of access to Mark VIe controllers running in Secure State. (This also includes the EX2100e Excitation controllers, LS2100e Static Starter controllers, and Mark Stat Power Conversion controllers.) Add users to one of these groups based upon the level of access they should be granted to Mark VIe controllers.
**HMI Administrators:** Members in this group are granted Administrator rights to all computers in the HMI and HST OUs. Add users to this group if they need to be an administrator on each HMI.

*Note* Running the ToolboxST application to alter configurations and download devices does not require this right. However, if you need to use the application to recreate a compact flash for a controller, you need administrator privileges.

Granting a user Administrator rights puts them in a position where any malware they trigger can do significantly more damage to the computer than a user running without Administrator rights.

---

**HMI Maintenance:** Members in this group are granted Maintenance rights on all computers in the HMI and HST OUs. Add members to this group if they need to run the ToolboxST application and modify the configuration of controllers or HMs.

**HMI Operators:** Members in this group are granted Operator rights on all computers in the HMI and HST OUs. Running with Operator rights includes using a reduced functionality user interface to limit access to non-essential functions in the HMI.

**Network Administrators:** Members of this group are granted management access to the network switches, and routers. Add users to this group if they are required to access or modify the configuration of the network switches and routers.

The following examples outline the process of adding various types of users:

**Example #1 - Adding a HMI user:** A typical HMI user would be added to the following groups based upon the site operating policy and expected role of the user:

1. Add the user to one of the HMI groups based upon the user's required access (HMI Administrators, HMI Maintenance, or HMI Operators)
2. On a site with Mark VIe controllers, EX2100e Excitation controllers, LS2100e Static Starter controllers, and Mark Stat Power Conversion controllers, add the user to one of the Controller Role groups based upon the user's required access to the controller and site policy (Controller Role-Base, Controller Role-Set, Controller Role-Force, or Controller Role-Download)

**Example #2 - Domain Administrator:** A user in charge of configuring and maintaining the domain, computers, users, group policies, RADIUS configurations, and actually join computers to the domain and add agents would typically be added to the following groups:

1. Domain Admins: to be able to support all domain and computer configuration changes
2. (Optional) Network Administrators: to be able to diagnose and manage networking equipment
2.2.5 **Active Directory Group Policy**

Active Directory Group Policies are groups of settings that can be applied to computers that join the domain. This ability allows you to enforce configuration settings required for proper operation, or for security purposes on each computer without having to visit the computer and change the settings manually.

Group Policies are maintained by the Domain Controllers and the policies are applied at the Organizational Unit (OU) level. Each OU can have one or more group policies applied at that level, and that policy and its setting are applied to all computers and users defined at that level and below. Group Policy categories include:

- **Computer Policies** are settings applied to the computer when the computer boots up after joining the domain. These settings are applied to the computer even if there are no users logged in.

- **User Policies** are settings applied when the user logs into the computer. These settings can be tailored to the individual users based upon the OU where the user was defined.

Group Policies are always applied in a specific order. In cases where the same setting is defined in multiple group policies, the last policy applied will always win and be used. This process is not a merge function; the last policy to define a setting is what will be used in the computer. When determining the order to apply the Group Policies, two concepts are used: Precedence and Inheritance.

- **Precedence** rules determine the order to apply the group policies when there are multiple policies applied within the OU. The Linked Group Policy Objects tab of the Group Policy Management Console for an OU is used to view and change the precedence of each Group Policy. It uses the term Link Order, where a lower number in the Link Order indicates the policy has a higher precedence. The result is that it overrides policies with a higher Link Order within the same OU.
Inheritance rules determine the order to apply the group policies when there are multiple OU levels. When group policies are applied, the policies at the top level of the OU structure are applied first. The policies are then applied at each level from the top down to where the computer or user is defined. This method allows more-specific OU policies to override more generic domain-wide policies. The Group Policy Inheritance tab of the Group Policy Management Console shows both the Inheritance and the Precedence orders to show the list of policies applied and the final order of execution.

GE supplies a predefined set of Group Policies applied to the various OUs. Most policies fall under one of the following categories:

**Agent Policy** supplies the settings required to run an agent program on a target machine. These typically include opening required firewall ports, making sure dependent services are available or started, and taking care of any required local group memberships.

**Application Policy** supplies the settings required for an application to run. These typically include opening firewall ports, making sure dependent services are available or started, and taking care of any required local group memberships.

**Computer Policy** supplies general purpose settings typically related to how the computer interacts with the domain, to supply extra Start Menu entries, and to take care of any required local group memberships outside of applications or agents.

**Hardening Policy** supplies the settings that are security-related. These settings typically control access to the computer, define password and account policies that must be followed, change security settings to harden it against various forms of attack, and limit the services that run on the computer to reduce potential attacks.
The following Group Policies are supplied:

**APx Computer Policy** supplies general settings used on all Application Servers.

**APx Hardening Policy** supplies the security settings to harden Application Servers.

**AutoEnrollment Policy** supplies the settings to enable the Certificate AutoEnrollment feature on computers running the ToolboxST application (HMIs and Engineering Workstations).

**Certificate Application Policy** supplies the settings required to supply certificates from the Certificate Authority hosted on the CA1 server.

**DCx Computer Policy** supplies settings used on the Domain Controllers.

**DCx Hardening Policy** supplies security settings to harden the Domain Controllers.

**GE Domain Controllers Policy** supplies general settings used on the Domain Controllers. (This policy overrides settings supplied in the Microsoft Default Domain Controllers Policy due to its precedence.)

**GE Domain Policy** supplies general settings used on all computers in the Domain. (This policy overrides settings supplied in the Microsoft Default Domain Policy due to its precedence.)

**HMI Computer Policy** supplies settings used on all HMI computers.

**HMI Hardening Policy** supplies security settings used to harden the HMI computers.

**HMI Operators Policy** supplies settings that limit the functionality of the User Interface of operators on the HMIs.

**HST Hardening Policy** supplies security settings used to harden the Historian computers.

**TC-WES7 Hardening Policy** supplies security settings used to harden the Windows (WES7) thin clients.

**Time Sync Policy** supplies settings used by the Application Servers and the HMIs to control synchronization of the time on the computers in the domain.

When customizing group policy to meet site-specific requirements, it is better not to modify an existing policy, but to create a new policy that (due to inheritance and precedence) overrides the existing policies. This method provides a number of benefits when it comes to maintaining a site over a long period of time:

- If Microsoft updates their default policies through a service pack or update, the site settings are protected.
- If an update to the Domain Services is performed that supplies updates to the policies, the site settings are protected.
- It is easier to debug issues with conflicting settings if it is obvious by using various Microsoft-supplied tools (such as RSOP.MSC or GPResult /H) that the GE setting was overridden by the site setting. This also allows a site to disable the site policy temporarily to see if that corrects the issue, thereby helping to focus on the next step in debugging the issue.

If a site policy is used to override either the Microsoft defaults or the GE policies, make sure to use the Group Policy Management Console to set the precedence of the site policy to override the Microsoft or GE policy.

Be careful not to apply new policies at too high a level in the OU structure. Specifically, be very careful of the impact of policy changes on the Domain Controllers and Application Servers. Apply changes at the HMI, Historian, or Thin Client level, unless they are intended to impact the Domain Services as well. Microsoft allows for the application (linking) of a policy at multiple location in the OU structure, so you can create a policy once and then apply it to any number of OUs. This capability can be advantageous in preventing the application of policy at too high an OU level.

One feature in Group Policy that GE uses to reduce the need for multiple levels of OU structure is the concept of Security Filtering of Group Policies. From the Group Policy Management Console Scope tab, the Security Filtering field allows you to control which computers or users have the policy applied to them (in addition to the normal OU structure). GE uses this setting to allow all the application servers to be in one Application Servers - Computers OU, but only apply the application policy to the one application server running the application. Using this method of security filtering (for policies that apply to only a few computers, or to all computers except a few) prevents having to make an overly complex OU structures. Since Security Filtering is on a per-policy basis, it allows different policies to be applied to different subsets of computers without requiring that they be in different OUs.
2.2.6 RADIUS Servers

Remote Authentication Dial-In User Service (RADIUS) is an industry-standard protocol that allows devices that are not members of the domain (such as the network switches) to verify the identity of a user, and determine what rights the user should have on the device.

Each Domain Controller (DC1, DC2) includes a RADIUS server. The RADIUS configuration is outside of Active Directory, and does not replicate between the domain controllers. Each RADIUS server must be configured separately.

To query a RADIUS server for user account information, each network device must:

1. Be listed as an expected client device in the RADIUS server configuration
2. Pass the RADIUS Server a shared secret to prove it is the trusted device

For the GE-configured network switches, the switch uses RADIUS to query the Active Directory database for the user credentials (user name, password); then check to see if the user is a member of the Network Administrators group. If the user is a member of this group, the switch is configured to grant the user management access to the switch. If the user is not a member of that group, the switch does not allow the user to perform management functions.

If the switch is not able to contact either of the RADIUS servers, the switch allows using the local switch manager account to access the switch. If a RADIUS server is available, the local switch management account is not allowed management access.

2.2.7 Certificate Authority

Certificates can be used to verify the identity of a server prior to logging on, or in cases where you do not log on, such as a Web server. They can also be used to prove your identity to computers that are not members of the domain, such as controllers, but require proof of identity. Certificates can also be used to encrypt the communication with a device as the information can be encrypted such that only the certificate holder can decrypt the information.

A Certificate Server is included in the CA1 VM, and it works with Active Directory to handle certificate requests and certification validation. Because it is part of the Active Directory subsystem, the computers that are joined to the network automatically trust the domain-based certificate server and the certificates that it issues.

Certificates from the domain certificate server are used in the Domain Controllers and Application Servers for the Remote Desktop subsystem to verify the identity of the computer before providing it with a user name and password.

The other main use of certificates is with a controller that is put into Secure State. Secure State makes many changes in the controller, including where communication with the controller looks for the client (the user running the ToolboxST application) to have a certificate issued by the domain certificate authority. If the user does not have such a certificate, the controller does not allow many functions that change the state of the controller (such as forcing variables or downloading new configurations or software). If the user does have the right type of certificate, the certificate is checked for the level of access that the user should be granted, and the controller then filters the user's commands based upon the access level (or role) that the user was granted.

Domain Services has been configured to use two Microsoft features when issuing certificates to clients to support controller hardening: Certificate Roaming and Certificate AutoEnrollment. These two features work together to make the use of certificates by clients an invisible operation. Users do not need to take any actions to acquire the certificates that they need to perform their (role-based) duties.

**Certificate Roaming** is a feature whereby when a user is granted a certificate, a copy of the certificate is placed into the user's Active Directory record. From there, the certificate is accessible from any domain location (HMI, EWS) where the user logs in. This situation allows one certificate to be issued, and then used from any HMI to contact the Mark VIe controller. If a user deletes the certificate on one HMI, it is marked as deleted in the Active Directory storage so that it will be deleted when the user logs onto other HMIs.

**Certificate AutoEnrollment** is a feature whereby when a user logs into a computer, it checks to see if the user should have a certain type of certificate based upon their Active Directory group membership. If the user should have a certificate and does not, it automatically requests the certificate from the Certificate Authority (Certificate Server) running on the CA1 server. It is this AutoEnrollment feature that allows the user to obtain required certificates without having to take any actions. The process of issuing certificates is reduced to the process of adding a user to the groups required to do their job function.
Certificate AutoEnrollment and Certificate Roaming combine together to trigger the following actions when a user logs into a domain computer, such as an HMI:

- Certificate Roaming checks to see if the user's set of certificates on the local computer match the set in Active Directory. If not, certificates are copied from the Active Directory certificate storage to the local computer for the user to use.
- Certificate AutoEnrollment checks the user's Active Directory group membership to see if they are a member of a group that provides a certain type of certificate. If so, and if the user has that certificate, there is no action taken. If the user should have a certificate and does not, it contacts the Certificate Authority to obtain the required certificate. Certificate Roaming then adds a copy of the new certificate to the user's Active Directory certificate storage.

For the Mark VIe controller, membership in any of the Controller Role groups is configured to provide the user with a certificate required to contact the controller in Secure State with the proper access rights.

Normally, users log off and on at least once a day, which triggers the AutoEnrollment process checks. If there is a condition where a user does not log on periodically, their certificate may expire. In that case, have the user log off and back on to trigger the AutoEnrollment process and issue a new certificate. Certificates for use with the Secure State controllers typically expire in a year.

While the Certificate AutoEnrollment process is in place for the HMIs, it is not used on the Application Servers or Domain Controllers. These computers should never have the ControlST software suite installed, and therefore never run the applications that require certificates to support Secure controllers. The Domain Services Servers (DC1, DC2, CA1) should never be used as general purpose computers or HMIs.
2.3 IP Address Management

Due to the proximity to the control system and historical best practices, most elements of a Control Server system use preassigned (fixed or static) IP Addresses. With the introduction of more "appliance" oriented elements, such as Thin Client Terminals, there is a desire to be able to dynamically assign IP addresses and then keep track of those assignments. Domain Services provides two Microsoft Active Directory based subsystems to support both methods of IP addressing:

- **DNS Server**: The Domain Name System (DNS) Server provides a database and lookup service that links a computer's host name to its IP address. By using a DNS Server a client can connect to a server using the name of the server and not its IP address.

- **DHCP Server**: The Dynamic Host Configuration Protocol (DHCP) Server provides devices that request an IP address with a currently unassigned IP Address, and then record that assignment with the DNS Server so that clients can reach the new element using its host name.

2.3.1 DNS Server

Domain Services provides the Microsoft Active Directory DNS Server running on both domain controllers (DC1 and DC2 for redundancy) to allow clients to retrieve the IP address of a computer given its host name. The DNS Server can also supply a list of hosts that provide a given service, such as the list of Domain Controllers for a particular domain. Once host entries are added to the DNS Server database the database can be queried by host name to retrieve its IP address. The DNS Server also supports reverse lookup where an IP address can be queried to get back the host name of the computer using that IP address.

Host entries are typically added to the DNS Server in one of three ways:

1. When a computer or VM is added to the domain, a host entry is automatically added to the DNS Server for its PDH IP address. This means any HMI that is added to the domain will automatically have its host name and PDH IP address added to the DNS Server.

2. When a DHCP Server provides a computer or VM with an IP address, it automatically adds a host entry with the IP address that it assigned to the DNS Server. This means that any host given a PDH IP address by the DHCP Servers will automatically have its host name and PDH address added to the domain DNS Server.

3. To support devices that have static IP addresses and are not joined to the domain, an administrator can configure a static address (or static host entry) into the DNS Server. Once added, clients retrieve these static entries the same way as the automatically entered (dynamic) addresses above.

For security purposes, the Microsoft Active Directory DNS Server limits who has the ability to change addresses in the DNS Server database to the entity that originally created it. This presents a problem when redundant DHCP Servers are used as it would prevent one DHCP server from being able to update the entries made by the other. To get around this problem Domain Services includes a special "DNS Agent" account and the DHCP Servers are configured to use that account when making DNS entry changes. Since both DHCP Servers are using the same agent account identity they are able to modify or update each other's entries.
2.3.2 DHCP Server

Domain Services provides the Microsoft Active Directory DHCP Server running on both domain controllers (DC1 and DC2 for redundancy) to allow clients to request a PDH IP address to use. This feature is typically used by items such as Thin Client Terminals, or by engineering laptops connected to the network for configuration or debugging purposes.

**Note** Not all site's security policies allow additional computers to be connected to the control system, and some may require static IP addresses be used for accountability if they do allow them to be added. Always check the site's security policy prior to adding equipment to the network.

When a DCHP client requests the use of an IP address it gets back more than just the IP address. DHCP assignments include additional information required by the client in order for it to operate smoothly within the network and domain environment. The information returned includes the following:

- IP Address: This is the IP address that the client is allowed to use.
- IP Subnet Mask: This defines the scope of the network and is used to determine the subnet broadcast address.
- Lease Time: This is the amount of time that the client is allowed to use this IP address. The client will attempt to renew the lease at 1/2 of the Lease Time, and if it cannot be renewed by the end of the lease time the client is not allowed to use that IP address any more.
- DNS Server: This is the location of the DNS Server(s) so that the client can use DNS to resolve addresses by name instead of IP address.
- Domain Name: Clients can use the Domain Name to lookup the supplier of domain services, such as to locate the domain controllers for that domain. Clients often use the Domain Name as a suffix when looking up host names. For example: If a client was told the domain name was "HMI.local", then when looking up the host name "EWS1" the client may look for both "EWS1" and "EWS1.HMI.local".

The DHCP Server can be programmed to return additional vendor specific information when it detects that the device is supplied by a particular vendor. This is often used with the Thin Client Terminals to return the location of the configuration server where the Thin Client Terminal goes to download firmware and configuration information. By making this vendor specific, multiple different types of Thin Client Terminals can be supported at the same time.

Domain Services reconfigures many of the default settings in the Microsoft DHCP Servers, changing default values to values more suited for a control system environment. One example of this is the DHCP Lease Time. Most environments use a fairly short lease time (from a hour or two to a day or two) so that as devices leave the network their IP addresses can be reused fairly soon by new devices entering the network. The Control Server environment tends to be much more static with respect to the devices present, so it does not gain that advantage of a short lease time. Availability is more critical to control systems, and short lease times mean that if both domain controllers were down then devices would quickly lose the ability to use their IP address. To improve control system availability, Domain Services sets the default Lease Time much longer, typically around the 2 month period. This means that even if both domain controllers (and their DHCP Servers) are unavailable no DHCP client will have to stop using their IP address for at least 1 month (1/2 the lease time in a worst-case scenario). This coincides with the Cached Credential period where cached domain credentials are no longer trusted after not being able to contact a domain controller for more than 1 month. With a large DHCP address pool (typically 254 addresses) and the slow turnover of devices using DHCP Services, this long lease period should not cause the DHCP address pool to run dry. If that does happen, an administrator can go in the DHCP Server database and manually remove devices that are no longer present on the network prior to their (typically 2 month) expiration.

The Microsoft DHCP Server supports redundancy, which is used to create a redundant pair from DC1 and DC2. Database entries are exchanged between the two DHCP servers, but the configuration information (the size of the DHCP address pool, the length of the lease…) is not automatically exchanged. When making changes to the DHCP Server settings you should make the changes on one of the DHCP Servers, then issue the command to copy the full configuration over to the other DHCP Server. Failure to copy the updated configuration should not cause any failures, but the information supplied to DHCP clients by the two DHCP servers will be different. This mode also opens up the possibility that the next change will be done on the other server, and if/when that is copied back the first set of changes will be undone. It is recommended to choose one server and apply all new settings changes to it, then copy the configuration from that server to the other server - for example, always make changes to DC1 and copy the results to DC2.
2.4 Hardening

Hardening a system includes the steps taken to reduce attack surfaces that may be used in an attack on the system. These steps include removing functions that are not essential and changing system settings that may help deter attacks. The following sections define some of the hardening concepts.

2.4.1 Controller Hardening

The Mark VIe controllers support the concept of being able to run in Secure State. Secure State is designed to reduce attack surfaces, and identify individual users and filter their allowable actions based upon their assigned role. Secure was introduced in ControlST V04.06.

The Mark VIe controller implements the following when the controller is placed into Secure:

**Authenticated Users**: When a connection is made from the ToolboxST application, the controller requests a secure connection. A secure connection can be established only if the user has obtained one of the Controller Role certificates due to being in one of the Controller Role groups. If the user does not have a certificate, the controller establishes an unsecured connection, and will not allow the user change the controller configuration. If the user does have a certificate, a secure connection is established, and the user actions allowed will be limited based upon the level of the certificate the user possesses.

The levels of certificates available in the order of increasing capability are:

- **Controller Role-Base**: This level establishes the identity of the user, but provides the same level of functionality as an unsecure connection.
- **Controller Role-Set**: This level adds the ability to issue commands that change the current operating point of the controller, but not its configuration.
- **Controller Role-Force**: This level adds the ability to force variables.
- **Controller Role-Download**: This level adds the ability to change the configuration of the controller, including the ability to enter and exit Secure State.

**Disabled Services**: When a controller is placed into Secure State, several industry-standard protocols and services are disabled, including Telnet and FTP. Information and changes that use those subsystems are no longer available, deferring to the methods available through the ToolboxST application and its secure connection.

**Program Whitelist**: When a controller is placed into Secure State, it activates a special whitelist for the processes running inside the controller. Any process that is not recognized as a trusted process is terminated. This check includes a validity check on the process binaries that assures they are unmodified.

**Web Page Authentication**: When a controller is placed into Secure State, the web interface (if supplied) requires password authentication before allowing commands that can change the state of the controller.

The roles assigned and enforced by Controller Hardening are in addition to the Users and Roles assigned in the ToolboxST application. This combination is a defense-in-depth strategy that also protects against rogue commands being issued by clients other than the ToolboxST application. The concepts behind Users and Roles allow a much more fine-grained approach to allowable functions per user. The controller hardening roles provide a second broader-level of access rights control. The two work together, but while Users and Roles is available at all times, the controller hardening roles are only available when the controller is in Secure State and users have been granted their appropriate certificates through inclusion in the Controller Role groups.
2.4.2 Computer Hardening

Hardening of computers in the domain is accomplished by using various Group Policies to change settings in the computer. A computer is hardened automatically when it is joined to the domain and moved into an organizational unit. Specific Hardening Policies exist for Domain Controllers (DCx), Application Servers (APx), HMIs (HMI), Historians (HST), and Windows Thin Clients (TC-WES7).

Some common actions taken by hardening policies include:

**Account Access:** Hardening policies disable certain access from certain accounts. For example, the agent accounts are used by background services to access resources in a controlled manner. By blocking the agent accounts from being able to log on to the computer (either locally or through a Remote Desktop session) it helps mitigate the impact of agent account credentials being leaked.

**Audit Policies:** Hardening policies enforce audit policies so that records of operation and break-in attempts will be logged.

**Communication Settings:** Hardening policies are used to enforce certain system-level communications (such as computers communicating to domain controllers) to be encrypted. This makes it more difficult to be able to obtain information from monitoring the network.

**Network Settings:** Hardening policies are used to disable unused protocols so that vulnerabilities in those protocols will not be exposed from this computer.

**Security Settings:** Hardening policies enforce certain operating system security settings. These include settings such as watching for multiple failed log on attempts, and locking out (temporarily disabling) an account if it believes that a continuous force attack is taking place. These settings are not made overly aggressive (typically locking out an account for only 15 minutes after 10 failed attempts), but sufficient to help block attacks.

**Services:** Hardening policies turn off (disable) operating system services that are not required in the computer. By turning off these services, any vulnerabilities found in the service will not make the target computer vulnerable.

If additional computers are added to the domain, they should be added so that they are covered by a hardening policy. The typical approach is to add computers to the GE Controls\Computers\HMI OU, where they will inherit the HMI Hardening Policy group policy. If additional OUs are created outside of this parent OU, it is recommended that the HMI Hardening Policy be applied to the new OU as well. If a custom hardening policy is required for the computers, it is recommended to either copy the existing HMI Hardening Policy and make incremental changes, or apply the HMI Hardening Policy and then override settings with a site-specific hardening policy that adds or removes settings as required.

2.4.3 Switch Hardening

The network switches are configured to look for RADIUS servers (DC1 and DC2), and if present, use them to determine if a user is to be granted management access to the switch. These exchanges that include credential information (user names, passwords) use encrypted communication connections to the switch. If the switch finds the RADIUS servers, only accounts that are defined with management access (membership in the Network Administrators group) are allowed management access. As a fallback, if no RADIUS servers can be contacted, the local switch management account is enabled.
2.5 Network Switches

Management access to each network device (switch or router) is granted through membership in the Network Administrators group in Active Directory. Members of that group are allowed to view and update the configuration of the network device and perform all other device management functions.

For network devices to verify the user's access rights, the following takes place:

1. The network device attempts to contact a RADIUS server (two are defined: DC1 and DC2).
2. The network device must be defined as an allowed client in the RADIUS server.
3. The network device must supply the RADIUS server the shared secret (to prove it is the trusted switch).
4. The network device must supply the credentials (user name and password) of the user attempting to log on to the network device to the RADIUS server.
5. The RADIUS server reports to the network device whether the user is valid and is a member of the Network Administrators group.
6. If the user is a member of the group, the network device grants the user management access, otherwise it is denied.

If a network device is unable to contact any of the RADIUS servers (DC1 or DC2), it will allow the device’s local management account to gain management access to the device. This is a fail-safe condition where there is at least one method for management access when either connectivity is lost or both domain controllers are unavailable. If one of the RADIUS servers can be contacted, access is denied to the device’s local management account.

Care must be taken when changing the shared secret used by the network devices to log on to Microsoft Active Directory. If you change the shared secret in Active Directory first, the network devices will not be able to let you log on to change the network device configuration to the new shared secret. You must log on to the network device first, update its configuration, then change the shared secret in Active Directory. If there are multiple network devices at the site, the change must be coordinated across all devices. (Multiple shared secrets can also be used. This is where a new secret is created, and network devices are slowly migrated from the old secret to the new secret. Once all have been migrated, the old shared secret can be deleted.)
2.6 Time Management

Microsoft Active Directory uses the Kerberos™ computer network authentication protocol to authenticate users and computers within the domain. Kerberos uses the concept of limited-time certificates (tickets) when granting access rights, which makes the time set on the computers in the domain significant. To prevent issues with divergent clocks, Microsoft by default has the Domain Controllers set the time on all the computers in the domain. This prevents issues with Kerberos authentication, but can cause issues in industrial applications where time management is done at a much finer level.

When Domain Services is first set up, the Microsoft defaults of having the Domain Controllers set the time on all computers in the domain will be in effect. At some point in the plant commissioning, the site's high-resolution time management structure will be implemented. This step typically includes the use of a site time reference that supports Network Time Protocol (NTP) and often IRIG-B time sources. Once this is in place and functional, the Domain Controllers (low-resolution time sources) should be configured to follow the site time (high-resolution time source) reference instead of using themselves as the time reference. They will attempt to follow the site time reference, but will go back to using their own clocks as the reference in case of loss of the site time reference.

A set of procedures have been created to configure the Domain Controllers to follow a site time reference. Once the site time reference is operational (or whenever the IP address of the reference is changed), follow these procedures to configure the Domain Controllers to follow the site time reference. Refer to the section Configure Time on Domain Controllers.

When a computer (such as an HMI) is first joined to the domain, the Microsoft standard is to have it synchronize its time to the Domain Controllers. When the ControlST software (specifically WorkstationST* application) is installed and configured with a high-resolution (NTP) time reference, it turns off the Microsoft low-resolution time sync to the Domain Controllers. This prevents a low-resolution time source from resetting the time out from under the high-resolution time source. If the site high-resolution source becomes unavailable, the low-resolution Domain Controller trusts its own time and the HMI references will follow their own time. This result may cause a slow divergence between the Domain Controllers and the HMIs. If the difference becomes greater than the Kerberos ticket time window (typically five minutes), domain authentication may become affected. Resynchronizing the two time bases fixes the problem. If this looks to be a long-term situation, the procedures to configure the Domain Controllers can be rerun to direct them to the same (low resolution) time base that the HMIs are using. This action should provide for a stable time base in the system until the high-resolution system can be put back into service, and the Domain Controllers can be reconfigured to use the high-resolution time source again.
2.7 Redundancy Concepts

Many redundant functions are built into the control system, and care should be taken to include the intent of the redundancy when performing maintenance and upgrade operations. Here are some things to keep in mind when planning maintenance and upgrade operations.

**Domain Controllers:** There are two domain controllers in the system, DC1 and DC2. These are located in two different computers, and it is best not to have both of these computers disconnected at the same time. Microsoft Active Directory uses a combination of peer-to-peer and Flexible single master operation, or Operations Master concepts in maintaining the domain. To accomplish this, the domain controllers replicate information between each other to keep them up-to-date. When a domain controller is started, it attempts to contact an existing running domain controller to resynchronize itself. If two domain controllers are started together, it can take some time for them to resolve the fact that each one wants to trust the other one and not itself. By keeping at least one domain controller running at all times, it will smooth out the transitions. When performing software updates, the two domain controllers should be updated separately so that they are not both restarted at the same time.

**HMIs:** In areas of high use, such as a central control room, there are typically multiple HMIs for redundancy. When performing software updates, the HMIs in the redundant groups should be updated separately. Allow the HMIs in each group to be restarted after the update (if required) before starting the update for the other HMIs performing the same function.

**Communication Gateways:** Many sites include communication gateways or HMIs that include communication links (Modbus, GSM, OPC Servers) to other DCS systems. Most of these are implemented as redundant pairs where the communication link will fail-over to the other device when communication is lost. When performing software updates, the gateways with the communication links should be updated separately so that they are not both restarted at the same time.

**Network Redundancy:** The network is configured to be highly redundant, with dual NICs on most all devices connected to redundant switches that make up a dual redundant network. Little planning is required to maintain the network redundancy; however in a star topology, care should be taken not to bring down the redundant root switches. Procedures that require changes to the operating systems or configuration on the switches (aside from resetting passwords) should be completed on one member of the switch redundancy group and it should be back in full operation before starting on other switches in the group.
2.8 Availability Concepts

The configuration of Domain Services has been influenced by the concept of requiring a highly available system. While a normal IT environment may wish to totally shut down segments when a possible security issue is detected, the SecurityST environment balances that against the need for continued operation and availability. Towards that end, there are a number of settings and features that are somewhat different than often recommended practice. This section outlines some of the concepts used in configuring the Domain Services protected domain.

**Cached Credentials:** Each computer in the domain has (through Group Policy) been configured to cache the network credentials of the users that have logged on. If the domain controllers are unavailable or unreachable, the computer can still authenticate a user and allow access with the appropriate access rights with the cached credentials stored on the local computer. Microsoft limits this to the last 50 users and keeps credentials for a maximum of 30 days, so make sure at least one domain controller is brought back online within that 30 day window.

**Local Account - Network Switch or Router:** Each network device has a local management account defined. This local account will be disabled automatically when the network device can contact a RADIUS server on a Domain Controller (DC1, DC2) as a security measure. If contact with the Domain Controllers is lost, the network device will enable the local management account so that management access to the device is still available.

**Note** Refer to the section [Reset Switch Passwords](#) for to change the password on the switch local management account.

**Local Account - HMI:** Each HMI is shipped with a set of standard local accounts (Oper, Maint, Admin). In a Domain Services environment, users should not use these accounts. They should always use their individually identifiable domain account. When the Domain Services system is turned over to the site, the passwords on these local accounts should be reset and the passwords kept secret and secured (not distributed). In the case of an emergency situation where access through domain credentials is not possible (such as the Domain Controllers being unavailable for more than 30 days), the HMI local account passwords can be handed out for the duration of the emergency. When the domain has been reestablished and users can return to using their own accounts, the password on the HMI local accounts should be reset and kept secured for the next emergency situation. Domain Services includes an automation script that resets the local account passwords on all HMIs in the domain (ConfigureLocalAccounts). You do not need to visit each and every HMI to reset its local passwords.

In summary:

- The HMIs have local accounts for emergency operation outside a domain.
- The HMI local account passwords can all be reset at once using Domain Services.
- The HMI local account passwords should be set and restricted until needed.
- In case of domain collapse, the local account passwords can be revealed and the plant can be operated using the HMI local accounts.
- When the domain has been reestablished, the HMI local account passwords should be reset and kept secret until the next time they are needed.

While a plant is running without domain controller support and Mark Vle controllers are running in the Secure State, access to the controllers is limited. Local HMI accounts (as opposed to domain accounts) cannot be trusted, and will not have certificates to allow secure actions to be taken on the controllers. This restriction includes the ability to force and unforce variables, as well as the ability to download controllers, or take them out of Secure State.

While a plant is running without domain controller support, the Configuration Management System (CMS) subsystem will not be able to validate the user and therefore will block access to the CMS repositories.
DHCP Lease Times: The DHCP subsystem, when it hands out IP address leases, has been configured to hand out a long duration lease as opposed to a short duration lease that gets renewed often. This is intentional as strict interpretation of the DHCP rules states that if a DHCP client cannot contact a DHCP server to renew its lease it is not allowed to use the IP address any more and must drop off the network. DHCP clients first attempt to renew their leases with the DHCP server at 1/2 the lease time, so at worst-case a computer will drop off the network if the DHCP server has been unavailable for 1/2 the lease time. Domain Services defaults the lease time to twice the period where computers will no longer trust cached credentials so that DHCP is not the first roadblock during long periods of Domain Controller (which hosts the DHCP server) absence. While long lease periods may be an issue at sites with a lot of computers arriving and leaving the site, the Domain Services environment typically does not fall into that category, and the available range of IP addresses (254 addresses by default) is sufficient to support long term leases. If IP address pressures do arise, a domain administrator can enter the DHCP configuration and manually remove leases for computers that are no longer present to free up additional IP addresses.

2.9 Security Concepts

The following concepts were used to configure Domain Services, and care should be taken not to override them.

Network Isolation (Internal): Access to the UDH where the Mark VI and Mark VIe controllers reside is limited to servers that require access, and blocked from servers that do not need this access. The Application Servers that do need access to the UDH have limited user interfaces, and do not require users to log on to these servers during normal operations. This arrangement helps limit the exposure these servers have to potential malware. The Domain Controllers are not connected to the UDH.

Network Isolation (Routed): Communication between the various networks (such as the UDH, PDH, and MDH) is done through a network router to filter and forward traffic between networks. The router filters messages using a set of rules that allow traffic based upon items such as the source, destination, and type of message. Limiting the traffic that crosses between networks helps isolate equipment from potentially unwanted access while still providing required access. Devices that must communicate with other devices not on its networks should have their default gateway set to the router address on one of its networks. Devices that do not need to communicate outside their networks should not have default gateways defined, thereby helping to protect them from outside attack. (Routers and the UTM are supplied in the optional NetworkST 4.x product.)

Network Isolation (External): An optional UTM is used as an EAP when network connections must be established between equipment on the local networks (UDH, PDH, and MDH) and equipment outside those networks. The UTM provides various options for authenticating users prior to allowing access, including two factor authentication or one-time passwords. Once granted access, the UTM acts as a firewall to allow only limited types of communication to a limited set of devices. It is traditionally used to allow controlled remote access to computers in the MDH (such as an OSM or RSG), or to create a DMZ outside the local networks with controlled limited access to the equipment inside (usually limited to computers in the MDH). The UTM can also be used to provide controlled access to enterprise-level networks or external control networks. The UTM is not intended for connection to the Internet at large. The SecurityST product supplies monthly updates to keep the antivirus, software patching, and UTM up-to-date without being connected to the Internet. (Routers and the UTM are supplied in the optional NetworkST 4.x product.)

Limited Logon: The Domain Controllers and the UDH resident Application Servers do not require users to log on to these computers in normal operation. When a logon is required, the software run is typically part of the Microsoft Operating System and not third-party applications. The installation of third-party applications is extremely limited on these computers to reduce the attack surfaces and opportunities. Security applications that require routine logons are centralized Application Servers that are not resident on the UDH. Aside from security management functions, most information from the application servers is provided through web servers or share names to prevent all but security management users from ever having to log on to the application server.

Domain Administration: Changing the configuration of the domain requires a user who is a member of the Domain Admins group. This group has the ability to add a new computer to the domain. Requiring Domain Admins membership helps make sure that the person adding the computer to the domain will be able to add the computer to the correct OU to receive the proper hardening group policies.
# 2.10 CA1 Sharenames

The following table provides a list and descriptions of the sharenames that are present on the AP1 Application Server.

<table>
<thead>
<tr>
<th>AP1 Sharename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin_Documentation</td>
<td>Used for security administrator documentation. Domain Admins membership is required to read from this sharename.</td>
</tr>
<tr>
<td>Admin_Procedures</td>
<td>Used for security administrator procedures. Domain Admins membership is required to read from this sharename.</td>
</tr>
<tr>
<td>Documentation</td>
<td>Used for general access to security documentation. Everyone has read-access to this sharename.</td>
</tr>
<tr>
<td>Procedures</td>
<td>Used for general access security procedures. Everyone has read-access to this sharename.</td>
</tr>
</tbody>
</table>
3 Ongoing Operations

3.1 Account Overview

Domain Services is pre-configured with user and device roles known as security groups. Placing a device or user account in a security group assigns privileges and restrictions associated with that group. The role-based structure matches users and devices to their approved functions within the site.

Note As a security best practice, GE recommends the following:

Do not assign a user or device to a group with greater authority than is needed for their job (example: do not assign general users to an administrator group). This is the principle of least privilege.

Use named accounts wherever possible to provide traceability and accountability of any actions.

The HMI domain has defined user security groups. Domain administrators have rights to control devices within their domain. By contrast, enterprise administrators have rights to control all domains in the connected network. Thus, enterprise administrators can act as domain administrators for each domain.

For more information, refer to the section Active Directory Groups.

Note Per NERC and Federal Energy Regulatory Commission (FERC) regulations, it is the responsibility of the customer to manage user accounts and access passwords. The Control Server ships preconfigured with a default set of user names and passwords to access the system. The customer must change these system passwords before placing the system into service.

For more information, refer to the section Access Management and Permissions.
3.2 Access Management and Permissions

3.2.1 User Access Control

Users log on to an HMI with a domain account, which is a user name set up by the system administrator. Domain user names are controlled by Microsoft® Active Directory®. The two Active Directory servers in this system are DC1 and DC2.

To log on to a computer in the system, the user enters \HMI\<username>, where <username> is the individual user name assigned by the system administrator. Per NERC rules, each user must have an individual user name. In the Control Server, each user has an account with the specific permissions to perform their role. Logging on to an HMI causes the system to check the credentials against the list of legitimate domain users. Once authenticated, the user is permitted to log on.

Note: Consult your site policies for additional guidance on adding, suspending, or removing user access.

3.2.1.1 Grant Access

The system administrator creates the user names as part of adding a user to the system. As the system administrator creates a new user account, the account must be assigned to the appropriate groups that authorize access that the user requires. For further details, refer to the section New User Setup.

3.2.1.2 Suspend or Remove Access

Domain Services can be used to suspend (or remove) a user from the HMI domain based on security or operational needs. This step is performed from the Domain Controller DC1 (or DC2). For further details, refer to the section Suspend or Delete User.

3.2.2 Domain Updates

The system administrator can adjust domain memberships by either adding new HMIs to the system or changing the assigned groups to each user (thus matching assigned role). The properties of each user include its assigned groups. Refer to the following sections for these procedures:

- New User Setup
- Change User’s Assigned Role
- Add HMI to System
3.2.3 Group Policy Updates

GE provides a tested and approved group policy structure. If your environment requires modifications to the group policy settings or structure as supplied, be certain to place the new group policy above (or override) the existing group policy.

Failure to establish this hierarchy may cause your changes to be overridden when GE provides updates to its known existing group policy and structure.

Contact GE for assistance with modifying group policy structures or settings.

Where required, adjustments to group policy settings are made through the Server Manager on DC1.

➢➢➢ To view group policy settings

1. From the Primary Domain Controller (DC1), start the Server Manager.

2. From the Server Manager menu, select Tools and Group Policy Management.

3. From the Tree View, drill down to group policy objects as shown in the following figure.

4. From the Settings tab, view the current settings of the selected policy.
For example, settings for the HMI Computer Policy display like to the following:

![Group Policy Management](image)

**Note** The first time that the settings are displayed, a dialog box may display indicating that the content is blocked. Click *Add* to add *about:security_mmc.exe* to the list of trusted sites so that active content can be displayed. (Active content allows you to hide and show individual sections.) For more information, refer to the section *Add Website to Internet Explorer Trusted Sites List.*
3.2.4 Reset System Account Passwords

A set of applications within the Domain Services environment uses several predefined agent accounts as their credentials. The following procedures describe how to set the password for the agent accounts in Microsoft Active Directory, and how to set the password in the software (agent) that uses the account, including:

- DNS Agent
- Certificate application (Certificate app)

3.2.4.1 Reset Agent Account Password in Microsoft Active Directory

➢➢ To reset the user passwords in the Microsoft Active Directory

1. Log on to DC1 as a domain administrator.
2. Open the Server Manager using the task bar icon.
3. From the Server Manager menu, select **Tools**, then select **Active Directory Users and Computers**.
4. In the Active Directory Users and Computers tree view, expand **HMI.local**, and select **GE Controls**.
5. Right-click the User requiring a password reset and select **Reset Password**.
6. Enter the New password and Confirm the password, then click **OK**.

![Reset Password dialog box](image)

7. Click **OK** again. Once the password is changed for the agent account in the Active Directory, change the password for the agent account in the application that uses that account.

### 3.2.4.2 Reset DNS Agent Password

1. Complete the procedure in the section *Reset Agent Account Passwords in Microsoft Active Directory* to reset the DNS Agent user password.
2. Log on to DC1 as a domain administrator.
3. Start the Server Manager.
4. From the Server Manager menu, select **Tools**, then select **DHCP**.
5. From the Tree View, expand **dc1.hmi.local**.

![DHCP Tree View](image)

6. Right-click on **IPv4** and select **Properties**.
7. Select the **Advanced** tab, then click **Credentials**.
8. Enter the following credentials:
   
   a. For **User name** enter DNSAgent.
   
   b. For **Domain** enter HMI.
   
   c. For **Password** and **Confirm Password** enter the password you assigned to the DNSAgent account.

   d. Click **OK** to close **DNS dynamic update credentials** window.
   
   e. Click **OK** to close **IPv4 Properties** window.
   
   f. Repeat this procedure for DC2.
3.2.4.3 **Reset Certificate Application Password**

➢ To reset the Certificate Application password

1. Complete the procedure in the section *Reset Agent Account Passwords in Microsoft Active Directory* to reset the Certificate Application user password.

2. Log on to the Certificate Server (CA1) as a domain administrator.

3. Start the Server Manager.

4. From the Server Manager menu, select **Tools**, then select **Internet Information Services (IIS) Manager**.

5. From the Tree view expand **CA1 (HMI\Admin)** and select **Application Pools**.

6. Right-click on **SCEP** and select **Advanced settings**.

7. Select **Identify** and click the **Ellipsis (…)** on the same row.
8. Verify that the Custom account radio button is selected, then click **Set**.

9. From the **Set Credentials** dialog box, enter **HMI\CertificateApp** as the **User name** and enter and confirm the new password. Click **OK**.

10. Click **OK** to close the **Application Pool Identity** dialog box.

11. Click **OK** to close the **Advanced Settings** dialog box.
### 3.2.4.4 Reset UTM Password

- **To reset the UTM administrator password on the UTM device**

1. From a computer on the PDH network, open Internet Explorer, and enter the following URL: https://utm.hmi.local.
2. If a certificate error page is displayed, select **Continue to website (not recommended)**.
3. Log on to the device using UTM local credentials with administrator privilege.

4. From the System tree view expand **Admin** and select **Administrators**.

5. Double-click the account to display account details.

6. Click **Change Password**.
7. Enter the old password, the new password, and confirm the new password, then click **OK**.

8. Close the browser to log off the UTM device (changes are saved automatically).
3.2.5 Reset DSRM Administrator Password

Complete the following procedures to reset the Directory Services Restore Mode (DSRM) password on each system if the user elects to set it.

➢➢ To change the DC1 DSRM administrative password
1. Log on to DC1 as a domain administrator.
2. Open a command prompt window as an administrator.
3. Enter **NTDSUTIL**.
4. Enter **Set DSRM Password**.
5. Enter **Reset Password on server DC1**.
6. Enter the new password.
7. Re-enter the password to confirm it.
8. Enter Quit to exit the Reset Password utility.
9. Enter Quit again to exit the NTDSUTIL utility.

➢➢ To change the DC2 DSRM administrative password
1. Log on to DC2 as a domain administrator.
2. Open an administrator command prompt window.
3. Enter **NTDSUTIL**.
4. Enter **Set DSRM Password**.
5. Enter **Reset Password on server DC2**.
6. Enter the new password.
7. Re-enter the password to confirm it.
8. Enter Quit to exit the Reset Password utility.
9. Enter Quit again to exit the NTDSUTIL utility.

![Command Prompt Window](image-url)
3.2.6 Reset Switch Passwords

This section provides the following procedures:

- Reset Shared Secret and Enable Passwords in Switch
- Reset Shared Secret in RADIUS Server

3.2.6.1 Reset Shared Secret and Enable Passwords in Switch

The following procedure changes the enable password and the RADIUS shared secret in the GE-supplied Cisco® switches. The switches and other network devices must already be connected and configured to work in the RADIUS database before this procedure can be performed.

---

**Note** The shared secret is used by the switches when validating domain credentials of users logging into the system.

---

**Attention**

This procedure should only be attempted by an authorized network engineer familiar with the Cisco IOS®. Misapplication of this procedure can render the switch inoperative, and may require initialization by GE personnel to recover.

---

**Attention**

The shared secret must be set first in all the switches before it is set in the RADIUS Server on DC1 and DC2. If it is not, the user cannot log on to the switch using SSH.

---

➢ To set the shared secret and enable password at the switch

1. Log on to the Engineering Workstation (EWS).
2. Start the PuTTy application.
3. Enter the **Host Name (or IP address)** of the switch to configure.
4. Accept all other defaults, and click **Open**.
5. At the login as: prompt, enter the user name and press [Enter]. (User Name is an HMI domain user who has been granted Network Administrator privileges.)

6. Enter the password when prompted (nothing is echoed to the terminal when you enter the password).

The following text displays after a successful login.

```
NOTICE TO USERS!
This is an official computer system and is the property of the owner.
It is for authorized users only. Unauthorized users are prohibited.
Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.
Any or all uses of this system may be subject to one or more of the following actions:
interception, monitoring, recording, auditing, inspection and disclosing to security
personnel and law enforcement personnel, as well as authorized officials of other agencies,
both domestic and foreign. By using this system, the user consents to these actions.
Unauthorized or improper use of this system may result in administrative disciplinary
action and civil and criminal penalties. By accessing this system you indicate your
awareness of and consent to these terms and conditions of use.
Discontinue access immediately if you do not agree to the conditions stated in this notice.
```

```bash
172.16.201.220 - PuTTY
login as: geswitch
Unauthorized access prohibited Accessing AAA Servers Using keyboard-interactive authentication.
Password:
```
7. At the command prompt, type `enable`, and press [Enter].

8. When prompted for a password, enter the enable password.

![Enable prompt](image)

9. Type each configuration command in the order provided, and press [Enter] after each one.

   ```
   config t (puts you into config mode. Do not use CNTL/Z to end; this procedure uses `exit` to end.)
   ```

   ```
   enable secret <new_enable_secret>
   username admin privilege 15 <new_admin_password>
   radius-server host 172.16.201.102
      auth-port 1812 acct-port 1813
      key <new_shared_secret>
   radius-server host 192.168.201.101
      auth-port 1812 acct-port 1813
      key <new_shared_secret>
   exit (exits config mode)
   ```

   ```
   copy run start
   exit (exits PuTTY)
   ```

   The IP addresses listed with the commands are those for the Controllers (DC1 and DC2) where the RADIUS server resides. The new_shared_secret must also be entered in the RADIUS server exactly as entered in the switch.

10. Log off the EWS.
3.2.6.2 Reset Shared Secret in RADIUS Server

This procedure sets the shared secret for the Domain Controllers (DC1 and DC2).

The shared secret must be set first in all the switches before it is set in the RADIUS Server on DC1 and DC2. If it is not, the user cannot log on to the switch using SSH.

➢➢➢

To set the shared secret for the RADIUS Servers

1. Log on to DC1 as a domain administrator.
2. Start the Server Manager.
3. From the Server Manager menu, select Tools, then select Network Policy Server.
4. From the Tree View, expand Templates Management, then select Shared Secrets.
5. Double-click GE SWITCH SECRET to display the GE Switch Secret Properties dialog box.
6. Enter the new Shared secret and confirm the shared secret, then click OK.
7. Repeat this procedure to set the shared secret for DC2.
3.2.7 Reset Network Switch SNMP Security Parameters

The network switches are configured in the factory with default SNMP security parameters that the user should change to values that are unique to the site to prevent unauthorized access to the switch SNMP data. The user must also update these values in ControlST to allow the WorkstationST Control System Health (CSH) and Network Monitor features to read the SNMP data from the switches. Perform the following steps to reset the network switch SNMP security parameters for a site.

➢➢ To reset the network switch SNMP security parameters

1. Update the system-level SNMP security parameters used by the WorkstationST CSH and Network Monitor features. Refer to the procedure in the section Update ControlST Feature-level SNMP Security Parameters.

2. Modify the switch-level SNMP security parameter overrides used by the WorkstationST CSH and Network Monitor features for each network switch device in ToolboxST. Refer to the procedure in the section Update ControlST Switch-level SNMP Parameter Overrides.

3. Modify the SNMP security parameters configured for each network switch. Refer to the procedure in the section View/Update Cisco Switch SNMP Security Parameters.

3.2.8 Reset HMI Local Account Passwords

Each HMI is provided three local accounts: Admin, Maint, and Oper. The accounts are provided for use prior to the domain controllers being available and for emergency operation if the domain controllers become unavailable. Users should not use these accounts as part of normal operations. Users should use their individual domain accounts that were provided by the system administrator. A PowerShell script allows the system administrator to set the passwords for these accounts on all the HMIs.

Note The system administrator should set the passwords on these local HMI accounts and tightly control access to these accounts.

The password must conform to site policy rules and Microsoft Windows policy rules. Microsoft policy requires three levels of password complexity, and does not permit the user name to be embedded in the password.

➢➢ To reset a password for each local account on each HMI

1. Log on to Certificate Server (CA1) as a domain administrator.

2. Open an Administrator PowerShell console.

   Tip The default configuration of Windows® Server includes a PowerShell icon on the Windows taskbar that can also be used to start a PowerShell console. Right-click the icon, and select Run as administrator.

3. From the Windows PowerShell console, enter the following commands:
   a. cd C:\Procedures\Private
   b. .\Configure-LocalAccounts.ps1 <Account Name>
      (where <Account Name> is the name of the local account having its password reset; either Admin, Maint, or Oper).
Note  The script goes through all the computers in the GE Controls organization unit and its children organizational units as follows:

- GE Controls\HMI\Computers
- GE Controls\HST\Computers

3.2.9 Change Passwords Associated with Proficy Historian Analysis

3.2.9.1 Change Password for sa User Account (SQL Server)

➢➢ To change the password

1. Log in to the Historian VM as a local administrator (\admin, <password>).
2. From the Start menu, select SQL Server Management Studio.
3. Log in as an sa user by entering the following details:
   - Server Type = Database Engine
   - Server Name = xxx\PROFICYHST (xxx = computer name)
   - Authentication = SQL Server Authentication
   - User Name = sa
   - Password = <password>
   - Click Connect.
4. From Object Explorer perform the following:
   a. Select xxx\ProficyHst (xxx = computer name), Security, then select logins.
   b. Double click on sa user.
   c. Enter new password.
   d. Confirm new password.
   e. Click OK.
   f. Close the SQL Server Management Studio.
Update the SOADB Database

If the sa account password is changed perform the following procedure.

➢ To update the SOADB Database

1. Log in to the Historian VM as a local administrator (\admin).
2. From the Windows Explorer menu, navigate to ProgramFiles(x86)\Proficy\Proficy WorkFlow\Program and run the ConfigureDatabase.exe file.
3. Update the password for the SOADB database.
4. Click Save.

5. If the Services Running dialog box displays, click OK to continue.
3.2.9.2 Change Database Password in Proficy Vision 6.3

➢ To change the database password in Proficy Vision 6.3

1. Login to the GE Customer Center at https://ge-ip.force.com/communities/.

2. In the Search field, enter KB16850 and press [Enter] to search for the Knowledge Base article.

3. Select the article title How do you Change the Database Password in Vision 6.3? to display the instructions.

4. Perform the procedure in the article.

---

Note  All command prompt windows and text editors must be run as an administrator.

Additional information is available for the following procedures used in KB16850:

• Change KSP User Password in SQL Server Management Studio

• Restart Default Website in IIS Manager

---

➢➢ To change the KSP user password in SQL Server Management Studio

Attention  Do not change the KSP user password unless you are performing the procedure in the KB16850 article.

1. Log in to the Historian VM as a local administrator (\admin).

2. From the Start menu, select SQL Server Management Studio.

3. Log in as sa user.

4. From Object Explorer, perform the following:

   a. Select \xx\ProficyHst (xxx = computer name), Security, then select logins.

   b. Double click on KSPUser.

   c. Enter new password.

   d. Confirm new password.

   e. Click OK.

   f. Close the SQL Server Management Studio.
3.2.9.3 **Change Proficy Client Password**

➢ To change the Proficy Client account password

1. Log in to Historian VM as a local administrator (.\admin)
2. Start Proficy Client and Login (phaadmin).
3. Select the **Navigate** tab, **Personnel, People**, then select **phaadmin** (shown in the following figure).

4. From the **Displays** window, expand **Security Configuration** and select **Security Editor**.

5. Select **Edit Security Credentials**.
6. Enter a new password, enter the new password again to confirm, and click **Save**.

---

**Update web.config for SOAWebService where Password is Stored**

The password to the Proficy Client is saved in the SOAWebService, and used by the Provisioning Tool. There are two entries in the web.config for the SOAWebService where the password is stored.

➢➢➢

1. **To update web.config**
2. Open a command prompt window as an Administrator.
3. Change directory to `C:\Windows\Microsoft.net\Framework\<Version>`.
   *Note* `<Version>` is any of the subfolders of either Framework or Framework64 that contains the `aspnet_regiis.exe` file.
4. Run the following commands to decrypt the SOAWebService\web.config:
   a. `aspnet_regiis.exe -pd "secureAppSettings" -app "/SOAWebService"
   b. `aspnet_regiis.exe -pd "connectionStrings" -app "/SOAWebService"
5. Open `Notepad` as an Administrator.
6. Open `C:\inetpub\wwwroot\SOAWebService\web.config`.
7. Change the password to new password under:
   a. `<secureAppSettings>`
   ```xml
   <secureAppSettings>
     <add key="SoaUser" value="pha">
     <add key="SoaPassword" value="phapassword">
   ```
   b. `<connectionStrings>` (under “App.Properties”\SOAPASS WORD)
Note  Do not make any changes to the other Connection strings.

c.  Save and close the file.

7. Encrypt the sections by running these commands from command prompt.
   a.  aspnet_regiis.exe -pe "secureAppSettings" -app "/SOAWebService"
   b.  aspnet_regiis.exe -pe "connectionStrings" -app "/SOAWebService"

8.  Restart the Default Website in IIS Manager.

3.2.9.4 Change Proficy Historian Analysis Administrator Account

➢➢ To change the password

1. Start Proficy Vision (ignore Internet Explorer content blocked messages).
2. Log in to the PHA administrator account (phaadmin).
3. From the User drop-down menu, select User Preferences, then select Change Password.
3.2.10 **Password Maintenance for VMware**

### 3.2.10.1 Change VMware VCenter Administrator Account Password

➢ **To change the password**

1. Open Mozilla Firefox or Google Chrome.
2. Enter the address for HC1 (https://172.16.199.7).
3. Select Log in to vSphere Web Client as an administrator (administrator@vsphere.local).
4. From the **Menu**, select **Administration**.
5. Expand the **Single Sign-on** area.
6. Select **Users and Groups**.
7. Select the **Users** tab.
8. Select Username “Administrator”.
9. Select **Edit User**.
10. Enter the **Current Password**.
11. Enter the **New Password**.
12. Confirm the **New Password**.
13. Click **OK**.

### 3.2.10.2 Update Password Policy for VMware

➢ **To update password expiration policy for VMware Web Client**

1. Open Mozilla Firefox or Google Chrome.
2. Enter the address for HC1 (https://172.16.199.7).
3. Select Log in to vSphere Web Client as an administrator (administrator@vsphere.local).
4. From the **Menu**, select **Administration**
5. Expand the **Single Sign-on** area.
6. Select **Configuration**.
7. Select **Policies** tab.
8. Click on **Edit**…
9. Change the password policy settings.
10. Click **OK**.
3.2.10.3 Reset VMware Hypervisor Password

➢ To reset the Hypervisor password
1. Log on to MC3 as a domain administrator.
2. From the desktop, double-click the **VMware vSphere Client** icon.
3. Connect to HS1.
4. Log on to the root account for the Hypervisor.
5. If the inventory display window does not open, select **Inventory**.

6. In the tree view, select the **IP address for HS1**, and then select the **Users** tab.

7. Right-click **Root** and select **Edit**.
8. Select **Change Password**.
9. Enter and confirm the new password, then click **OK**.
10. Repeat for HS2 and MC2.
3.3 Certificate Management

The Certificate Authority used to manage certificates is Microsoft Active Directory Certificate Services. Refer to the Microsoft documentation for additional details on how to use the application.

3.3.1 Issue Individual Certificates

When a user logs on to an HMI for the first time, their account automatically receives a certificate from the Certificate Authority. The certificate is stored in the certificate store for the user on the HMI. Certificate Manager (certmgr) is used for viewing the certificate store for the user. Once the HMI user account has the certificate, the account can perform actions as per defined roles.

Certificates issued follow the user to the location of the logon request (certificate roaming). Certificates are issued automatically to users through certificate auto-enrollment.

➢➢

To view issued certificates

1. Log on to CA1.
2. Start Server Manager, and from the menu, select Tools, then select Certificate Authority.
3. Expand HMI-CA1-CA and select Issued Certificates.

---

To view issued certificates

1. Log on to CA1.
2. Start Server Manager, and from the menu, select Tools, then select Certificate Authority.
3. Expand HMI-CA1-CA and select Issued Certificates.
3.3.2 **Revoke Individual Certificates**

Users assigned to the Controller Role user groups are issued a certificate that allows them to authenticate with a controller operating in Secure State. If a user in one of the Controller Role groups is removed from the system, the certificate that was issued to that user should be revoked. This prevents the user who is no longer allowed on the system from authenticating to a controller.

Individual certificates can be managed through the Certificate Authority. Refer to the section *Account Overview*.

➢➢ **To revoke an individual certificate**

1. Log on to CA1.
2. Start **Server Manager**, and from the menu, select **Tools**, then select **Certificate Authority**.
3. Expand **HMI-CA1-CA** and select **Issued Certificates**.
4. Right-click the certificate to revoke, and select **All Tasks** and **Revoke Certificate**.
5. From the Tree View, select **Revoked Certificates**.
6. Confirm that the revoked certificate displays in the right side of the screen.
7. Right-click **Revoked Certificates**, and select **All Tasks** and **Publish**.

3.3.3 **Renew Expired Individual Certificates**

If a message displays that a certificate is missing or expired, the user must log off, then log on. The user account is then reissued a new certificate.
3.3.4 Renew System Certificates

Certificates are used by many features of the system for authentication. These certificates allow components and users to verify the identity of the component or user they are communicating with. Each component is configured with two certificates:

- A certificate unique to the component that uniquely identifies that component.
- A certificate that identifies the issuer of the certificates in the system. This certificate is called the root certificate.

The procedure regenerates all certificates on the system, including the root certificate. All certificates are regenerated normally only when the system is turned over to the customer. The goal is to invalidate certificates that were used for authentication before customer handover. The new certificates are in place when the customer takes control of the equipment.

All system users who rely on certificates for authentication need to have their certificates renewed. These systems/users are:

- Mark VIe controllers
- LS2100e Static Starters
- EX2100e Excitation Controls
- HMI users with Controller-Role certificates
- Remote Desktop Services (RDS)

Complete the following steps in the following order:

1. Take Controllers out of Secure State.
2. Revoke Issued Certificates.
4. Delete Previous Client Certificates.
5. Obtain and Install SSL Certificate in the UTM Device.
6. Renew RDS Certificates.
7. Renew https Certificates on CA1 and EWS.
8. Place Controllers in Secure State.

3.3.4.1 Take Controllers Out of Secure State

➢➢ To take controllers out of Secure State: refer to the ToolboxST User Guide for Mark Controls Platform (GEH-6700), the chapter Mark VIe Working Online, the section Secure State.

3.3.4.2 Revoke Issued Certificates

➢➢ To revoke issued certificates

1. Using an account with Domain Administrator privileges, log on to the Certificate Server (CA1).

2. Open Server Manager. From the Windows task bar, click the Server Manager icon.

3. From the server manager dashboard, select Tools, then select Certification Authority.

4. From the Tree View, expand HMI-CA1-CA and select Issued Certificates.

5. From the Issued Certificates list, select all certificates (select any certificate and press Ctrl+A), then right-click and select All Tasks and Revoke Certificate.
6. From the **Reason code** drop-down menu, select **Cease of Operation** and click **Yes** to revoke all issued certificates.
7. From the Tree View, right-click **Revoked Certificates** and select **All Tasks** and **Publish**.

![Publish Revoked Certificates](image)

8. From the **Publish CRL** dialog box, select **New CRL** and click **OK** to publish a new certificate revocation list.
3.3.4.3 **Renew Root Certificate**

➢ To renew a root certificate

1. Using an account with Domain Administrator privileges, log on to the Certificate Server (CA1) and click to open Server Manager.

2. From the Server Manager dashboard select **Tools** and **Certification Authority**.

3. From the Tree View, expand HMI-CA1-CA, select **Revoked Certificates**

4. Double-click the **CA Certificate**.

5. From the Certificate dialog box, select the **Details** tab and make note of the **Serial number** of the old root certificate. Click **OK** to close the certificate.
6. From the Tree View, right-click **HMI-CA1-CA**, and select **All Tasks, Renew CA Certificate**.
7. Click **Yes** to stop the Active Directory Certificate Services.

![Install CA Certificate dialog box]

8. Select **Yes** and click **OK** to create a public and private key pair.

![Renew CA Certificate dialog box]

9. If prompted to overwrite the private key, click **Yes**.

10. Close the CertSrv and Server Manager to allow certificate data to be refreshed when the Server Manager is reopened.

11. Restart the Server Manager, and then select **Tools**, and **Certification Authority**.

12. Expand **HMI-CA1-CA** select **Issued Certificates**.

13. From the right pane, double-click **CA Certificate**.

14. From the **Certificate** dialog box select the **Details** tab select **Serial number**. Click **OK** to close the certificate.

---

**Note**  The new root certificate version number should be different from the old version number.

15. Restart all HMIs to receive the new root certificate from Active Directory.
3.3.4.4 **Delete Previous Client Certificates**

Users who are members of the HMI domain Controller Role user group must replace their client certificates with new ones signed by the new root certificate. These user groups include:

- Controller Role-Base
- Controller Role-Set
- Controller Role-Force
- Controller Role-Download

➢➢

**To delete previous client certificates**

1. For each user account in one of the Controller Role user groups, log on to an HMI.
2. Map a share to `\CA1\Procedures\Public`.
3. Run the batch file `DeleteCertificates.bat` (double click on the .bat file).
4. Answer Yes (Y) to **Do you wish to continue and delete the user certificates**.
5. Log off the HMI.
6. Log on to the same HMI as a member of a Controller Role user group to force Active Directory to issue a new client certificate to the user. This new client certificate has been signed by the new root certificate.
7. Repeat the steps in this procedure for all users who are members of a Controller Role user group in the HMI domain. The intent is to delete a single instance of the old client certificate for all users that are members of these groups.

**Note** The command prompt window displays any certificates that were deleted.

```
Deleting Client Certificates

Confirm User Certificate Deletion
This operation deletes all user certificates issued by a specific Certificate Authority. It is typically only run in situations where all existing certificates must be replaced, such as when the trusted root certificate at the site has been changed.

Do you wish to continue and delete the user certificates? [Y] Yes [N] No [?] Help (default is "N")?: y
CA name: HMI-CA1-CA
Deleted 290000001EBA56CB7CE899DBCD000010000001E for user HMI\GEmaint at 2016-10-06 03:10:16
Deleted Client Certificates Complete
Press any key to continue . . .
```

5. Log off the HMI.
6. Log on to the same HMI as a member of a Controller Role user group to force Active Directory to issue a new client certificate to the user. This new client certificate has been signed by the new root certificate.
7. Repeat the steps in this procedure for all users who are members of a Controller Role user group in the HMI domain. The intent is to delete a single instance of the old client certificate for all users that are members of these groups.

**Note** Only one client certificate has to be deleted for each user in these groups. Active Directory replaces automatically all other instances of client certificates on other HMIs when the user logs on to those HMIs.

It may be necessary to perform these steps on more than one HMI if all ToolboxST users have not logged onto this particular HMI.
3.3.4.5 Obtain and Install SSL Certificate in UTM Device

The FortiGate UTM device includes a web server for the user interface. The web server uses an HTTPS connection to encrypt the transfer of credentials on the network, which indicates that it must be provided a certificate trusted within the domain. A script has been provided to obtain a certificate from the CA, which is then transferred to the UTM device. The UTM device then uses the configured certificate as its web server.

➢➢ To obtain the FortiGate certificate

1. Log on to the Certificate authority Server (CA1) using a Domain Administrator account.
2. Run PowerShell as an Administrator.

   Tip The default configuration of Windows® Server includes a PowerShell icon on the Windows taskbar that can also be used to start a PowerShell console. Right-click the icon and select Run as administrator.

3. From the Windows PowerShell console, enter the following commands:
   a. Cd C:\Procedures\Private
   b. .\Create-UTMCertificate.ps1

   ![PowerShell Console](image.png)

   Note The script creates the certificate files. Two new files display on the desktop: GEUTM.crt and GEUTM.key.

To copy the FortiGate certificate to the UTM device, refer to the Fortigate product documentation for importing an https certificate in the firewall documentation.
3.3.4.6 Renew Remote Desktop Services Certificates

This procedure deletes the certificates that are used by the Remote Desktop Services (RDS) to verify the identity of the server when a client connects.

Note This procedure should be performed whenever the root certificate of the Certificate Authority (CA) has been renewed. Refer to the section Renew Root Certificate.

➢➢ To renew RDS certificates
1. From CA1, log on to an account that is a member of the Domain Admins group.
2. Start a PowerShell console as an Administrator.
3. From the Windows PowerShell console, enter the following commands:
   a. `cd C:\Procedures\Private`
   b. `.\Delete-RDSCertificates.ps1`
4. When prompted, enter Y to delete remote desktop certificates. The script deletes remote desktop certificates from CA1, DC1, and DC2.
5. When complete, close the Windows PowerShell console.

The RDS certificates are regenerated automatically when the next group policy update occurs on the computers.
3.3.4.7 Renew https Certificates on CA1 and EWS

➢➢ To renew the https certificate on EWS

1. Log in to EWS as a domain Administrator.
2. Start the server manager.
3. From the server manager menu, select Tool, then select Internet Information Services (IIS) Manager.
4. In the tree view, select EWS (HMI\admin).
5. Double-click Server Certificates.
6. Right-click **EWS Web Server** and select **Renew**.

7. Select **Renew an existing certificate** and click **Next**.
8. To specify the online certificate server authority, click **Select...**

![Renew an Existing Certificate](image)

Specify online certificate server authority.

Specify the certification authority within your domain that will sign the certificate.

Specify Online Certification Authority:

Example: CertificateAuthorityName;ServerName

9. Select **HMI-CA1-CA** and click **OK**.

![Select Certification Authority](image)

10. Click **Finish**.

11. Repeat the above process for the CA1 server.

### 3.3.4.8 Place Controllers in Secure State

➢ To place controllers back into Secure State: refer to the *ToolboxST User Guide for Mark Controls Products* (GEH-6700).
3.4 UTM Account Management

3.4.1 Create New Administrator Account for UTM

Note Refer to the section Add Website to Internet Explorer Trusted Sites List if an untrusted site message displays.

➢➢ To create new Administrator account for UTM
1. Open a browser and navigate to the address https://utm.hmi.local.
2. Enter the credentials for an existing Administrator account.
3. Expand Admin and select Administrators.

4. Click Create New.
5. Enter the Administrator name and Password for the new account.
6. From the Admin Profile drop-down menu, select super_admin and click OK.
The New Administrator account displays.

<table>
<thead>
<tr>
<th>Name</th>
<th>Trusted Hosts</th>
<th>Profile</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEAdmin</td>
<td>0.0.0.0/0</td>
<td>super_admin</td>
<td>Local</td>
</tr>
<tr>
<td>NewAdmin</td>
<td>0.0.0.0/0</td>
<td>super_admin</td>
<td>Local</td>
</tr>
</tbody>
</table>
3.4.2 Delete GE Admin Account

**Note** Before performing this procedure, a new administrator account must be added to the UTM device. Refer to the section *Create New Administrator Account for UTM*.

**Note** Refer to the section *Add Website to Internet Explorer Trusted Sites List* if an untrusted site message displays.

**Attention**

Do not use the GE Admin account.

➢➢ To delete the GE Admin account

1. Open a browser and navigate to the address `https://utm.hmi.local`.
2. Enter the credentials for an existing administrator account.
3. Expand **Admin** and select **Administrators**.
4. Right-click the administrator account and select **Delete**.
5. Click **OK** to confirm the deletion.
3.5 **AVG Antivirus Maintenance**

### 3.5.1 Updating Antivirus Definitions

Updating of Antivirus Definitions should be done on one computer first, followed by a full system scan. The results of the scan should be verified before updating subsequent machines. If you have more than one type of VM (HMI, Historian, Engineering Work Station, and so forth) in the system, you should verify the updates on each type of VM before updating subsequent VM’s of that type.

➢➢ **To update AVG Antivirus definitions offline (from a local directory)**

**Note** Anytime Antiviruses are updated on a VM a full system scan should be done and the results verified.

1. On a computer with Internet access, go to [www.avg.com/update](http://www.avg.com/update).
2. Select the update files you need (typically Virus definitions and All necessary modules for your operating system) and download them to a portable media, such as a USB flash disk.
3. Make the portable media available to the desired window’s VM.

**Note** Refer to the *Control Server Dell Wyse Thin Client HMI System Support and Thin Client Maintenance Guide* (GEH-6842) for instructions to access the USB flash drive on the Thin Client.

4. Log in to the desired window’s VM to be updated.
5. Open your AVG program by double-clicking on the AVG desktop icon.
6. From the **Options** menu, click **Update from directory**.
7. Navigate to the folder where you stored the update files and click **OK**.

### 3.5.2 Grant Access to Incorrectly Blocked File

➢➢ **To create an Anti-Virus Exception**

1. Log in to the VM with an account that has administrator privileges.
2. Open the user interface for your AVG anti-virus by double-clicking on the AVG desktop icon.
3. Click the **Computer** tile on the main screen.
4. Click the advanced settings icon on the anti-virus tile.
5. From the *AVG Advanced Settings* dialog box select **Exceptions**.

![AVG Advanced Settings](image)

6. Click **Add exception**.

7. Click the **Exception Type** drop-down menu and select **Application or File** from the options.

8. Click **Browse** and select **All files (*.*)**.

![Browse All Files](image)

9. Select the program file you want to set as trusted and click **Open**.

10. Leave the default settings as displayed in the following figure.
11. Click **OK** to apply the new setting.

12. Click **OK** to close the advanced settings window. (Click **Yes** if Windows asks permission to save the change.)

### 3.5.3 Perform Full System Scan

➢➢ To perform a full system scan

1. Login in to the desired Windows VM to be scanned.
2. Open the AVG application by double-clicking on the AVG desktop icon.
3. From the **Options** drop-down menu, select **Scan Computer**.

**Note** Normal activity can continue while the scan is in progress.

4. When the scan is complete, review the results, take appropriate actions, and close the AVG window.
3.6 ControlST Software Suite Procedures

From the ToolboxST application, several properties must be set at both the system and component level for the controller to be placed in a Secure State.

3.6.1 System Editor Properties

➢ To configure the ToolboxST application

1. Open a .tcw file.
2. From the System Editor, expand the Property Editor.

3.6.1.1 Security Servers

The .tcw file must have the following Security Server properties configured:

• CA Server Full Name
• CA Server IP Address
• CA Server Thumb Print (Refer to the ToolboxST* User Guide for Mark* Controls Platform, GEH-6700, the section CA Server Thumb Print.)
• RSystem Log Server IP Address

➢➢ To configure the Security Servers: from the System Editor Property Editor, configure the properties for the Security Servers.

![Security Servers Configuration](image)
3.6.1.2 Configure UDH and MDH Gateways

**Note** These gateways must be configured for Network 4.0.

➢ To configure the UDH and MDH Gateways

For a source device to communicate to a target device where there is no common network, a default gateway must be defined as the router’s address on a network the source device is connected to.

1. Configure the **GatewayIPAddress** and **SubnetMask** properties of the UDH network to define the default gateway on the UDH network.

![Gateway IPAddress and Subnet Mask Configuration](image)
2. Configure the **GatewayIPAddress** and **SubnetMask** properties of the **MDH** network to define the default gateway on the MDH network.

**Note** For changes to the network default gateways to take effect, perform the *Build* and *Download* commands.
3.6.2 Component Editor Property

➢ To configure the command event log

1. From the System Editor, open a Mark VIe component.
2. From the Property Editor, set the Log to Disk property to Yes.
3.6.3 Configure Time on Domain Controllers

The Domain Services domain controllers have been configured by default to manage the time for all machines in the domain. To ensure that consistent time exists across the site system (including the Control Server VMs), the Control Server VMs must be configured to receive time from the same time servers as the rest of the system. The domain controllers should be configured to synchronize to the time sources in the ToolboxST configuration.

➢ To identify the time sources configured in the ToolboxST application: open the .tcw file for your system.

![Screenshot of ToolboxST with time synchronization settings]

**Designated Primary Time Source** is the time source used for the domain controllers.

**Note** Some sites also have a Designated Secondary Time Source. When available, the domain controllers can be configured to synchronize to both time sources. If one time source becomes unavailable, the domain controller then switches to the other.

A Windows PowerShell script has been created to assist in configuring the domain controllers to synchronize to the system time servers.
➢ To configure domain controllers to synchronize to system time servers

1. Log on to the Certificate Server (CA1) as a domain administrator.
2. Run PowerShell as an administrator.
3. From the PowerShell console, enter the following commands:
   • `cd C:\Procedures\Private`
   • `.\Set-TimeServers.ps1 -server <server1>, [<server2>]`
     where:
     <server1> is the DNS name or IP address of the Designated Primary Time Source.
     [<server2>] is optional, and is the DNS name or IP address of the Designated Secondary
➢ To verify that the time system has been configured properly

1. From DC1 or DC2, open a command prompt window as an Administrator.

2. Enter `w32tm /query /configuration`.

In the command output, the value displayed for NtpServer under NtpClient (Local) matches the NtpServer value entered in the PowerShell script. The server portion of this setting should match one of the displayed Time Sources (Primary or Secondary) in the ToolboxST application.
➢ To verify time server to which DC1 or DC2 is synchronizing

1. From DC1 or DC2, open a command prompt window.
2. Enter `w32tm /query /status`.

In the command output, the Source field displays the NTP server to which the computer is currently synchronizing.
3.6.4 **ToolboxST Application Users and Roles**

Regulatory standards often require that all system configuration changes be traced to individual users. Therefore, each user must be assigned an individual account.

Each new user account must be added to the ToolboxST application. The site administrator will determine the user role to be assigned for the ToolboxST and CIMPLICITY® applications.

**Note** Refer to the *ToolboxST User Guide for Mark Controls Platform* (GEH-6700).

➢➢ **To add a user account in the ToolboxST application**

1. Open the .tcw file using the ToolboxST application.
2. From the System Editor tree view, double-click the system item to display the System Information Editor.
3. From the Tree View, select **Users and Roles**.
4. From the Data Grid, enter a user name, then select the desired role from the drop-down menu.

5. For the new user, select the **HMI resources** cell.
6. From the HMI resources property, click the ellipsis (…) to select the devices available for changing variables and set points, and controlling HMI screens.
7. Select the available devices, use the arrow button to move devices to the selected list, and then click **OK**.

8. New user Name, Role, and HMI resources display. HMI resources are the devices that the user can access to configure, make variable and set point changes, and control HMI screens.

9. From the **File** menu, click **Save**, and close the system item.
Set Up CIMPLICITY Screens to Autostart

This procedure describes how to set up an Autostart CIMPLICITY screen to display when a user logs on to an HMI. Before completing this procedure, add the customer user account to the domain, and to the ToolboxST Users and Roles. For more information, refer to the section New User Setup.

Note If configuring an account for a user in the HMI Operators group, that operator must log on to the HMI once before completing this procedure.

➢➢ To set up CIMPLICITY to autostart

1. Log on to the HMI as the user who needs the CIMPLICITY screen to autostart.

Note If a user is a member of the HMI Operators group, that user does not have sufficient privileges to configure the Autostart screen. In this case, log on to the HMI as an HMI administrator.

2. Open Windows Explorer, and locate the CIMPLICITY screen that should open upon login of the customer user (such as Gt7f_startup.cim).

3. Right-click the screen name file, and select Send to, then select Desktop to create a shortcut.

4. Copy the CIMPLICITY screen file shortcut to the following directory:
   C:\Users\<User Name>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
   where <User Name> is the name of the user being configured.

5. Log off the HMI, and log on to the account that was just configured to verify the CIMPLICITY screen opens as required.
3.6.6 CMS Procedures

3.6.6.1 Add Domain Users to CMS

Each domain user who will access the CMS repository must be added as a CMS user.

➢➢

To add domain users to CMS

1. Log on to the EWS that is running the CMS Server using a domain account with administrator privileges.

2. From the desktop, double-click the CMS Administrator Tool icon.

3. Enter the **User name** and **Password** of a user with Administrator credentials.

4. From the CMS Administrator Tool menu, select **Repository**, then **Select**.

5. Select the repository from the drop-down menu and click **Open**.

6. From the **Users** menu, select **Add**.

7. Enter the name of the **User**, enable the **User has read-only access** setting if appropriate, then click **OK**.
When complete, the new user displays in the list of CMS Administrators.

<table>
<thead>
<tr>
<th>CMS Administrator - <a href="https://ts-ews.hmi.local/svn/BlueTeam">https://ts-ews.hmi.local/svn/BlueTeam</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File</strong></td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td><strong>User</strong></td>
</tr>
<tr>
<td>hmi\admin</td>
</tr>
<tr>
<td>hmi\geadmin</td>
</tr>
<tr>
<td>hmi\gemaint</td>
</tr>
</tbody>
</table>

### 3.6.6.2 Create Local Copy of System on HMI

This procedure allows you to connect to a CMS repository to create a local copy of a system on an HMI. The local copy can then be used to check out system components from CMS, make modifications, and check them in again.

For instructions to get a working copy from the CMS Server, refer to the *ToolboxST User Guide for Mark Controls Platform* (GEH-6700), the chapter *Configuration Management System (CMS)*, the section *Get System from Repository*. 

4 Common Procedures

The following sections describe common and recovery procedures for this system. If further assistance or technical information is desired, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

4.1 New User Setup

*Note* The domain administrator following site policies must determine what system privileges the operations and maintenance personnel receive. This decision is based on the use of Operator, Maintenance, and Administrator roles at each site.

This section includes the following information:

- *Example Group Assignments*
- *Add New User*
4.1.1 Example Group Assignments Based on Function

When creating a new user, the system administrator should carefully consider the functions that the user will need to perform and add them to the appropriate groups. The assignment should conform to the principle of least privilege. The following examples provide guidance in assigning groups based on functions performed. Refer to the section Account Overview for additional details on available groups.

**Note** The examples in the following table are for reference only.

<table>
<thead>
<tr>
<th>User Role</th>
<th>Group Membership</th>
<th>Functions</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Domain Administrator    | Domain Admins            | • Add users to a domain  
• Add computers to the domain  
• Add a switch to the system  
• Modify group policy  
• Deploy patches to domain computers | This example provides full access to the domain. Use caution when using this account because no restrictions exist on what it can do. |
| HMI Administrator       | HMI Administrators       | • Install software  
• Apply software updates  
• Administer CMS | This example allows an administrator to configure or modify the operating system or installed software. |
| HMI Maintenance         | HMI Maintenance  
Controller Role-Download | • Start ToolboxST application  
• Download controllers  
• Download HMIs | This example allows a maintenance user to download Mark Vle controllers, LS2100e Static Starters, and EX2100e Excitation controls. |
| HMI Operators           | HMI Operators  
Controller Role-Set    | • Start ToolboxST application  
• Set variables in controllers | This example allows a maintenance user to set variables in Mark Vle controllers, LS2100e Static Starter controllers, and EX2100e Excitation controllers.  
The Controller Role group is dependent on the site policies. The site could decide to have multiple types of HMI Operators users and grant them different Controller Roles. |
4.1.2 Add New User

➢ To add a new user to the system

1. Log on to DC1 as a domain administrator.
2. Start the Server Manager application (if it does not start automatically).
3. From the Server Manager menu, select Tools, then select Active Directory Users and Computers.
4. In the tree view expand HMI.local, GE Controls, and HMI.
5. Right-click Users and select New, then select User.
6. Enter user information and click **Next**.

7. Enter password information for the user, select the option to require a password change at next logon and click **Next**.
8. Confirm the new user in the domain and click **Finish**.

![New Object - User dialog box]

9. From the **Server Manager**, verify that the new account was added to the Users directory.

![Active Directory Users and Computers]

10. Double-click the new account name to display the **Properties** dialog box.
11. On the **Member Of** tab, click **Add** to select the appropriate group memberships for the new account. (Refer to section *Account Overview*, the table *Example Group Assignments based on Function*, and the section *Active Directory Groups* for assistance in selecting groups.)

![Image of Member Of tab](image1)

12. On the **Select Groups** dialog box, enter the desired group name. Available names typically include Operator, Maintenance, or Administrator groups according to site policies. Click **Check Names**; the group name displays as underlined if it is validated. Click **OK** to close.

---

**Tip**  
Click Advanced to search for groups from the full list available.

![Image of Select Groups dialog box](image2)

The Properties dialog box is displayed.

---
**Note** In this example, the Domain Administrator also added the new user *Joe H. Doe* to the *Controller Role-Set* and *HMI Operators* groups.

13. Click **Add** to make the new user account a member of another group, then click **OK**.
4.2 Add HMI to System

All procedures in this section must be completed in the order presented.

Attention

Complete the following procedures:

• Add HMI to Domain
• Configure DNS Server Addresses
• Add HMI to Domain

4.2.1 Add HMI to Domain

➢➢ To add an HMI to the Domain

1. Log on to the Primary Domain Controller (DC1) using an account that has privileges to add a computer to the domain.
2. From the task menu, start the Server Manager.
3. From the Server manager menu, select Tools, then select Active Directory User and Computers.
4. From the Tree View, expand HMI.local, GE Controls, and HMI.
5. Right-click Computers, and select New, then select Computer.
6. Enter the HMI name in the **Computer name** field, leave the **User or group** field as its default (Domain Admins), and click **OK**.
4.2.2 Configure DNS Server Addresses

➢ To configure DNS Server addresses

1. Log in to the HMI using an account with Administrator privileges.
2. From the Start menu, select Control Panel.
3. Click Network and Sharing Center.
4. Click change adapter settings.
5. Right-click PDH and select properties.

7. Select Use the following DNS server addresses.
8. For Preferred DNS server enter the PDH IP address for DC1.
9. For Alternate DNS server enter the PDH IP address for DC2.
10. Click Advanced....
11. Select **DNS**.
12. Click **Append these DNS suffixes (in order)**.

13. From the **TCP/IP DNS server** dialog box, type the domain suffix **HMI.Local** and click **Add**.

14. Verify that **Register this connection's addresses in DNS** is selected and click **OK**.
4.2.3 Add HMI to Domain

➢ To add the HMI to the domain

1. Log on to the HMI using an account that includes local administrator privileges.

2. From the Start menu, select Control Panel, System, and Advanced system settings. (If prompted for User Account Control, select Yes.)

3. From the System Properties dialog box, select the Computer Name tab and click Change.

4. Enter the Computer name, select Domain, and enter HMI in the Domain: field, then click OK.

5. From the Windows Security dialog box, enter the credentials of an account that has Domain Admin privileges to add a computer to the domain, and click OK. When the Welcome to Domain dialog box displays, click OK.

Note If entering HMI in the Domain: field generates the following error: An Active Directory Domain Controller could not be contacted, enter the fully qualified domain name HMI.local.
6. From the **System Properties** dialog box, click **Close**. When the following dialog box displays, click **Restart Now**.

![Microsoft Windows dialog box for restart](image)

The HMI performs a restart. As the restart completes, it receives updated group policies from the domain controller.

**Note** The computer may restart multiple times while the update process is completing.

### 4.3 Add Computer to MDH

Adding a computer to the MDH follows the same procedures as adding an HMI, with the following exceptions:

- When a computer is added to Active Directory® users and computers, it should be added to the an appropriate OU, such as the **GE Controls-HMI-Computers OU** or **GE Controls-HST-Computers OU**. This gives the computer the correct Group Policy Objects needed for operation in the MDH.
- The definition of the Default Gateway on the MDH NIC is always required. This must be set to the router address on the MDH (typically 172.16.0.1).
- Computers in the MDH that need to join the domain must have their RPC port range configured to pass through the router. To do this, Start PowerShell as an administrator and run the following script on the MDH computer:
  \CA1\Admin_Procedures\Setup-RPC_MDH.ps1, then perform a restart before you attempt to join the domain.

**Note** Refer to the section *Add HMI to System*. 

---

110 GEH-6845C Control Server - Domain Services Maintenance Guide Public Information
4.4 Add Switch

Before starting these procedures, verify that the network switches are installed with the latest posted configuration that supports SSH communication.

Note To gain access to switches configured for Control Server, the switches must be configured correctly in RADIUS. If RADIUS is not configured, console access is available through the serial link only if the switch is disconnected from the network.

➢➢➢ To add network devices to the RADIUS Client

1. Log in to DC1 as a network Administrator.
2. Start the Server Manager application (if it does not start automatically).
3. From the server manager menu, select Tools, then select Network Policy Server.
4. From the Tree View, expand RADIUS Clients and Servers.
5. Right-click RADIUS Clients and select New.

6. From the New RADIUS Client dialog box, select the Settings tab.

Note Click Select an existing template, then select GE Switch Template as the template populates the settings associated with that template. After these values populate, clearing Select an existing template permits you to edit settings as needed for your site.

7. If not already selected, click Select an existing template and select GE Switch Template.
8. When the GE Switch Template displays, clear select an existing template.
9. Enter the **Friendly name** and **IP address** of the new switch and click **OK**.

![New RADIUS Client dialog box](image)

**Note** If needed, click **Verify** to confirm the IP address of the switch. Consult the GE 4108 drawing or responsible engineering party for assistance with the friendly name and IP addresses.

10. Confirm that the Server Manager displays the new switch name.
4.5 Change User’s Assigned Role

A user’s role within applications can be modified through the assigned groups for the user.

➢ To change groups assigned to a user

1. Log on to DC1 as a domain administrator.
2. Start the Server Manager application (if it does not start automatically).
3. From the Server Manager menu, select Tools, then select Active Directory Users and Computers.
4. Expand HMI.local, GE Controls, and Users.
5. Right-click the user and select Properties.

6. From the Properties dialog box, select the Member of tab to display the currently assigned groups for the user.
7. Click Add to include additional groups.
8. Select a group and click Remove to delete its association with the user, then click OK.
### Joe H. Doe Properties

<table>
<thead>
<tr>
<th>Member Of</th>
<th>Active Directory Domain Services Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller Role:</td>
<td>HMI\local\GE Controls</td>
</tr>
<tr>
<td>Domain Users</td>
<td>HMI\local\Users</td>
</tr>
<tr>
<td>HMI Operators</td>
<td>HMI\local\GE Controls</td>
</tr>
</tbody>
</table>

- **Primary group:** Domain Users

There is no need to change the Primary group unless you have Macintosh clients or POSIX-compliant applications.

- **Add... Remove**
- **Set Primary Group**

- **OK Cancel Apply Help**
4.6 Suspend or Delete User

➢ To suspend user access
1. Log on to DC1 as a domain administrator.
2. Start the Server Manager application (if it does not start automatically).
3. From the Server Manager menu, select Tools, then select Active Directory Users and Computers.
4. Expand HMI.local, GE Controls, HMI, then select Users.
5. Right-click the user name and select Properties.
6. From the Properties dialog box, select the Account tab.

7. In the Account options: field, enable Account is disabled and click OK.
8. Revoke the Controller-Role certificate for the user (if one exists). (Refer to the section Revoke Individual Certificates.)

➢ To delete a user
1. Log on to DC1 as a domain administrator.
2. Start the Server Manager application (if it does not start automatically).
3. From the Server Manager menu, select Tools, then select Active Directory Users and Computers.
4. Expand HMI.local, GE Controls, HMI, then select Users.
5. Right-click the user, and select Delete.
4.7 Add Website to Internet Explorer Trusted Sites List

When an untrusted website with active content is detected, a message displays. To mark a site as trusted and allow active content, the site can be added to a Trusted Sites list.

**Note** Users must determine the appropriate sites to trust based on their site configuration. Contact GE for assistance.

➢➢ To add a Website to the Trusted Sites list

The Untrusted Site message should no longer display for that site.

**Note** Users should add about:blank to the list of trusted sites.
4.8 **Restart Default Website in IIS Manager**

➢ To restart the default website in IIS Manager

1. Start **Server Manager**.

2. From the menu, select **Tools**, then select **Internet Information Services (IIS) Manager**.

3. Restart IIS Manager.

4. Click **No** if the following dialog box displays.
4.9 Update ControlST Feature-level SNMP Security Parameters

The Control System Health (CSH) and Network Monitor features must be configured with the SNMP security parameters configured in the network switches. All of the switches at a site will typically use the same SNMP security parameters. The SNMP security parameters configured in the CSH and Network Monitor features are used for all of the network switches in the system.

Note: This section provides specific procedures to configure the ControlST feature-level SNMP security parameters. For more information on configuring SNMP settings in the CSH feature, refer to the WorkstationST Control System Health Instruction Guide (GEI-1000834). For more information on configuring SNMP settings in the Network Monitor feature, refer to the WorkstationST Network Monitor Instruction Guide (GEI-100693).

➢➢➢

To update ControlST feature-level SNMP security parameters

1. Open a ToolboxST system .tcw file and open the Workstation Device that is hosting the CSH or Network Monitor feature.

2. Select the **Control System Health** or the **Network Monitor** tab. The SNMP Mode and security information is configured and displayed from the WorkstationST Control System Health configuration tab, located under the Network Monitor Data Acquisition property group.

![SNMP V1 Configuration Properties](image)

SNMP V1 Configuration Properties
3. If the SNMP Mode is set to V1, modify the SNMP V1 Mode security parameters. Refer to the procedure in the section
   Modify SNMP V1 Mode Security Parameters.

4. If the SNMP Mode is set to V3, modify the SNMP V3 Mode security parameters. Refer to the procedure in the section
   Modify SNMP V3 Mode Security Parameters.
4.9.1 Modify SNMP V1 Mode Security Parameters

When SNMP Mode is set to V1, the SNMP V1 Community setting is the only SNMP security parameter shared between the SNMP Clients (CSH or Network Monitor) and the network switches.

➢➢➢ To modify the SNMP V1 security parameter

1. Click the **SNMP V1 Community** property **Edit** button to display the **Change Password** dialog box.

![Change Password dialog box](image)

2. Enter the new SNMP V1 Community name in the **New Password** field, re-enter it in the **Verify Password** field, and click **OK** to save it.

![Network Monitor Data Acquisition](image)

3. Perform a **Build, Download** to the WorkstationST device to save the configuration. The CSH and Network Monitor features restart and use the updated SNMP security parameters when sending SNMP requests to the network switches.
4.9.2 Modify SNMP V3 Mode Security Parameters

When SNMP Mode is set to V3, the SNMP V3 security parameters shared between the SNMP Clients (CSH or Network Monitor) and the network switches are SNMP V3 User Name, Authentication Password, and Encryption Password.

4.9.2.1 Modify SNMP V3 Authentication Password

➢➢ To modify the SNMP V3 Authentication Password

1. Click the **SNMP V3 Authentication Password** property **Edit** button to display the **Change Password** dialog box.

2. Enter the SNMP V3 Authentication password in the **New Password** field, re-enter it in the **Verify Password** field, and click **OK** to save it.

3. Perform a **Build, Download** to the WorkstationST device to save the configuration. The CSH and Network Monitor features restart and use the updated SNMP security parameters when sending SNMP requests to the network switches.
4.9.2.2 Modify SNMP V3 Encryption Password

➢➢ To modify the SNMPV3 Encryption Password

1. Click the SNMP V3 Encryption Password property Edit button to display the Change Password dialog box.

2. Enter the SNMP V3 Encryption password in the New Password field, re-enter it in the Verify Password field, and click OK to save it.

3. Perform a Build, Download to the WorkstationST device to save the configuration. The CSH and Network Monitor features restart and use the updated SNMP security parameters when sending SNMP requests to the network switches.

4.9.2.3 Modify SNMP V3 User Name

➢➢ To modify the SNMP V3 User Name

1. Select the SNMP V3 User Name property field and enter the SNMP V3 user name for the SNMP V3 User Name property.

2. Perform a Build, Download to the WorkstationST device to save the configuration. The CSH and Network Monitor features restart and use the updated SNMP security parameters when sending SNMP requests to the network switches.
4.10 Update ControlST Switch-level SNMP Parameter Overrides

The SNMP settings configured for the CSH and Network Monitor features are used for all of the network switches configured in the system; however, these feature-level settings can be overridden at the individual switch level. When the override is set for the switch device in ToolboxST, the CSH/Network Monitor features use the override values instead of the feature-level values. Perform the following procedures for each network switch in the system to determine if the SNMP Parameter Override is set and to modify the override parameters if it is.

**Note** This section provides specific procedures to configure the ControlST switch-level SNMP parameter override settings. For more information on configuring SNMP settings in the CSH feature, refer to the *WorkstationST Control System Health Instruction Guide* (GEI-1000834). For more information on configuring SNMP settings in the Network Monitor feature, refer to the *WorkstationST Network Monitor Instruction Guide* (GEI-100693).

4.10.1 Determine SNMP Parameter Override State

➢➢ To determine the state of the SNMP Parameter Override setting

1. Open a ToolboxST system .tcw file and open the switch device.
2. Locate the **SNMP Local Parameter Override** property under the SNMP Overrides property group.

---

**Image:**

- A screenshot of a switch device configuration window in ToolboxST.
  - The **SNMP Local Parameter Override** property is highlighted with a text box showing the value **False**.
  - Additional properties like **Management IP Address**, **Switch Type**, and others are visible in the configuration window.

---
3. If the SNMP Local Parameter Override value is False, the feature level SNMP values are used for this switch and no further actions are needed.

4. If the SNMP Local Parameter Override value is True, the CSH or Network Monitor features use the override settings when requesting SNMP data from the switch and these values must be modified as followed:
   a. If the SNMP Mode is set to V1, modify the SNMP V1 Mode security parameters. Refer to the procedure in the section Modify SNMP V1 Mode Security Parameter Settings.
   b. If the SNMP Mode is set to V3, modify the SNMP V3 Mode security parameters. Refer to the procedure in the section Modify SNMP V3 Mode Security Parameter Settings.

4.10.2 Modify SNMP V1 Parameter Override Settings

If the SNMP Mode is set to V1, perform the following procedure to change the SNMP V1 Community Name.

➢➢ To modify SNMP V1 Community Name

1. Click the SNMP V1 Community Name property Edit button to display the Change Password dialog box.

2. Enter the new SNMP V1 Community Name in the New Password field, re-enter it in the Verify Password field, and click OK to save it.

3. Perform a Build to build the switch device, save the configuration, automatically restart the CSH or Network Monitor feature, and use the updated SNMP security parameter overrides when sending SNMP requests to the corresponding network switch.
4.10.3  **Modify SNMP V3 Parameter Override Settings**

When SNMP Mode is set to V3, the SNMP V3 parameter override settings are SNMP V3 User Name, Authentication Password, and Encryption Password.

4.10.3.1  **Modify SNMP V3 User Name Override Setting (Optional)**

Perform the following procedure to change the SNMP V3 User Name used in the switch.

➢➢ To modify the SNMP V3 User Name Override setting

1. Select the **SNMP V3 User Name** property field and enter the SNMP V3 user name.

2. Perform a **Build** to build the switch device, save the configuration, automatically restart the CSH or Network Monitor feature, and use the updated SNMP security parameter overrides when sending SNMP requests to the corresponding network switch.

4.10.3.2  **Modify SNMP V3 Authentication Password Override Setting**

Perform the following procedure to change the SNMP V3 Authentication Password used in the switch.

➢➢ To modify the SNMP V3 Authentication Password Override setting

1. Click the **SNMP V3 Authentication Password** property **Edit** button to display the **Change Password** dialog box.

2. Enter the new SNMP V3 Authentication password in the **New Password** field, re-enter it in the **Verify Password** field, and click **OK** to save it.

3. Perform a **Build** to build the switch device, save the configuration, automatically restart the CSH or Network Monitor feature, and use the updated SNMP security parameter overrides when sending SNMP requests to the corresponding network switch.
4.10.3.3 Modify SNMP V3 Encryption Password Override Setting

Perform the following procedure to change the SNMP V3 Encryption Password used in the switch.

➢➢➢ To modify the SNMP V3 Encryption Password Override setting

1. Click the SNMP V3 Encryption Password property Edit button to display the Change Password dialog box.

2. Enter the new SNMP V3 Encryption password in the New Password field, re-enter it in the Verify Password field, and click OK to save it.

3. Perform a Build to build the switch device, save the configuration, automatically restart the CSH or Network Monitor feature, and use the updated SNMP security parameter overrides when sending SNMP requests to the corresponding network switch.
4.11 View/Update Cisco Switch SNMP Security Parameters

Perform the procedures in this section to view and/or update the SNMP security parameters configured in the Cisco switch. These procedures require a connection to the switch in Enable mode. For the procedure to connect to the switch in Enable mode before performing these procedures, refer to the section Connect to Switch in Enable Mode using PuTTy Application.

Note Replace text in <> in the following sections with the appropriate value.

4.11.1 View Current Switch SNMP Settings

➢➢ To view the current switch SNMP settings

1. Run the `show run | include snmp` command.

```
SW2#show running-config | include snmp
snmp-server group GroupV3 v3 priv access 61
snmp-server group GroupV3 v3 priv context vlan- match prefix access 61
snmp-server community sws RO 61
```

2. Run the `show snmp user` command to view the currently configured SNMP V3 users.

```
SW2#show snmp user
User name: v3user
Engine ID: 80000090300186B9D85903
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: DES
Group-name: GroupV3
```

Note SNMP V3 user Authentication and Encryption (privacy) passwords are not viewable. These passwords are managed by a site administrator. If these passwords are lost, it will be necessary to reconfigure the SNMP V3 user with new passwords in the switch and make the corresponding changes in the ControlST configuration.

4.11.2 Modify SNMP V1 Community Name

➢➢ To modify SNMP V1 Community Name

1. Run the `config terminal` command to enter the switch configuration mode.

2. Run the `snmp-server community <newCommunityName> RO 61` command to create a new community name with Read Only privileges.

3. Run the `no snmp-server community <oldCommunityName>` command to remove the old community name.

4. Run the `exit` command to return to the switch enable mode.

5. Run the `copy run start` command to make the changes permanent.
4.11.3  Modify SNMP V3 Security Parameters

Each SNMP V3 user has an associated Authentication and Encryption password. In some cases, a site may want to keep the existing user and simply modify the associated passwords. Other sites may have stricter rules and require modification of the username and passwords. These procedures are provided in this section.

4.11.3.1 Modify SNMP V3 User Passwords Only

➢➢ To modify the Authentication and Encryption passwords for an existing SNMP V3 user

1. Run the `configure terminal` command to enter the switch configuration mode.

2. Run the `snmp-server user <existingUsername> GroupV3 v3 auth md5 <newAuthenticationPassword> priv des <newEncryptionPassword>` command to modify the passwords for the existing user.

3. Run the `exit` command to return to the switch enable mode.

4. Run the `copy run start` command to make the changes permanent.

4.11.3.2 Modify SNMP V3 Username and Passwords

➢➢ To create a new user with updated Authentication and Encryption passwords

---

*Note*  The existing user should be removed after the new user is created.

---

*Note  Replace text in <> with the appropriate value.*

1. Run the `configure terminal` command to enter the switch configuration mode.

2. Run the `snmp-server user <newUsername> GroupV3 v3 auth md5 <newAuthenticationPassword> priv des <newEncryptionPassword>` command to create the new SNMP V3 user.

3. Run the `no snmp-server user <oldUsername> GroupV3 v3` command to remove the existing user.

4. Run the `exit` command to return to the switch enable mode.

5. Run the `copy run start` command to make the changes permanent.
4.12 Enable SNMP V3 Support in Cisco Switch not Configured for SNMP V3 Support

SNMP V3 support requires the configuration of a group with SNMP V3 access, as shown in the following figure.

Note For the procedure to view the current switch SNMP settings, refer to the section View Current Switch SNMP Settings.

If a group with SNMP V3 access is not configured in the switch, perform the following procedure to create the required SNMP V3 group and user.

➢➢ To create the required SNMP V3 group and user

Note Replace text in <> with the appropriate value.

1. Refer to the section Connect to Switch in Enable Mode using PuTTY Application and perform the procedure to connect to the switch in enable mode.
2. Run the configure terminal command to enter the switch configuration mode.
3. Run the snmp-server group GroupV3 v3 priv access 61 command to create the SNMP V3 group.
4. Run the snmp-server group GroupV3 v3 priv context vlan- match prefix access 61 command to give the group visibility to all of the vlan contexts in the switch.
5. Run the snmp-server user <username> GroupV3 v3 auth md5 <authenticationPassword> priv des <encryptionPassword> command to create the SNMP V3 user.
6. Run the exit command to return to the switch enable mode.
7. Run the copy run start command to make the changes permanent.
4.13 Connect to Switch in Enable Mode using PuTTY Application

Perform the following procedure to log in to the switch to check and/or modify the switch configuration.

Only attempt this procedure if you are an authorized network engineer familiar with the Cisco IOS®.

➢➢ To connect to the switch using the PuTTY application

1. Log on to the Engineering Workstation (EWS).
2. Start the PuTTY application.
3. Enter the Host Name (or IP address) of the switch to configure.
4. Accept all other defaults, and click Open.
5. At the *Username:* prompt, enter the user name and press [Enter]. (User Name is an HMI domain user who has been granted Network Administrator privileges.)

6. Enter the password when prompted (nothing is echoed to the terminal when you enter the password and there may be a delay before the command prompt is displayed).

   Unauthorized access prohibited Accessing AAA Servers
   Username: admin
   Password:

   Unauthorized access prohibited Accessing AAA Servers
   Username: admin
   Password:

   The following command prompt displays after a successful login.

   Unauthorized access prohibited Accessing AAA Servers
   Username: admin
   Password:

   SW2>

7. At the command prompt, type *enable*, and press [Enter].

8. When prompted for a password, enter the enable password.
4.14 View ControlST Configured Switch SNMP Settings

➢ To view ControlST configured switch SNMP settings: hover over each switch device in the Network Status Viewer to display the tool tip information, including the SNMP mode and security parameters.

Configured Switch SNMP Settings Displayed in Network Status Viewer
4.15 Create and Deploy SDI Certificates for WorkstationST Features

When a Mark VIe controller (V06.00 or higher) is running in Secure mode, clients who send SDI commands to the controller are required to have an SDI certificate. This certificate identifies the client and defines the commands that client is allowed to issue.

WorkstationST features (and other background programs) that send SDI commands must be issued certificates for these connections. SDI secure connection certificates are only required if the WorkstationST feature (or other background program) issues SDI commands. A standard HMI issuing only EGD-based setpoint commands does not require an SDI connection certificate. An HMI running a program that issues SDI commands (such as the ExperTune® application or an HMI supporting the WorkstationST Device Manager Gateway feature) requires an SDI certificate. Typically, a Controller Role-Set certificate is required for these programs to allow them to request that values be changed in the controller.

The following table lists the certificates that may be needed, depending on which functions the site requires.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Certificate Type</th>
<th>Certificate Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>GeCssOpcServer</td>
<td>Set</td>
<td>Only required if computer needs to support SDI Write commands (such as when using ExperTune application)</td>
</tr>
<tr>
<td>GeCssDeviceManagerGateway</td>
<td>Set</td>
<td>Only required if computer needs to support Device Manager Gateway function to controllers in Secure mode</td>
</tr>
</tbody>
</table>

➢➢ To create and deploy an SDI certificate

1. Log in to the CA1 VM using an account that is a member of the Domain Admins group.
2. Open an administrator mode PowerShell window.
3. Navigate to the /Procedures/Private directory.
4. Run the Create-SDICertificate.ps1 script to create the needed certificate(s).
   - Example: Create-SDICertificate -Subject GeCssOpcServer
   - Example: Create-SDICertificate -Subject GeCssDeviceManagerGateway

Note The script defaults to a Controller Role of Set. If something else is needed, use the -CertType parameter to override the certificate template used.

5. Follow the instructions provided at the end of the script to export the resulting certificate to a PFX file. Be sure to include the private key and protect it with a strong password.

Note The PFX file is used by the deployment script to push the certificate to the computers that need it; you do not need to visit each computer to install the certificate or copy the PFX file to each computer.

6. Run the Deploy-SDICertificate.ps1 script to deploy the certificate in the PFX file to the target computer(s).
   - Example: Deploy-SDICertificate -Filename GeCssOpcServer.pfx -Password "NotMyPassword" -ComputerName EWS1_SVR
   - Example: Deploy-SDICertificate GeCssOpcServer.pfx "NotMyPassword" -ComputerName CRM1_SVR,CRM2_SVR
Appendix A Reference

Default Address Information

In some cases, this information is available through the GE 4108 drawing provided as part of site setup. Otherwise, contact your GE representative for assistance with default IP address information for each device. The binder shipped with the system also includes additional address information.

Default Credentials

Attention

It is the responsibility of the site to change these default account credentials upon system handover. It is also the responsibility of the site to maintain and hold confidential new and existing account credentials, and make them available to authorized personnel only.

Contact your GE representative for assistance with default account and password information.

Expected Local and Domain Accounts

At the time of system handover, the site must review the list of local accounts that are configured in the system, and compare with the expected local accounts. For user accounts that are not on the expected list, the site must verify whether the account is valid.

Note  Software installed on the computer may create a local/domain account for its use. The site must determine whether a local account not on this list is legitimate.

Attention

The site is responsible for all accounts not listed in the following tables.
### Provided Local Accounts and Status

<table>
<thead>
<tr>
<th>Computer</th>
<th>User Name</th>
<th>Function</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA1, MC3</td>
<td>Admin</td>
<td>Administrator User</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>Built-in Windows Operating System</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Guest</td>
<td>Built-in Windows Operating System</td>
<td>Yes</td>
</tr>
<tr>
<td>HMI</td>
<td>Admin</td>
<td>Administrator User</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>Built-in Windows Operating System</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Guest</td>
<td>Built-in Windows Operating System</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Maint</td>
<td>Maintenance User</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Oper</td>
<td>Operator User</td>
<td>No</td>
</tr>
<tr>
<td>HIST</td>
<td>Admin</td>
<td>Administrator User</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>Built-in Windows Operating System</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Guest</td>
<td>Built-in Windows Operating System</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Maint</td>
<td>Maintenance User</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Oper</td>
<td>Operator User</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>SOAWebService</td>
<td>Built in PHA account</td>
<td>No</td>
</tr>
</tbody>
</table>

### Provided Domain Accounts and Status

<table>
<thead>
<tr>
<th>User Name</th>
<th>Function</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Domain Administrator</td>
<td>No</td>
</tr>
<tr>
<td>Administrator</td>
<td>Built-in Windows Operating System</td>
<td>Yes</td>
</tr>
<tr>
<td>Guest</td>
<td>Built-in Windows Operating System</td>
<td>Yes</td>
</tr>
<tr>
<td>Certificate Application</td>
<td>Certificate Authority</td>
<td>No</td>
</tr>
</tbody>
</table>
Glossary

**Active Directory** is the Microsoft Active Directory access and account management application that includes Certificate Services

**Certificate Authority (CA)** is an application used to issue and revoke digital certificates

**Cisco IOS** is the Cisco Internetwork Operating System multitasking operating system for network and telecommunications functions

**Electronic Access Point (EAP)** is the point where external devices and networks connect to the site local devices and networks. An EAP allows external access to devices in the ESP

**Electronic Security Parameter (ESP)** is a networked region of the plant where site local computers reside. An ESP is required to cross into or out of the ESP. Determination of what is inside and outside the ESP is essential for defining and maintaining site security.

**Group Policy Object (GPO)** is a collection of computer configuration settings sent from domain controllers to computers that join the domain. GPOs change settings to allow certain applications to run, and are also used to harden computers in the domain.

**Hardened** is the state of a computer or network device that has been configured through settings or application installations to be less vulnerable to security-related attacks

**Hypervisor** is the physical server divided to support the work of several virtual servers

**Monitoring Data Highway (MDH)** is a network containing computers that only need to monitor plant operation

**Plant Data Highway (PDH)** is a plant-level supervisory network connecting the HMI server with remote viewers, printers, Historian applications, and external interfaces

**Remote Authentication Dial-In User Service (RADIUS)** provides network authentication for privileged access.

**Secure Shell (SSH)** is a cryptographic network protocol for secure data communications.

**Unified Threat Manager (UTM)** is an optional separate device that monitors network traffic crossing the ESP using rules and attack definitions

**Unit Data Highway (UDH)** is the portion of the network that carries controller-to-controller or controller-to-HMI data
Notes
Index

A
Active Directory 16
  group policy 21
  groups 19
  Organizational units 16
  users 18
Add
  Computer to MDH 110
  HMI to Domain 104, 109
  HMI to System 104
  New User 99
  Switch 111
Add Network Devices to RADIUS Client 111
Add Website to IE Trusted Sites List 116
AVG Antivirus 81
  Exception 81
  Full System Scan 83
  Updating Definitions 81

C
CA1
  Sharenames 35
Certificate Authority 24
Certificate Management 64
  Delete Previous Client Certificate 72
  Individual 64
  Obtain and Install SSL Certificate 73
  Place Controllers in Secure State 77
  Renew Expired 65
  Renew https Certificates on CA1 and EWS 75
  Renew Remote Desktop Services Certificates 74
  Renew Root Certificate 69
  Renew System Certificates 66
  Revoke Individual Certificates 65
  Revoke Issued Certificates 66
Certificates
  SDI 133
  WorkstationST features 133
Change User’s Assigned Role 113
CIMPLICITY 94
Cisco 127, 129
CMS Procedures 95
  Add Domain Users 95
  Create Local Copy of System on HMI 96
Computer 110
Configure
  DNS Server Addresses 106
Control Server Core
  HA 11
Control Server Module 12
Controller
  domain hardening 28
Controllers 66, 77
ControlST
  Component Editor Property 87

D
Database Password in Proficy Vision 6.3 57
Defense-in-Depth 15
Device Manager Gateway 133
DHCP Server 27
DNS Server 26
DNS Server Addresses 106
Domain Services Module 12

E
EGD 133
Enable SNMP V3 Support 129
ExperTune 133

F
Feature-level 118

G
Group Assignments 98

H
Hardening 28
High Availability (HA) Core 12
HMI 133
  Add to domain 109
  add to domain controller 104
  Add to system 104
HMI Local Account Passwords 54

I
IIS Manager
  Restart Default Website 117
IP Address Management 26

M
MDH 110
MDH Gateways 85

N
network
  switches 30
Network Switch SNMP Security Parameters
  Reset 54

P
Password