GEH-6848A

Control Server
Hand-over Guide

Public Information

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.

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

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.

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: April 2018
Issued: March 2017

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

Document Updates

Location	Description
Reset Switch SNMP Security Parameters	Added this section with a reference to the *Control Server Domain Services Maintenance Guide* (GEH-6845) for the procedure to reset the switch Simple Network Management Protocol (SNMP) security parameters

Related Documents

Doc #	Title
GEH-6703	ToolboxST User Guide for Mark Controls Platforms
GEH-6839	Mark VIe Control Systems Secure Deployment Guide
GEH-6844	Control Server System Overview
GEH-6845	Control Server — Domain Services Maintenance Guide

Contents

1 Hand-over Overview

Note Information provided from third-party applications can vary due to updates. Consult the third-party documentation for the latest information. Application vendors retain trademark and copyright protections as permitted by law or contract.

This document provides the procedures required to hand over the Control Server to a customer.

These procedures *must* be completed in the order presented:

1. *Create New Customer Accounts*
2. *Configure ToolboxST Users and Roles*
3. *Remove Controllers from Secure State*
4. *Transition CMS Repository to New Customer Account*
5. *Delete GE Accounts for HMI*
6. *Change Administrator Account Password on Certificate Server*
7. *Set Administrator Password on DC1*
8. *Configure Domain Time Server*
9. *Verify Local Accounts*
10. *Reset Account Passwords*
11. *Renew System Certificates*
12. *Return Controllers to Secure State*
13. *Update Antivirus Protection and Scan System*
14. *Complete and sign the Hand-over Checklist*

2 Create New Customer Accounts

User roles (Operator, Maintenance, Administrator, and such) for the site must be determined by the site administrator. This individual must also create the site user accounts such that each user is a member of the correct groups to match the user role (duties). Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *New User Setup*.

Note Certificates will only be issued to customer accounts that are members of Controller Role groups.

3 Configure ToolboxST Users and Roles

Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *ToolboxST Application Users and Roles*.

4 Remove Controllers from Secure State

Note This procedure applies to all Mark* VIe controllers, EX2100e Excitation controllers, and LS2100e Static Starter controllers. Refer to the *ToolboxST User Guide for Mark Controls Platforms* (GEH-6700), the section *Secure State* for the specific product (Mark VIe, Mark VIeS, MarkStat, EX2100e, or LS2100e).

➢ **To remove controllers from Secure state**

1. Log on to an HMI using the new customer account that is a member of the *Controller Role-Download* group.
2. Open the site project *.tcw* file.
3. From the ToolboxST* System Editor, open a Mark VIe controller and go online.
4. From the **Device** menu, select **Security State**.
5. If the controller is in the Secure state, click **Open** to go to the Open state.
6. Repeat these steps for each Mark VIe control, EX2100e Excitation control, LS2100e Static Starter control, and MarkStat power conversion control in the system.

5 Transition CMS Repository to New Customer Account

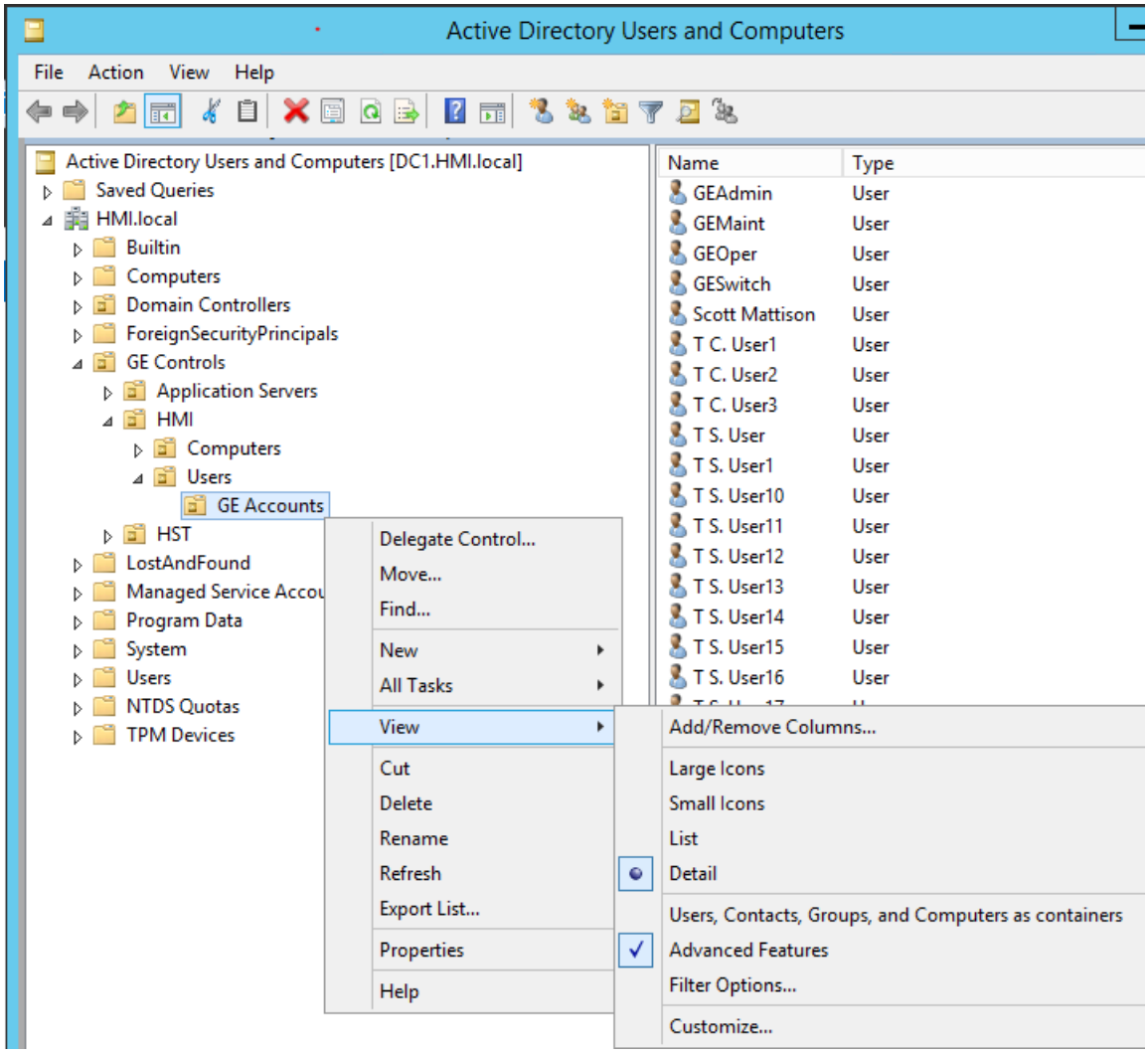
Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *Add Domain Users to CMS*.

6 Delete GE Accounts for HMI

Note After being deleted, an account will not function. If another user is logged in to an account when it is deleted, their session may become unstable and they will need to log off.

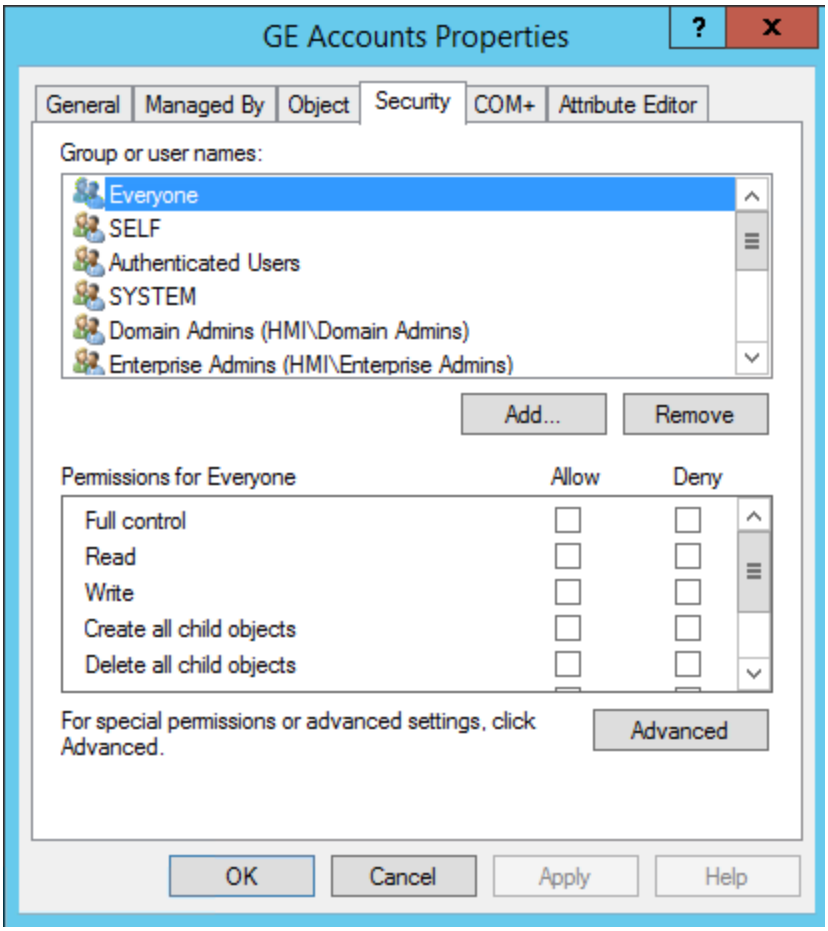
➢ To delete GE accounts for HMI

1. From the Primary Domain Controller (DC1), log on to an account that is a member of the *Domain Admins* group.
2. From the Task bar, click the server manager icon  to launch the Server Manager.
3. From the Server Manager menu, select **Tools**, **Active Directory Users** , and **Computers**.
4. Expand HMI.local, GE Controls, HMI, Users.
5. Right-click **GE Accounts**, select **View**. (Advanced Features should have a check mark next to it. If it does not, select **Advanced Features**.

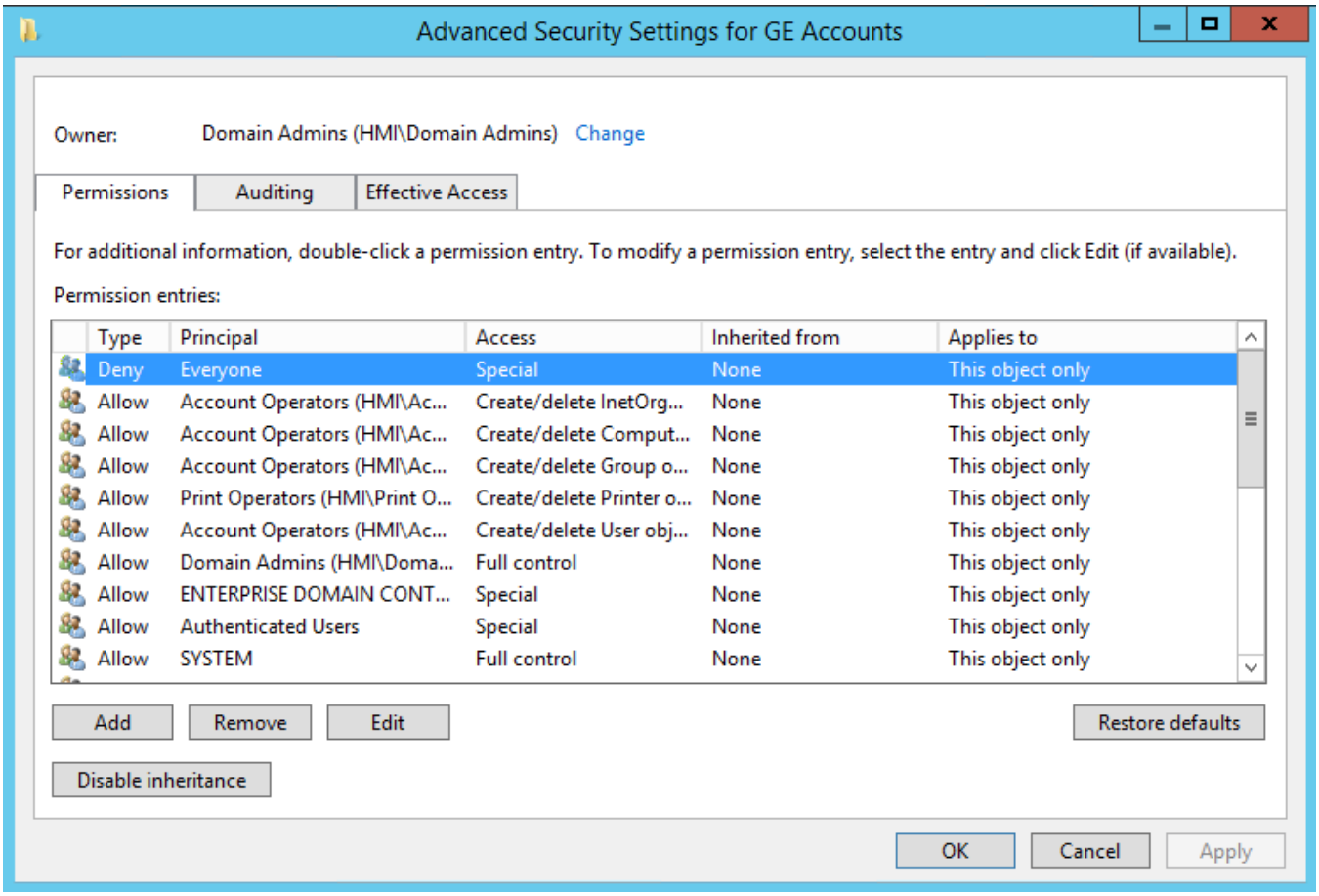


6. From the tree view, right-click **GE Accounts** and select **Properties**.

7. Select the **Security** tab, select **Everyone** listed for Group or user names, then click **Advanced**.

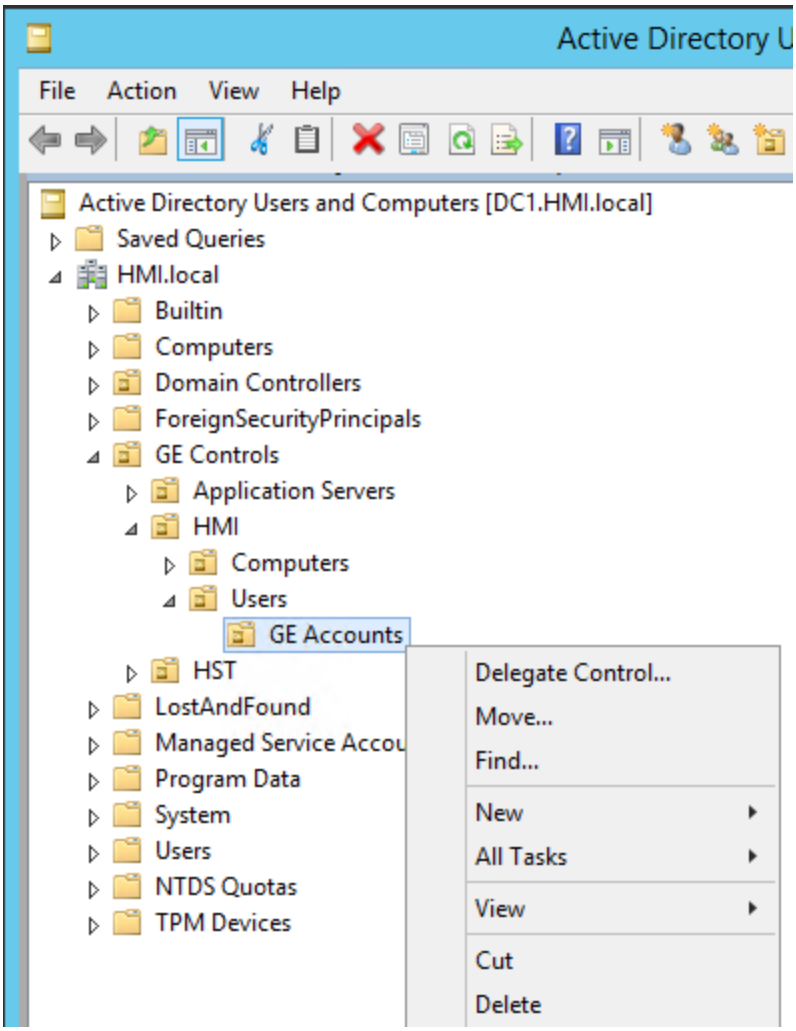


8. From the **Permissions** tab select the **Deny Everyone** row and click **Remove**.

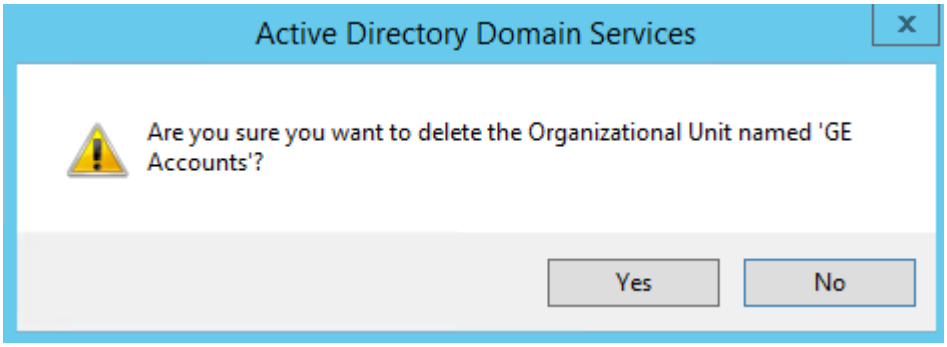


9. Click **Apply**, then click **OK**.

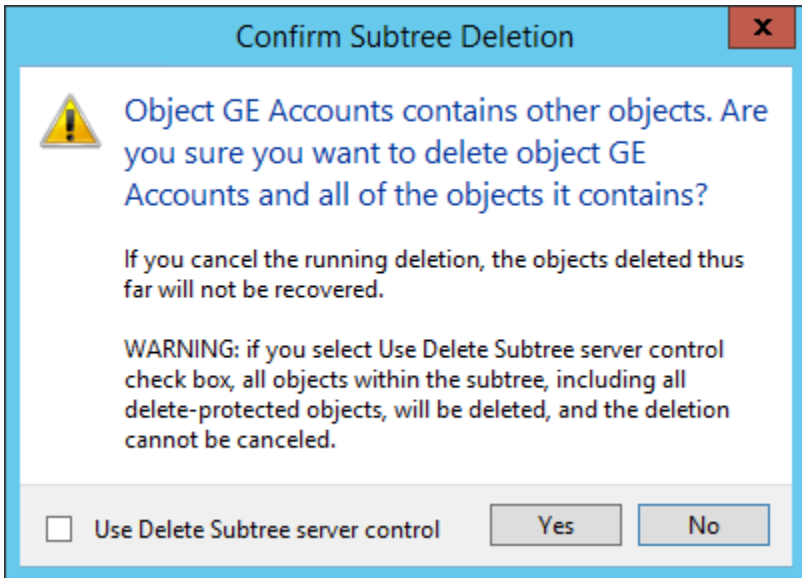
10. From the tree view, right-click **GE Accounts** and select **Delete**.



11. Click **Yes** to confirm deletion.

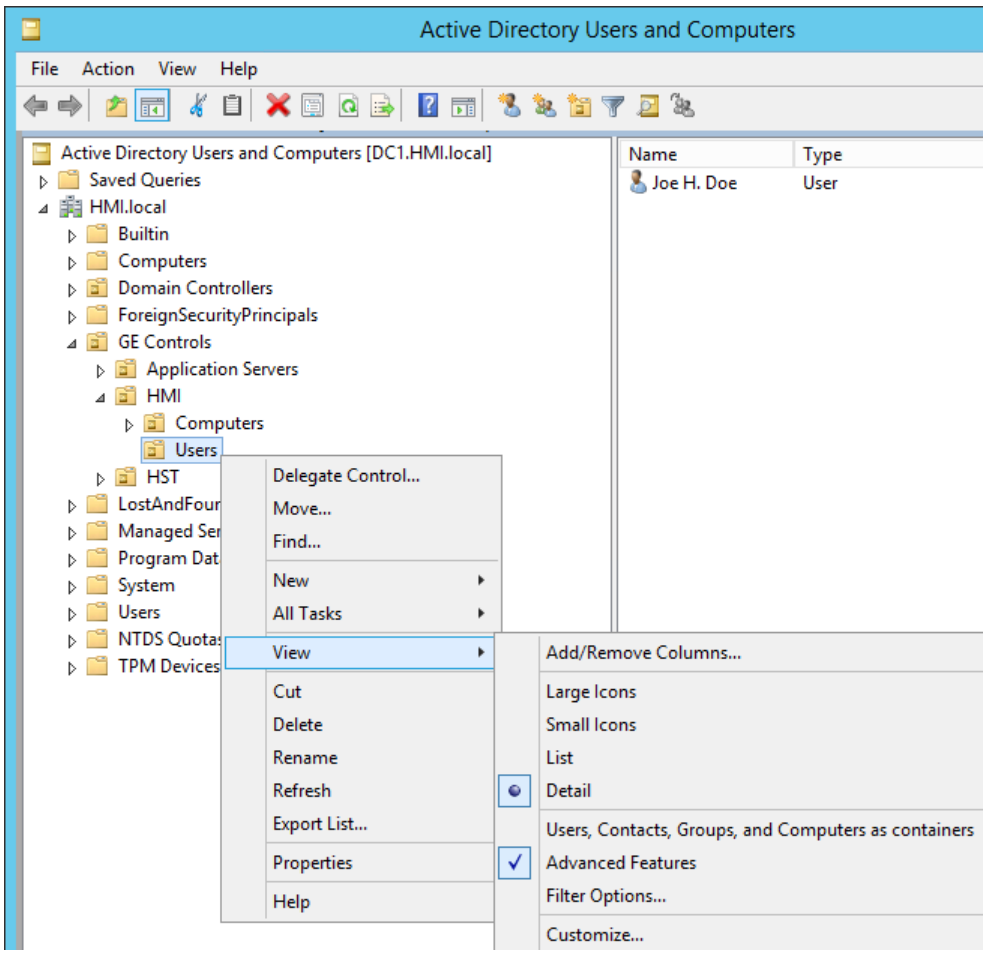


12. Click **Yes** to confirm the subtree deletion.



Note Once the *GE Accounts* folder in the Server Manager tree view has been deleted, the *Users* folder will be automatically highlighted.

13. Right-click **Users**, select **View**, then select **Advanced Features** to disable this feature (removes the check mark).

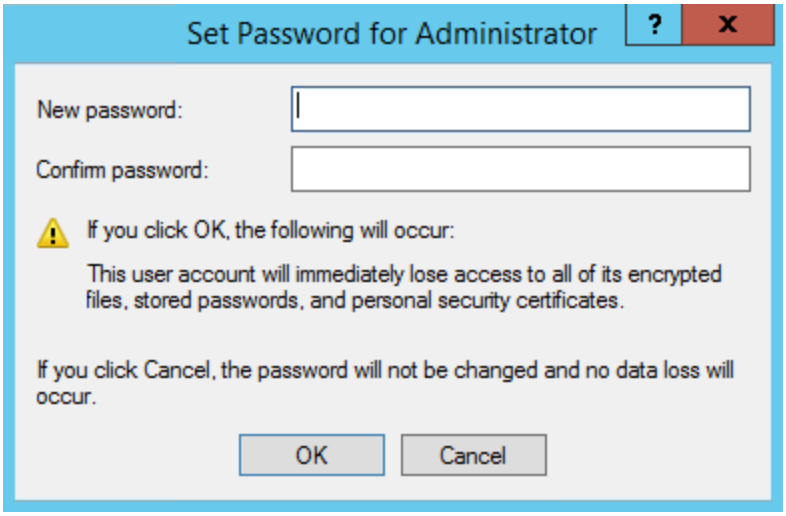


7 Change Administrator Account Password on Certificate Server

➢ **To change the password of the administrator account on the Certificate Authority Server CA1**

1. From CA1, log on to an account that is a member of the *Domain Admins* group.
2. From the taskbar, open the Server Manager.
3. From the Server Manager menu, select **Tools**, then select **Computer Management**.
4. Expand **Local Users and Groups** and select **Users**.
5. Right-click the Admin account and select **Set Password**.
6. From the warning dialog box, click **Proceed** to display the *Set Password for Admin* dialog box.

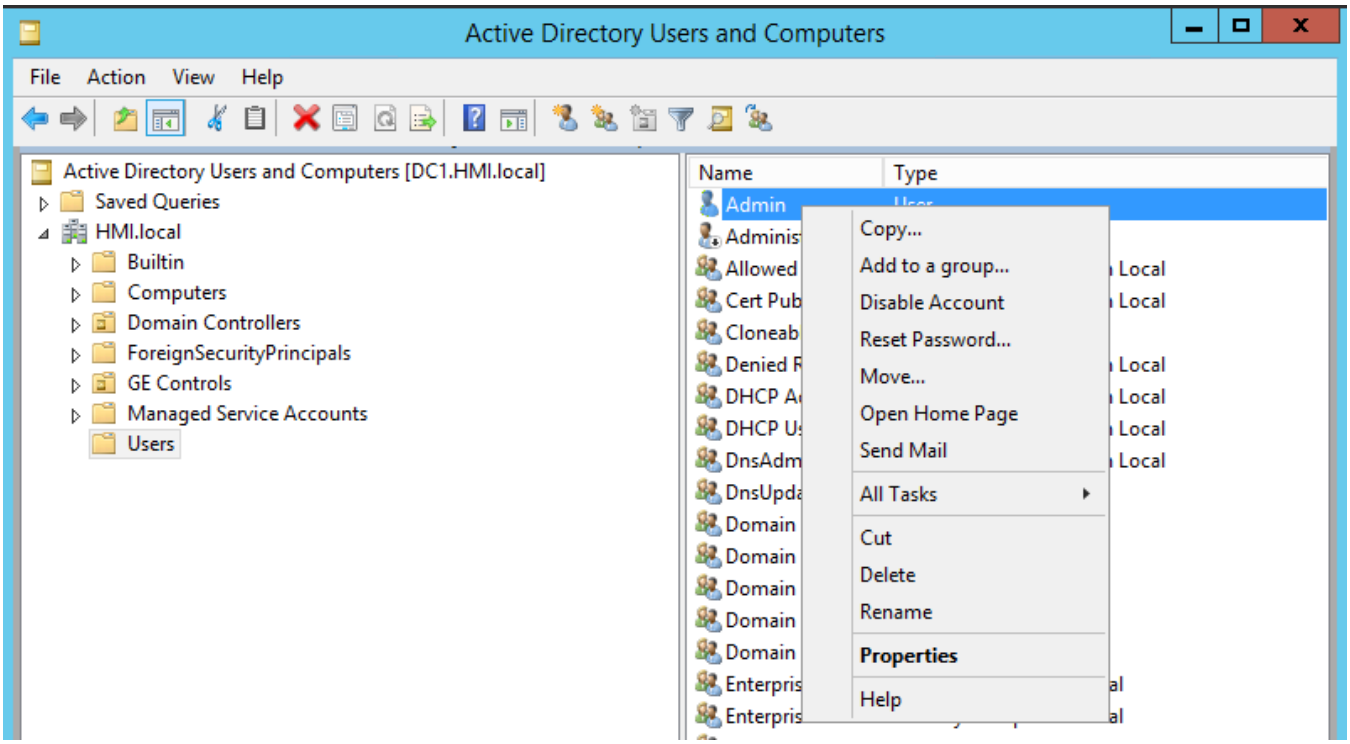
7. Enter and confirm a unique password and click **OK**.



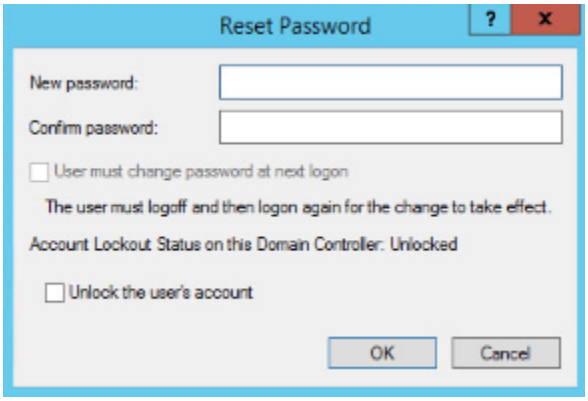
8 Set Administrator Password on DC1

➢ **To reset the administrator password for the Primary Domain Controller DC1**

1. From DC1, log on to an account that is a member of the *Domain Admins* group. If another user is logged on to an account when it is deleted, their session may become unstable and they will need to log off.
2. From the taskbar, open the Server Manager.
3. From the Server Manager menu, select **Tools**, then select **Active Directory Users and Computers**.
4. Expand **HMI.local**, and select **Users**.
5. From the **Users** list, right-click **Admin** and select **Reset Password**.



6. Enter a new password and confirm the new password, then click **OK**.



The Backup Domain Controller (DC2) will synchronize with DC1 to reflect these changes.

9 Configure Domain Time Server

This procedure causes the domain controllers to synchronize with the site time source. Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *Configure Time on Domain Controllers*.

10 Verify Local Accounts

Perform the following procedure to verify that no local accounts were added to any Windows® operating system computers (including virtual machines) in the system. Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), for more information.

➢ **To verify local accounts**

1. From an Engineering Workstation (EWS), log on to an account that is a member of the *Domain Admins* group.
2. Map a network share drive to *\\CA1\Procedures\Private*.
3. Copy the file *Get-LocalAccounts.ps1* to the local Temp directory.
4. Open a Powershell window as an Administrator.
5. Enter the command **Cd c:\temp** (local temp directory where the file was copied).
6. From the PowerShell command window, enter **.\Get-LocalAccounts.ps1** to display local accounts on all computers (including virtual machines) in the domain.
7. Resolve all local accounts not included on the list of valid accounts. Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), *Appendix A References*, the section *Expected Local and Domain Accounts* and the table *Provided Local Accounts and Status* for a list of valid accounts.

11 Reset Account Passwords

The Control Server includes predefined accounts and passwords used during the initial setup and configuration. When you reset these during the hand-over process, you are assured that only site personnel have access to the system. When creating the passwords, do not use any type of *pattern or template*. Knowledge of a password should not provide any clues as to the value of another password. Do not follow the example of GE Standard passwords. They are not appropriate for production systems, and must be changed.

Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the chapter *Ongoing Operations*, to complete the procedures in the following sections. These procedures must be completed in the order presented.

11.1 Reset System Account Passwords

Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *Reset System Account Passwords* to reset the following passwords:

Note This step includes procedures to reset agent and account passwords.

---

1. DNS agent

2. Certificate Application

11.2 UTM account management

Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *UTM Account Management* to perform the following functions:

1. Create new administrator account

2. Delete GEAdmin account

11.3 Reset DSRM Administrator Password (Directory Services Restore Mode)

Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *Reset DSRM Administrator Password*.

11.4 Reset Switch Passwords

Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *Reset Switch Passwords* to perform the following functions:

Note This step includes procedures to set shared secret and console passwords.

---

1. Set shared secret and enable passwords in switch

2. Set shared secret in RADIUS server

11.5 Reset Switch SNMP Security Parameters

For the procedure to reset the switch Simple Network Management Protocol (SNMP) security parameters, refer to the *Control Server Domain Services Maintenance Guide* (GEH-6845), the section *Reset Switch SNMP Security Parameters*.

11.6 Reset HMI Local Account Passwords

Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *Reset HMI Local Account Passwords*.

11.7 Reset VMware Hypervisor Passwords

The VMware hypervisor accounts on HS1, HS2 and MC2 are initially configured with a standard password. The user must change these passwords during the hand-over process per the guidelines of the local site. Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *Reset VMware Hypervisor* for the procedure to change this password.

11.8 Change VMware Vcenter Administrator Account Password

The administrator account for VMware Web Client is initially configured with a standard password. The user must change this password during the hand-over process per the guidelines of the local site. Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *Change VMware VCenter Administrator Account Password* for the procedure to change this password.

11.9 Update Password Policy for VMware

Prior to shipment the password policy is set such that Passwords never expire. This policy setting should be changed if necessary to match the site's operational and security policies. Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *Update Password Policy for VMware* for the procedure to change this policy.

11.10 Change Passwords Associated with Proficy Historian Analysis

The Proficy Historian Analysis (PHA) is initially configured with a set of standard passwords. The user must change these passwords during the hand-over process per the guidelines of the local site. Refer to the following sections in the *Control Server — Domain Services Maintenance Guide* (GEH-6845) for the procedures to change these passwords:

- *Change Password for sa User Account (SQL Server)*
- *Change Proficy Client Password*
- *Change Proficy Historian Analysis Administrator Account*

12 Renew System Certificates

The Certificate Authority (CA) root certificate is used for authentication in the domain. When the system is turned over to the customer, the root certificate must be updated. This update invalidates all prior certificates.

➢ **To renew system certificates**

1. Confirm that the controllers are not in the Secure state. Refer to the section *Remove Controllers from Secure State*.
2. Renew the system certificates by completing the following procedures in the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *Renew System Certificates*. Complete these procedures in the order given:
   a. *Revoke Issued Certificates*
   b. *Renew Root Certificate*
   c. *Delete Previous Client Certificates*
   d. *Obtain and Install SSL Certificate in the UTM Device*
   e. *Renew RDS certificates*
   f. *Renew https Certificates on CA1 and EWS*
   g. *Place controllers in Secure State* (if you previously removed them from the Secure State)

13 Return Controllers to Secure State

➢ **To return controllers to the Secure state**

1. From the ToolboxST System Editor, open and go online with each controller.
2. From the **Device** menu, select **Security State**.
3. From each controller that is in the Open state, click **Secure** to go to the Secure state.

14 Update Antivirus Protection and Scan System

This procedure updates all antivirus signatures and runs a full virus scan to all computers. Refer to the *Control Server — Domain Services Maintenance Guide* (GEH-6845), the section *AVG Antivirus Maintenance* for this procedure.

15 Hand-over Checklist

Site personnel must complete this checklist and a signed copy of this completed checklist is required as part of the Control Server hand-over process. Check with the GE representative on site for further details.

- □ Create new customer accounts
- □ Remove controllers from Secure State
- □ Transition CMS repositories to new customer account (*if used*)
- □ Delete GE accounts for HMI
- □ Rename default administrator accounts on Certificate Authority Server CA1
- □ Set administrator password on DC1
- □ Configure domain time server
- □ Verify local accounts
- □ Reset system account passwords
  - □ HMI\CertificateApp
  - □ HMI\DNS agent
- □ UTM Account Management (*if present*)
  - □ Create new administrator account for UTM
  - □ Delete GE admin account
- □ Reset Directory Services Restore Mode (DRSM) administrator password
  - □ DC1 server
  - □ DC2 server
- □ Reset switch passwords
  - □ Set Shared Secret and enable password in each switch
  - □ Set SNMP security parameters in each switch
  - □ Set Shared Secret in DC1 RADIUS server
  - □ Set Shared Secret in DC2 RADIUS server
- □ Reset HMI Local account passwords
- □ Reset VMware hypervisor passwords
  - □ HS1
  - □ HS2 (*Core HA only*)
  - □ MC2 (*Core HA only*)
- □ Change VMware Vcenter administrator account password (*Core HA only*)
- □ Update password policy for VMware (*Core HA only*)
- □ Change passwords associated with Proficy Historian analysis (*if present*)
- □ Renew system certificates
  - □ Revoke issued certificates
  - □ Renew root certificate
  - □ Obtain and install an https (SSL) certificate to the UTM device (*if present*)
  - □ Delete previous client certificates
  - □ Renew RDS certificates
  - □ Renew https certificates on CA1 and EWS
- □ Return controllers to Secure state
- □ Update antivirus protection and scan system

Signature:_____ Date:_____

Printed Name:_____