Control Server
Dell® Windows® 10 Thin Client HMI System
Support and Maintenance Guide

June 2019
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.

Issued: June 2019

© 2019 General Electric Company.

* 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
Acronyms and Abbreviations

CAL  Client Access License
CSH  Control System Health
DHCP Dynamic Host Configuration Protocol
EWS  Engineering Workstation
HMI  Human-machine Interface
MAC  Media Access Control
PDH  Plant Data Highway
RDP  Remote Desktop Protocol
RDS  Remote Desktop Services
UDH  Unit Data Highway
VM   Virtual Machine

Related Documents

<table>
<thead>
<tr>
<th>Document #</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEH-6840</td>
<td>NetworkST 3.1/4.0 for Mark VIe Controls Application Guide</td>
</tr>
<tr>
<td>GEH-6846</td>
<td>Control Server Installation and Startup Guide</td>
</tr>
<tr>
<td>GEH-6863</td>
<td>Control Server Dell Windows 10 Thin Client HMI System User Guide</td>
</tr>
<tr>
<td>GEH-6865</td>
<td>Control Server Dell Windows 10 Thin Client HMI System Secure Deployment Guide</td>
</tr>
<tr>
<td>GHT-200059</td>
<td>How to Remove Unused Software for Control Server Dell Windows 10 Thin Client HMI Systems</td>
</tr>
<tr>
<td>GEH-6721_Vol_I</td>
<td>Mark VIe and VIeS Control Systems Volume I: System Guide</td>
</tr>
</tbody>
</table>
## Contents

1 **Thin Client HMI System Overview** ................................................................. 7  
   1.1 Introduction ..................................................................................................... 7  
   1.2 HMI Architecture ............................................................................................ 7  

2 **Thin Client Initial Configuration Procedures** .................................................... 11  
   2.1 Disable Write Filter ........................................................................................ 12  
   2.2 Local Administrator Account Login .............................................................. 12  
   2.3 Copy GE Files to Thin Client .......................................................................... 12  
   2.4 Configure Windows Settings .......................................................................... 13  
      2.4.1 Configure Display Settings ..................................................................... 13  
      2.4.2 Configure Desktop Wallpaper ............................................................... 14  
      2.4.3 Configure Audio Settings ..................................................................... 16  
      2.4.4 Configure Power Settings ..................................................................... 16  
      2.4.5 Configure Time Zone .......................................................................... 17  
   2.5 Remove Unused Software .............................................................................. 17  
   2.6 Connect Thin Client to PDH Network .............................................................. 18  
      2.6.1 Configure Private Network ................................................................... 18  
      2.6.2 Rename Network Connection ................................................................ 19  
      2.6.3 Configure Network Adapter ................................................................ 20  
      2.6.4 Configure PDH Network ....................................................................... 21  
   2.7 Join Domain Network and Apply Group Policy .............................................. 22  
   2.8 Create RDP Connection Desktop Shortcuts During Initial Configuration .... 24  
   2.9 Make Configuration Changes Permanent ...................................................... 27  

3 **USB Drive Support** .......................................................................................... 29  
   3.1 Enable File Sharing ....................................................................................... 29  
   3.2 File Share Persistence .................................................................................... 30  
   3.3 File Share Removal ....................................................................................... 30  

4 **Remote Desktop Services Overview** .................................................................. 31  

5 **System Configuration and Maintenance Use Cases** ........................................... 33  
   5.1 Change Local Thin Client Default Account Passwords .................................. 33  
   5.2 Verify Thin Client Time Synchronization to Domain Controllers ............... 33  
   5.3 Verify Domain Controller Time Synchronization .......................................... 34  

6 **Troubleshooting Scenarios** .............................................................................. 35  
   6.1 Thin Client Login Failure .............................................................................. 35  
   6.2 Failure to Establish RDP Connection to Host .............................................. 35  
      6.2.1 Incorrect User Credentials ..................................................................... 36  
      6.2.2 Network Connection Issue or Target Host (VM) is Offline .................. 36  
      6.2.3 Remote Desktop Services Connection Issues ...................................... 37  
   6.3 Remote Desktop Connection Unknown Publisher Warning ....................... 38  
   6.4 Thin Client Terminal Reported as Offline by Control System Health ........ 38  

7 **Common Procedures** ...................................................................................... 39  
   7.1 Thin Client Account Login ............................................................................ 39  
      7.1.1 Local User Account Login ...................................................................... 39  
      7.1.2 Local Administrator Account Login ..................................................... 39
7.2 Change Local Thin Client Account Passwords .......................................................... 40
  7.2.1 Change Thin Client Local User Account Password .............................................. 40
  7.2.2 Change Thin Client Local Administrator Account Password ......................... 41
7.3 Get Thin Client Hardware and Software Information ............................................. 42
  7.3.1 Product Information ......................................................................................... 42
  7.3.2 MAC Addresses ............................................................................................. 42
  7.3.3 Client Information ......................................................................................... 43
7.4 Verify Thin Client Network Connection ................................................................. 44
  7.4.1 Verify Connection Status ............................................................................... 44
  7.4.2 Verify IP Address Assignment from DHCP ..................................................... 45
7.5 Verify Domain Name Server (DNS) Status ............................................................. 46
7.6 Verify DHCP Server Status .................................................................................. 46
7.7 Verify Thin Client Domain Network ...................................................................... 47
7.8 Write Filter ........................................................................................................... 48
  7.8.1 Write Filter Status .......................................................................................... 48
  7.8.2 Enable/Disable Write Filter ............................................................................ 48
7.9 Open Administrator Mode PowerShell Window on Thin Client ............................ 49
7.10 Launch RD Licensing Diagnoser Tool ................................................................. 49
7.11 Check Location and Status of RDS License Server ............................................ 50
7.12 Restart RDS License Server ................................................................................ 53
7.13 Determine Number of Available Client Licenses in RDS License Server .......... 54
7.14 Manage RDS Per Device CALs .......................................................................... 54
  7.14.1 Launch RD Licensing Manager ...................................................................... 54
  7.14.2 Determine Number of Available (Unused) RDS Per Device CALs ................. 54
  7.14.3 Revoke Unused Device CAL .......................................................................... 55
7.15 Manage User Sessions on HMI VMs ................................................................... 56
  7.15.1 View Active andDisconnected User Sessions ............................................... 56
  7.15.2 CloseDisconnected User Sessions .................................................................. 56
7.16 Create Thin Client Configuration USB Drive ....................................................... 57
7.17 Modify Thin Client Host Name ............................................................................ 61
7.18 Create RDP Connection Desktop Shortcuts ......................................................... 64

Glossary of Terms ...................................................................................................... 67

GEH-6864 Support and Maintenance Guide 5
1 Thin Client HMI System Overview

1.1 Introduction

Control Server is a virtualized platform that can be used to integrate the traditional features provided by Workstations, Historians, and Communication Gateways. The Human-machine Interface (HMI) architecture involves a client-server system, using Thin Client terminals, that view virtual HMIs through a centralized Control Server. This system also provides an integrated, supervisory control platform, which allows control applications to be developed and deployed in an integrated, tiered control architecture.

The intended audience of this document is the site maintenance engineer responsible for ensuring proper system operation. The document scope is limited to Thin Client terminals and the Thin Client support infrastructure. Procedures such as the following examples are provided in this document:

- How to diagnose and fix issues that may occur as the result of component failures over time
- How to make small system configuration changes to support changes in the plant over time

1.2 HMI Architecture

Traditional control system architecture uses stand-alone HMI desktop computers (thick clients) to provide physical interface to the system. Control system software processes are distributed across the HMI computers on the plant network (PDH).

The Control Server approach uses HMI Virtual Machines (VMs) running on a server and Thin Client terminals in place of stand-alone HMIs (thick clients).
The following figure displays a Control Server architecture that uses a dedicated Thin Client terminal for each HMI VM. In this example, Thin Client 1 is dedicated to hosting connections to HMI1 VM, while Thin Client 2 is dedicated to HMI2 VM, and so forth.
Another architecture choice is the many-to-one architecture, multiple Thin Clients connect to a single HMI VM as shown in the following figure. Each Thin Client establishes a user session over an Remote Desktop Protocol (RDP) connection to the HMI VM, resulting in concurrent user sessions on the VMs. Typical systems will have more than one HMI VM.
2 Thin Client Initial Configuration Procedures

This chapter provides the standard procedures required to configure the Thin Client for the first time. A high-level overview of the steps to configure a Thin Client for the first time are as follows:

2. Remove unused software.
3. Connect the Thin Client to the PDH network.
4. Join the Domain Network and apply group policy.
5. Create RDP connection desktop shortcuts.

Most of the Thin Client configuration procedures are common to all Thin Client terminals at a site. The final step, creating the RDP connection desktop links, is where the Thin Client terminal is uniquely configured for a specific location at the site and is only performed when deploying the Thin Client terminal. Spare terminals should be configured (minus the RDP connections) before they are placed in storage so that, in the event of a terminal failure, the spare can replace the failed unit without having to go through the configuration process in a potentially time-critical situation. Spare units can be temporarily connected to the network, configured, and returned to storage until they are needed.

---

**Attention**

It is critical to perform all procedures outlined in the following sections of this document. All steps within each section must be performed exactly as documented and in the order provided. The overall procedure is divided into three parts to make the process more understandable, but the sections are interdependent and must be performed from start to finish as a coherent set in the following order:

1.) Configure Windows Settings.
2.) Remove Unused Software.
3.) Connect the Thin Client to the PDH network.
4.) Join the Domain Network and apply group policy.

---

**Attention**

The procedures in this chapter require local Administrator account privileges, and the Write Filter must be disabled in order to make the changes permanent.
2.1 Disable Write Filter

Disable the Write Filter.

➢ To disable the Write filter: perform the procedure To disable the Write Filter. The Thin Client will restart and automatically log in to the local User account.

2.2 Local Administrator Account Login

1. Press [CTRL] [ALT] [DEL] and sign out of the User account.
2. Click on the desktop to display the User login window.
3. Select the Admin user (in the lower left-hand corner) and log in as the local Administrator.

Note The default local Administrator password is DellCCCvdi.

2.3 Copy GE Files to Thin Client

When this step is performed, the files that are needed during the configuration process are copied from a USB drive to the Thin Client terminal. Refer to the section Create Thin Client Configuration USB Drive for the procedure to copy the required files from the server to the USB drive.

➢ To copy GE files to the Thin Client
1. Insert the Thin Client configuration USB drive into the Thin Client.
2. Open File Explorer on the Thin Client and navigate to the USB drive.
3. Copy the GE directory on the USB drive to the C: directory on the Thin Client.
4. Eject the USB drive and remove it from the Thin Client.
2.4 Configure Windows Settings

Perform the procedures in this section to configure the Windows settings.

2.4.1 Configure Display Settings

In some cases, the display settings need to be changed to match the number of connected monitors or other display considerations.

➢ To modify the display settings: from the Control Panel, select Display, then select Change Display Settings and modify the display settings as needed.
2.4.2 Configure Desktop Wallpaper

Set the desktop wallpaper to display the GE logo.

➢➢ To modify the desktop wallpaper

1. Open a Run command and enter `gpedit.msc`, then click OK.

2. In the Local Group Policy Editor Tree View, expand **Local Computer Policy**, **User Configuration**, **Administrative Templates**, **Desktop**, **Desktop**, and double-click **Desktop Wallpaper**.

3. Configure the Desktop Wallpaper settings as follows:
   a. From the Desktop Wallpaper dialog box, select **Enabled**.
   b. In the Wallpaper Name field, enter `C:\GE\GEDesktop.jpg`.
   c. In the Wallpaper Style field, select **Fill**.
d. Click **OK** to save the changes and close the window.

4. Click the **X** to close the Local Group Policy Editor.
2.4.3 Configure Audio Settings

➢ To modify sound settings: from the Control Panel, select Hardware and Sound, select Sound, then modify the Sound properties as needed.

2.4.4 Configure Power Settings

Configure the High performance plan power settings to never turn off the display and never go to sleep.

➢ To modify the High performance plan power settings

1. From the Control Panel, select Power Options.
2. Select (enable) the High performance plan (expand Show additional plans to display it), then select Change Plan settings.
3. Set the options for Turn off the display to Never.
4. Set the options for Put the computer to sleep to Never.
5. Click Save changes.
2.4.5 Configure Time Zone

Configure the time zone to match the site’s time zone.

➢➢ To modify the time zone

1. From the Control Panel, select Date and Time.

2. Click Change time zone... and select the time zone that matches the site’s time zone.

3. Click OK to save the changes.

4. Click OK to close the window.

![Time Zone Configuration](image)

2.5 Remove Unused Software

Refer to How to Remove Unused Software from Control Server Dell Windows 10 Thin Client HMI Systems (GHT–200059) for the instructions to remove unused software.
2.6 Connect Thin Client to PDH Network

➢ To connect the Thin Client to the PDH network and configure the connection: connect the client Ethernet port to the PDH network.

2.6.1 Configure Private Network

➢ To configure a private network

1. Click on the Ethernet icon in the system tray of the task bar and select Network Settings.

2. From the Settings dialog box, click the Ethernet connection (HMI.local).

3. Set the Make this PC discoverable option to On to enable the Private network mode.
4. Verify that the network displays the **Private network** mode for the connection.

2.6.2 **Rename Network Connection**

➢ To rename the network connection

1. From the **Control Panel**, select **Network and Sharing Center**, then select **Change adapter settings**.

2. Right-click the connection name (Ethernet), select **Rename**, and enter **PDH**.

---

Example Network Connection Before Rename

Example Network Connection After Rename
2.6.3 Configure Network Adapter

Configure the Network Adapter settings to enable DHCP.

➢ To modify the IP address

1. From the Control Panel, select Network and Sharing Center.
2. Select the PDH network adapter to display the PDH Status dialog box.
3. Click Properties to display the PDH Properties dialog box.
5. From the General tab, click to select (enable) Obtain an IP address automatically.
6. Click OK to save the changes.
7. Click Close to close the windows.
2.6.4 Configure PDH Network

➢ To configure the PDH network

1. From the Control Panel, select Network and Sharing Center.
2. Double-click the PDH network connection, then click Properties to display the PDH Properties dialog box.
3. Deselect (uncheck) the following properties:
   • Microsoft Network Adapter Multiplexor Protocol
   • Microsoft LLDP Protocol Driver
   • Internet Protocol Version 6 (TCP/IPv6)
   • Link-Layer Topology Discovery Responder
   • Link-Layer Topology Discovery Mapper I/O Driver
4. Select (check) the following properties:
   • Client for Microsoft Networks
   • File and Printer Sharing for Microsoft Networks
   • QoS Packet Scheduler
   • Internet Protocol Version 4 (TCP/IPv4)
5. Click **OK** to save the changes and close the *PDH Properties* dialog box.
6. Click **Close** to close the *PDH Status* dialog box.
7. From the **Network and Sharing Center**, click **Change adapter settings**.
8. Right-click on the PDH Network and select **Disable**.
9. Right-click on the PDH Network and select **Enable**.
10. Close the open windows.
11. Verify that the PDH Network connection is active. For instructions, refer to the section *Verify Thin Client Network Connection*.

### 2.7 Join Domain Network and Apply Group Policy

Add the Thin Client terminal to the domain network for security hardening. Use the *Join-Domain.ps1* PowerShell script in the *C:\GE* folder to perform this procedure.

➢➢ **To join the domain network and apply group policy**

1. Open Windows PowerShell in Administrator mode. For instructions, refer to the section *Open Administrator Mode PowerShell Window on Thin Client*.
2. Issue the **Set-ExecutionPolicy Unrestricted -Scope Process -Force** command from the PowerShell prompt as shown in the following figure.

![Set-ExecutionPolicy Unrestricted -Scope Process -Force Command](image)

3. Issue the **cd c:\GE** command from the PowerShell prompt.
4. Enter **Join** and press the [tab] key to create the command to run the *Join-Domain.ps1* script, followed by the [Enter] key to perform the command.
5. When prompted, enter the password for a Domain Administrator account.
The Thin Client will restart and automatically log in to the local User account.

6. Log in to the Thin Client using the local Administrator account. For instructions, refer to the section *Local Administrator Account Login*.

7. Open Windows PowerShell in Administrator mode.

8. Issue the `gpupdate /force` command from the PowerShell prompt as shown in the following figure. Expect a delay of at least 60 seconds for the command to complete.
2.8 Create RDP Connection Desktop Shortcuts During Initial Configuration

The desktop RDP Connection shortcuts can be created as part of the initial Thin Client configuration, or at any other time (refer to the procedure in the section Create RDP Connection Desktop Shortcuts).

➢➢ To create RDP connection desktop shortcuts during initial Thin Client configuration

1. Open the Remote Desktop Connection window and expand **Show Options**.

2. In the **Computer** field, enter the target computer host name or IP address.

3. (Optional) In the **User name** field, enter a user name.
4. From the **Display** tab, select (check) **Use all my monitors for the remote session**.

5. (Optional) Modify the settings on the other tabs as needed.

6. From the **General** tab, select **Save As…**, modify the name, and save to the `C:\Users\User\Desktop` folder.
7. If prompted, click **Continue** to access to the C:\Users\User directory.
8. Repeat this procedure for each RDP connection.
9. Verify that the RDP connection shortcuts are available on the User desktop.

![Example RDP Desktop Connection Shortcut]

### 2.9 Make Configuration Changes Permanent

After the Thin Client configuration is complete, enable the Write Filter to save the configuration changes. This also prevents future configuration changes.

➢ To enable the Write Filter: refer to the procedure [To enable the Write Filter](#).

The Thin Client will restart and automatically log in to the local User account.
3  **USB Drive Support**

USB drives that are plugged into the Thin Client can be shared for access by the VMs in the Control Server. The Windows operating system automatically detects and mounts USB drives plugged into the USB port. A local Thin Client Administrator can set up shared file access to the contents of the USB drive.

### 3.1 Enable File Sharing

➢ **To enable the USB device for shared file access**

1. Log in to the local Administrator account. Refer to the section *Local Administrator Account Login*.
2. Plug in the USB device.
3. Open File Explorer, select the drive, and create a share to enable access to the device from other VM’s.
4. Verify the permissions on the share have *Everyone* with Read permission (the default). If the USB contents require updating, add Administrators with Change permission (requires Domain Administrator credentials).

The contents of the USB device can now be accessed by any VM in the Control Server using Windows standard shared file access with the appropriate credentials.

➢ **To access the USB contents:** right-click on the shared drive and select the **Sharing** tab to find the Network Path to the shared drive.
Note  Thin Client local Administrator account credentials are required when accessing the shared directory from a VM or another Thin Client.

### 3.2 File Share Persistence

The following summarizes USB drive file share persistence.

The file share:

- will persist if the USB drive is removed and reinserted later.
- will persist between user logins.
- will not persist between reboots. The share will be removed and the device will not be accessible to other VM’s in the system.

Note Although it is not recommended, the file share can be made to persist across reboots by disabling the Write Filter, creating the share, then enabling the Write Filter.

### 3.3 File Share Removal

Leaving the USB device shared is a security risk. Perform one of the following to remove the file share when finished:

- Remove the file share, then remove the USB device.
- Remove the USB device and reboot the Thin Client.

Note If the file share was created to persist across reboots, disable the Write Filter, remove the file share, then enable the Write Filter.
4 Remote Desktop Services Overview

Systems can be set up for one Thin Client terminal to one HMI VM operation (one-to-one), or many Thin Client terminals to one HMI VM operation (many-to-one). Windows Thin Client terminals connect to the VMs using Remote Desktop sessions. For the many-to-one case, Remote Desktop Services (RDS) is enabled on the HMI VMs, and a Remote Desktop Services License Server is configured on the Engineering Workstation (EWS) VM. The HMI VMs are configured as Remote Desktop Session Host Servers using the Per Device licensing mode. The Thin Client terminals are issued RDS Per Device Client Access Licenses (CALs) by the Remote Desktop License Server. When a Thin Client terminal connects to an RD Session Host server (HMI VM) for the first time, the client is issued a temporary license. When a client connects to an RD Session Host server (HMI VM) for the second time, the license server issues it a permanent RDS Per Device CAL, providing there are CALs in the pool of available RDS Per Device CALs on the license server.

Note The use of RDP connections between VMs should be limited, as this may prematurely deplete the pool of available RDS Per Device CALs on the license server and lead to RDP connection issues. Per Device CALs are purchased based only on the number of Thin Client terminals. VM to VM RDP connections are also allocated licenses from this pool and should therefore only be initiated from a single VM in the system, and it is recommended that only the EWS VM be used for this purpose.

User Sessions

The HMI VMs run within the Windows Server operating system. Windows Server supports up to two concurrent user sessions by default, and supports an unlimited number of user sessions when RDS is enabled. Typically, whenever a Remote Desktop connection is established with the VM, a new user session is created based on the user credentials provided when the connection is established. In this case, the user session is in the Connected state because it is associated with an active Remote Desktop connection. If the user logs out of the connection, the user session is terminated and the Remote Desktop connection is closed. However, if the user simply closes the Remote Desktop connection without logging out, the user session remains active on the server in a Disconnected state. The user can establish a new Remote Desktop connection and resume the Disconnected session by logging in with the same user credentials.

Windows Task Manager can be used to display the user sessions, as shown in the following figure. Windows Task Manager can also be used to close Disconnected sessions. Refer to the section Manage User Sessions on HMI VMs for detailed procedures.
5 System Configuration and Maintenance Use Cases

This chapter describes scenarios related to both initial site installation and long-term maintenance of the site that a plant maintenance engineer is likely to encounter.

5.1 Change Local Thin Client Default Account Passwords

Thin Clients are shipped from the factory with local Administrator and local User accounts. The default password is the same for both accounts; the local Administrator password is DellCCCvdi and the local User password is DellCCCvdi. These widely-shared default passwords should be changed on all of the Thin Clients at the site as part of the hand-over procedure to prevent unauthorized users from logging in to the Thin Client terminals. Refer to the section Change Thin Client Local User Account Password for the procedure to modify the default account passwords.

5.2 Verify Thin Client Time Synchronization to Domain Controllers

Because the Thin Clients are members of the Domain, they will only use the system Domain Controllers to synchronize their time. This requires the Domain Controllers to be configured to synchronize to the site time sources to provide a consistent time reference between the Thin Clients (which use the Domain Controller time) and the HMIs (which use the site time sources as the time reference). Perform the following procedure to verify the successful synchronization of the Thin Client to the Domain Controllers.

➢ To verify the successful synchronization of the Thin Client to the Domain Controllers
1. Log in to the local Administrator account. Refer to the section Local Administrator Account Login.
2. Open a Windows Command window.
3. Issue the command w32tm /query /status. The command output (illustrated in the following figure) shows that the Thin Client is successfully synchronized to DC2. Thin Client synchronization to either DC1 or DC2 is expected.
5.3 Verify Domain Controller Time Synchronization

Refer to the Control Server — Domain Services Maintenance Guide (GEH-6845), the section Configure Time on Domain Controllers, for the procedures to verify the Domain Controller time synchronization configuration and status, as well as to modify the Domain Controller time settings, if required.
6 Troubleshooting Scenarios

This chapter describes potential failure modes and provides procedures to determine root cause and issue resolution.

6.1 Thin Client Login Failure

The local User account should be used for normal operation, and the Thin Client will automatically log in to this account. The local Administrator account should be used only for configuration and troubleshooting activities.

Failure to log in to an account is the result of entering an incorrect user name or password.

Incorrect User Name or Password Message

6.2 Failure to Establish RDP Connection to Host

Thin Clients typically communicate with VMs running on the Control Server, as well as servers on other systems. After successful login to the Thin Client, a connection to a host is initiated. The connections can be launched automatically, or they can be manually initiated by the user, depending on how they are set up in the configuration file.

Failure to establish a connection to a host can be caused by many issues, such as:

- Incorrect user credentials
- Loss of network connection
- Target Host (VM) is offline
6.2.1 Incorrect User Credentials

If login to the host fails, the following dialog box displays. Verify that the username, domain, and password information are correct.

![Logon Attempt Failed Dialog Box]

6.2.2 Network Connection Issue or Target Host (VM) is Offline

If the Thin Client network connection has been lost (refer to the section Verify Thin Client Network Connection), or the target VM is offline, the Remote Desktop Connection displays the following error dialog box. Follow the instructions provided in the Remote Desktop Connection Error Message.

![Remote Desktop Connection Error Message]
6.2.3 Remote Desktop Services Connection Issues

Remote Desktop Services (RDS) connection-related errors, like the following example, may occur on systems configured for many Thin Client terminals to one HMI VM operation (many-to-one).

RDS connection issues can be caused by Remote Desktop License Server issues or an insufficient number of RDS Per Device CALs. Use the following procedures to resolve License Server or available license pool issues.

➢ To resolve License Server or available license pool issues

1. Verify the operation of the RDS License Server and restart it if necessary. Refer to the section Check Location and Status of RDS License Server.

2. Determine the number of client licenses available on the RDS License Server. Refer to the section Determine Number of Available Client Licenses in RDS License Server.

3. Free up unused client licenses and/or purchase additional RDS Per Device CALs if the number of RDS Per Device CALs is not sufficient to cover the number of device connections required by the site. Refer to the section Manage RDS Per Device CALs.
6.3 **Remote Desktop Connection Unknown Publisher Warning**

The Remote Desktop Connection Unknown Publisher warning message is typically displayed when a Remote Desktop connection is launched using a desktop icon. The *Unknown Publisher* message indicates that the desktop RDP file has not been signed. This is not an indication of an authentication failure between the Thin Client and the Remote Host.

➢➢ To proceed with the connection process from the *Remote Desktop Connection Unknown Publisher* dialog box: click **Connect**.

![Remote Desktop Connection Unknown Publisher Warning](image)

6.4 **Thin Client Terminal Reported as Offline by Control System Health**

An incorrectly configured Thin Client host name can result in the Control System Health (CSH) feature reporting that the Thin Client terminal is offline even though it is communicating on the network. The CSH feature in WorkstationST releases prior to V07.04.02C (included in ControlST versions prior to V07.04.00C SP01) require the use of a standard host name in order to communicate with the Thin Clients.

The standard name provides a mechanism for CSH to manufacture a host name for the client to compensate for the fact that the Thin Clients IP addresses are dynamically assigned via DHCP. This standard host name is also required by legacy configuration software used with older Thin Client models, which were factory shipped with the default host name already configured.

Thin Clients deployed in a system with CSH prior to WorkstationST V07.04.02C must be configured with the standard Thin Client name in order to be monitored by the CSH feature. The Windows 10 Thin Client host name must start with WIE, followed by the MAC address of the Thin Client as reported on the Thin Client MAC sticker. (Refer to the section on *Get Thin Client Hardware and Software Information*). For example, a Windows 10 Thin Client with MAC address 588A5A47EF3 must be configured with a host name of WIE588A5A47EF3A. Refer to the section *Modify Thin Client Host Name* for the procedure to configure the host name to the required value.
7 Common Procedures

This chapter contains common procedures used for Thin Client maintenance and debugging.

7.1 Thin Client Account Login

There are two login account types: local User account and local Administrator account.

7.1.1 Local User Account Login

Thin Clients are configured to automatically log in to the local User account. Auto login does not require the user to enter the local User account password.

Note The factory default local User password is DellCCCvdi.

7.1.2 Local Administrator Account Login

Changes to the Thin Client can only be made using the local Administrator account.

➢ To log in to the local Administrator account

1. Press [CTRL] [ALT] [DEL] and select Sign out to log out of the current account.

Note Thin Clients are configured to automatically log in to the local User account so log off this account to log in to the local Administrator account.

2. Click the desktop or press any key.

3. Select the Other User account on the lower-left corner of the desktop.

4. Enter the user name as \Admin.

5. Enter the local Administrator account password and press [Enter].

Note The factory default local Administrator password is DellCCCvdi.
7.2 Change Local Thin Client Account Passwords

Thin Clients come from the factory with well-known default local User and Administrator account passwords. The default password for both accounts is DellCCVdi. For security, the default passwords should be changed to reduce the risk of unauthorized users gaining access to the Thin Client terminals at the site.

7.2.1 Change Thin Client Local User Account Password

Perform the following procedures to change the local User account password and update the auto logon password setting with the newly created password.

➢➢ To change the local User account password
1. Log in to the local Administrator account. Refer to the section Local Administrator Account Login.
2. Disable the Write Filter. Refer to the procedure To disable the Write Filter.
   The Thin Client will restart and automatically log in to the local User account.
3. Log in to the local Administrator account.
4. From the Control Panel, select User Accounts, then select Manage User Accounts.
5. In the User Accounts dialog box, select User, then click Reset Password.
6. In the Reset Password dialog box, enter the new password and confirm the new password, then click OK.
7. In the User Accounts dialog box, click OK.
8. Click the X to close the User Accounts window.

➢➢ To update auto logon password setting
1. Launch the Dell Thin Client Application and select Auto Logon.
2. Verify that Enable Auto Logon is selected (checked).
3. In the Default Password field, enter the new User account password and click Apply.

5. Enable the Write Filter. Refer to the procedure To enable the Write Filter. The Thin Client will restart and automatically log in to the local User account.

6. Verify that the local User auto logon is successful.

### 7.2.2 Change Thin Client Local Administrator Account Password

Perform the following procedure to change the local Administrator account password.

➢ To change the Thin Client local Administrator account password

1. Log in to the local Administrator account. Refer to the section Local Administrator Account Login.

2. Disable the Write Filter. Refer to the procedure To disable the Write Filter. The Thin Client will restart and automatically log in to the local User account.

3. Log in to the local Administrator account.

4. Press [CTRL] [ALT] [DEL] and select Change a password.

5. Enter the user name as \Admin.

6. Enter the old and new passwords and confirm the new password.

7. Press [Enter] to make the change and select OK to confirm.

8. Enable the Write Filter. Refer to the procedure To enable the Write Filter. The Thin Client will restart and automatically log in to the local User account.

9. Verify the new password by logging in to the local Administrator account using the new password.
7.3 Get Thin Client Hardware and Software Information

The first level of Thin Client information is found in multiple locations on the chassis.

7.3.1 Product Information

The pull-out Product Information tag on the back of the chassis shows the model number and compliance certifications.

![Product Information Tag]

7.3.2 MAC Addresses

The small MAC stickers on the side of the Thin Client face show the MAC addresses (physical address of the internal NICs) for the Thin Client. The Thin Client can be uniquely identified and tracked using the MAC addresses.

![MAC Address Stickers]
7.3.3 **Client Information**

The next level of information requires logging into the Thin Client to get further information about the hardware and operating system.

➢ To **view client information**: open the Dell Thin Client Application.

![Client Information Viewer](image-url)
7.4 Verify Thin Client Network Connection

7.4.1 Verify Connection Status

Most Thin Client functionality depends on its connection to the Plant Network (PDH). The Thin Client displays the icon shown in the following figure in the status tray when it is connected to the PDH network. The *No Internet access* warning is typical.

![Connected Network Connection Icon](image1)

The Thin Client displays the icon shown in the following figure in the status tray when the network connection is lost. The network connection icon in the system tray is displayed with a red X when the network is disconnected. Hovering over the icon with the mouse generates the tooltip. If the icon is displayed, the Thin Client has lost its connection to the PDH. Verify that the network cable is plugged in to the Thin Client. If the network cable is connected and the problem persists, the problem could be a Thin Client or network issue.

![Not Connected Network Connection Icon](image2)
7.4.2 Verify IP Address Assignment from DHCP

Using the Dell Thin Client Application, verify the network connection status and the IP address assignment from DHCP.

➢ To verify the IP address assignment from DHCP

1. Open the Dell Thin Client Application and click Client Information.
2. Scroll down to Network.
3. Verify that an IP address has been assigned as displayed in the following figure.


### 7.5 Verify Domain Name Server (DNS) Status

- **To verify DNS status**
  1. Log in to the DC1 VM.
  2. From the **Control Panel**, select **Administrative Tasks**, then select **Services**.
  3. Verify that the Active Directory Domain Service is running.

![Active Directory Domain Service](image)

### 7.6 Verify DHCP Server Status

The system uses redundant DHCP Servers, hosted on the DC1 and DC2 VMs, to provide DHCP services to the Thin Clients. The Thin Clients rely on DHCP to get their IP addresses. If the Thin Client cannot access the DHCP Servers, the Thin Client will be unable to communicate on the network.

- **To verify DHCP Server status**
  1. Establish a remote session with the DHCP Server VM.
  2. Verify that the DHCP Server service is running.
  3. Repeat for both the DC1 and DC2 VMs.

![DHCP Server Service](image)
7.7 **Verify Thin Client Domain Network**

View the computer System Information to locate the Thin Client domain network membership.

**Note**  This procedure can be performed with the terminal disconnected from the network.

➢ **To verify the Thin Client domain network**

1. From the **Control Panel**, select **System**.
2. Verify that the Domain is **not** set to WORKGROUP.

The following figure shows that the terminal has been joined to the Control Server HMI.local domain.

![Thin Client Joined to Control Server HMI.local Domain](image)
7.8 Write Filter

When enabled on Windows 10 Thin Clients, the Write Filter prevents changes from being made to the Thin Client. Any changes made while the Write Filter is enabled are lost when the Thin Client is restarted. Changes are only persisted when the Write Filter is disabled.

7.8.1 Write Filter Status

The Write Filter status is displayed in the system tray. A green circle icon indicates that the Write Filter is enabled (ON), and a red circle icon indicates that the Write Filter is disabled (OFF).

![Write Filter Disabled Icon](image1)
![Write Filter Enabled Icon](image2)

7.8.2 Enable/Disable Write Filter

➢➢ To enable the Write Filter

1. Log in to the local Administrator account. Refer to the section [Local Administrator Account Login](#).
2. Right-click the Dell Wyse WF Enable desktop icon and select Run as administrator.

![Enable Write Filter Desktop Icon](image3)

The Thin Client will restart, and the Write Filter will be enabled after the reboot completes.

➢➢ To disable the Write Filter

1. Log in to the local Administrator account. Refer to the section [Local Administrator Account Login](#).
2. Right-click the Dell Wyse WF Disable desktop icon and select Run as administrator.

![Disable Write Filter Desktop Icon](image4)

The Thin Client will restart, and the Write Filter will be disabled after the reboot completes.

3. In the Unified Write Filter dialog box, click **OK** to acknowledge the Write Filter disabled warning.
7.9 Open Administrator Mode PowerShell Window on Thin Client

Perform the following procedure to open a PowerShell window in Administrator mode on a Thin Client.

➢➢ To open an Administrator mode PowerShell window

1. Log in to the local Administrator account. Refer to the section Local Administrator Account Login.
2. From the Start menu Search area, type PowerShell.
3. Right-click on Windows PowerShell and select Run as administrator.

**Note** You must be logged in to an Administrator account on the Thin Client to run PowerShell.

7.10 Launch RD Licensing Diagnoser Tool

The RD Licensing Diagnoser tool provides information to help identify possible licensing problems for the Remote Desktop Session Host server.

➢➢ To launch the RD Licensing Diagnoser tool

1. Establish a Remote Desktop connection to one of the HMI VMs. If RDS License Server issues are preventing Remote Desktop connections, connect to one of the HMI VMs using a Remote Console launched from VMware vSphere Client or vSphere web client.
2. Log in to a Domain Administrator account.
3. Launch the Windows Server Manager tool.
4. From the Tools menu, select Terminal Services.

**Note** If Terminal Services does not display in the Tools menu, RDS is not enabled on the VM, and is a likely indication that the site is using a one Thin Client to one HMI VM (one-to-one) architecture and RDS licensing does not apply.

5. Select RD Licensing Diagnoser.
### 7.11 Check Location and Status of RDS License Server

The RD Licensing Diagnoser tool can be used to display information about the Remote Desktop Session Host Server on the local VM, as well as the location and status of the RDS License Server. (Refer to the procedure [To launch the RD Licensing Diagnoser Tool](#) to launch the application.)

In the example in the following figure, no problems were detected and the location and status of the RDS License Server is displayed.
Select the license server entry to view further details.

<table>
<thead>
<tr>
<th>Name</th>
<th>Credentials</th>
<th>Connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ts-ews.hml.local</td>
<td>Available</td>
<td>Available</td>
</tr>
</tbody>
</table>

**License Server Configuration Details**

- Version: Windows Server 2012 R2
- Remote Desktop Session Host server in RDS Endpoint Servers group: Yes
- “Prevent license upgrade” Group Policy setting: Not enabled
- “Licensing server security group” Group Policy setting: Enabled
- Per User tracking and reporting: Available

The license server has the following licenses installed and available:

<table>
<thead>
<tr>
<th>License Type</th>
<th>License Version</th>
<th>Installed</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDS Per Device CAL</td>
<td>Windows Server 2012</td>
<td>250</td>
<td>241</td>
</tr>
</tbody>
</table>
If a problem is detected, the RD Licensing Diagnoser tool provides a description of the problem and instructions to resolve the problem. The following figure illustrates the RD Licensing Diagnoser tool display after the Remote Desktop Licensing service was stopped. Perform the steps in the *Suggested Resolution* area to resolve any existing issues.
7.12 Restart RDS License Server

➢ To restart the RDS License service on the VM hosting the RDS License Server information

1. Establish a Remote Desktop connection to the VM hosting the RDS License Server.
   a. If RDS License Server issues are preventing Remote Desktop Connections, connect to one of the HMI VMs using a Remote Console launched from VMware vSphere Client or vSphere web client.
   b. If the location of the RDS License Server is not known, refer to section Check Location and Status of RDS License Server to determine which VM is hosting the license server.

2. Log in to the VM hosting the RDS License Server with a Domain Administrator account.

3. From the Windows Control Panel, select Administrative Tools, then select Services.

4. Locate the Remote Desktop Licensing service.

   Note If the service cannot be found, the RDS License Server is not installed on this VM.

5. Right-click Remote Desktop Licensing service and select Start (if it is not running).

6. Verify that it successfully starts up.

7. Verify that the service Startup Type is configured as Automatic. If not, right-click, and select Properties and change Startup Type to Automatic.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Status</th>
<th>Startup Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Desktop Licensing</td>
<td>Provides registered licenses for Remote Desktop Services clients. If this service is stopped, the service is unable to issue licenses.</td>
<td>Running</td>
<td>Automatic</td>
</tr>
<tr>
<td>Remote Desktop Services UsersIp</td>
<td>Allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop Users are configured to connect to the same IP address.</td>
<td>Running</td>
<td>Manual</td>
</tr>
<tr>
<td>Remote Desktop Services UseSocks</td>
<td>Remote Desktop Services UseSocks is a component of Remote Desktop Services. It is used to connect to a remote computer.</td>
<td>Running</td>
<td>Manual</td>
</tr>
<tr>
<td>Remote Procedure Call (RPC)</td>
<td>The RPCSS service is the Service Control Manager for COM and DCOM services. It performs object activation requests.</td>
<td>Running</td>
<td>Automatic</td>
</tr>
<tr>
<td>Remote Procedure Call (RPC) Loc</td>
<td>In Windows 2003 and earlier versions of Windows, the Remote Procedure Call (RPC) Locator service is used to locate and connect to remote procedure calls (RPCs).</td>
<td>Running</td>
<td>Manual</td>
</tr>
<tr>
<td>Remote Registry</td>
<td>Enables remote users to modify registry settings on this computer. If this service is stopped, the registry is locked.</td>
<td>Running</td>
<td>Automatic</td>
</tr>
<tr>
<td>Resultant Set of Policy Provider</td>
<td>Provides a network service that processes requests to simulate application of Group Policy settings for computers. This service is needed for computers on networks with Active Directory Domain Services (AD DS) domains.</td>
<td>Running</td>
<td>Disabled</td>
</tr>
<tr>
<td>Routing and Remote Access</td>
<td>Offers routing services to businesses in local area and wide area network environments.</td>
<td>Running</td>
<td>Manual</td>
</tr>
<tr>
<td>RPC Endpoint Mapper</td>
<td>Resolves RPC interfaces to transport endpoints. If this service is stopped or disabled, programs that use RPC may fail.</td>
<td>Running</td>
<td>Automatic</td>
</tr>
<tr>
<td>SDII Server</td>
<td>GE Signal Data Base (SDII) Server for sharing signals between controllers</td>
<td>Running</td>
<td>Automatic</td>
</tr>
</tbody>
</table>
7.13 **Determine Number of Available Client Licenses in RDS License Server**

Refer to the section *Check the Location and Status of the RDS License Server* for the procedure to launch the RD Licensing Diagnoser tool and display the license server status, including the number of installed and available RDS Per Device CAL licenses.

7.14 **Manage RDS Per Device CALs**

7.14.1 **Launch RD Licensing Manager**

➢➢ **To launch the RD Licensing Manager**

1. Establish a Remote Desktop connection to the VM hosting the RDS License Server. If the location of the RDS License Server is not known, refer to section *Check the Location and Status of the RDS License Server* to determine which VM is hosting the license server.

2. Log in to the VM hosting the RDS License Server with a Domain Administrator account.

3. Launch the Windows Server Manager tool.

4. From the **Tools** menu, select **Terminal Services**.

   **Note**  If **Terminal Services** does not display in the **Tools** menu, Remote Desktop Services are not enabled on the VM, and is a likely indication that the site is using a one Thin Client to one HMI VM (one-to-one) architecture and RDS licensing does not apply.

5. Select **Remote Desktop Licensing Manager**.

7.14.2 **Determine Number of Available (Unused) RDS Per Device CALs**

➢➢ **To determine the number of available RDS Per Device CALs**

1. Launch RD Licensing Manager.

2. Select the server node from the tree view to display the overview of the installed and temporary RDS Per Device CALs.
7.14.3 **Revoke Unused Device CAL**

➢ To revoke an unused Device CAL

1. Launch RD Licensing Manager.
2. Expand the server node and select the **Installed** node to display the details for each installed RDS Per Device CAL and to which device it is allocated.

If a device is no longer available (for example, a Thin Client terminal has failed and has been replaced by a new terminal), the RDS Per Device CAL allocated to it can be revoked. Revoking a license returns it to the available license pool, making it available to be reassigned to a new device.

**Note** Additional RDS Per Device CAL licenses can be purchased and added to the available license pool if required by the site.
7.15  **Manage User Sessions on HMI VMs**

This section provides the following procedures:

- View Active and Disconnected User Sessions
- Close Disconnected User Sessions

### 7.15.1 View Active and Disconnected User Sessions

➢ To view Active and Disconnected user sessions on an HMI VM

1. Establish a Remote Desktop connection to the HMI VM.
2. Log in to the HMI VM with an Administrator account.
3. Launch the Windows Task Manager.
4. Select the **Users** tab to display the active user sessions on the VM.
   
   The following figure shows that the *admin* user session is connected to a Remote Desktop (or another type) connection, and the *TSUser4* user session is active but is running in Disconnected mode.

![Task Manager](image)

### 7.15.2 Close Disconnected User Sessions

➢ To close Disconnected user sessions: right-click a Disconnected user session and select **Sign off** to terminate it.

![Task Manager](image)
7.16 Create Thin Client Configuration USB Drive

Thin Client configuration requires copying files to the Thin Client terminal from a USB drive. The required files are typically archived on one of the VMs (typically the EWS VM) on the Control Server, which allows a configuration USB drive to be created as needed. Perform the following procedure to copy the files from the VM to a USB drive. The configuration files are generic, so one USB drive can be used to configure all of the Thin Clients at a site.

Note Configuration files are archived on the server. As a result, a configuration USB drive can be created at any time, and multiple drives can be created for parallel configuration efforts. Keeping at least one configuration USB drive on hand is recommended for convenience, but this procedure allows the creation of a new one if an existing one cannot be found.

➢➢

To create a Thin Client configuration USB drive

1. Insert the USB drive into a USB port on the HS1 or HS2 node of the Control Server.
2. From the vSphere Web Client, select the VM hosting the Thin Client configuration files (typically EWS).
3. From the Manage tab, click Edit....
4. From the **New device** drop-down list, select **Host USB Device**.
5. Click **Add** and confirm that the USB drive is identified.

6. Click **OK** to enable access to the USB drive.

7. Connect to the VM using RDP or by opening a console from the vSphere Web Client.

8. Open File Explorer and verify that the USB drive is visible.

9. Create a folder named **GE** at the top level of the USB drive.

10. Copy the `c:\inetpub\WES-Procedures\Join-Domain.ps1` file to the GE directory at the top level of the USB drive.

11. Copy the `C:\inetpub\wwwroot\wyse\wlx\bitmap\GEDesktop.jpg` file to the GE directory at the top level of the USB drive.

12. Close File Explorer and eject the USB drive from the VM system tray.

13. Select the EWS VM in the vSphere Web Client.
14. From the **Manage** tab, click **Edit**.

15. Hover over the USB drive entry and click **X** to remove it.

16. Click **OK** to remove the USB drive connection.

17. Remove the USB drive from the USB port on the Control Server.
7.17 Modify Thin Client Host Name

➢ To modify the Thin Client host name

1. Disable the Write Filter. Refer to the procedure To disable the Write Filter. The Thin Client will restart and automatically log in to the local User account.

2. Log in to the local Administrator account. Refer to the section Local Administrator Account Login.

3. From the Control Panel, select System to view computer information.

4. Locate Computer name, domain, and workgroup settings and select Change settings.
5. From the **System Properties** dialog box **Computer Name** tab, click **Change**...
6. Enter the computer name and click **OK** to save it.

![Computer Name/Domain Changes dialog box](image)

7. Enable the Write Filter. Refer to the procedure *To enable the Write Filter*. The Thin Client will restart and automatically log in to the local User account.
7.18 Create RDP Connection Desktop Shortcuts

➢ To create RDP connection desktop shortcuts

1. Disable the Write Filter. Refer to the procedure *To disable the Write Filter.*
   The Thin Client will restart and automatically log in to the local User account.
2. Log in to the local Administrator account. Refer to the section *Local Administrator Account Login.*
3. Open the Remote Desktop Connection window and expand Show Options.

4. In the **Computer** field, enter the target computer host name or IP address.
5. (Optional) In the **User name** field, enter a user name.
6. From the **Display** tab, select (check) **Use all my monitors for the remote session.**
7. (Optional) Modify the settings on the other tabs as needed.

8. From the **General** tab, select **Save As…**, modify the name, and save to the `C:\Users\User\Desktop` folder.

![Remote Desktop Connection](image)

9. If prompted, click **Continue** to access to the `C:\Users\User` directory.
10. Repeat this procedure for each RDP connection.

11. Enable the Write Filter. Refer to the procedure to enable the Write Filter.
    The Thin Client will restart and automatically log in to the local User account.

12. Verify that the RDP connection shortcuts are available on the User desktop.
Glossary of Terms

Client Access License (CAL) A license that grants a client device access to the services provided by the Windows Server.

Domain Controller (DC) A domain controller is a server that responds to security authentication requests (logging in, checking permissions, and so forth) within a Windows domain.

Dynamic Host Configuration Protocol (DHCP) A protocol used to automatically assign and manage dynamic IP addresses to devices on a network.

Plant Data Highway (PDH) The plant level supervisory network. PDH connects the HMI server with remote viewers, printers, historians, and external interfaces. Usually there is no direct connection to the Mark Vle controllers, which communicate over the UDH. Use of Ethernet with the TCP/IP protocol over PDH provides an open system for third-party interfaces.

Remote Desktop Protocol (RDP) A proprietary protocol that provides a user with a graphical interface to connect to another computer over a network connection.

RDS Per Device CAL A Client Access License (CAL) that allows a Thin Client terminal or other device to establish a Remote Desktop session with a Windows Server that has Remote Desktop Services enabled.

Remote Desktop Services (RDS) Allows a user to operate a virtual machine over a network connection.

Remote Desktop Session Host Server A Windows Server with Remote Desktop Services enabled. The Windows Server will work in coordination with the Remote Desktop License Server to verify that a device has a valid license before allowing it to establish a Remote Desktop session.

Terminal Services (TS) was renamed Remote Desktop Services in Windows Server 2008 R2.

Virtual Machine (VM) A virtual computer that emulates a physical computer.