Honeywell

Experion PKS

Windows Domain and Workgroup Implementation Guide for Windows Server 2003 and Windows Server 2008

EPDOC-X148-en-431A
February 2015

Release 431

Honeywell

Document	Release	Issue	Date
EPDOC-X148-en-431A	431	0	February 2015

Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Contents

1 About this document

This guide describes how to perform the following:

- Implementing Microsoft Windows domain controllers for Experion
- Implementing stand-alone Microsoft Windows domain controllers
- Migrating existing domain controllers to the latest supported Windows operating system for domain controllers
- Demoting domain controllers

Intended audience

- Customers who want to integrate their process domains into their corporate hierarchy and IT staffs who support them
- Customers with limited networking and IT experience who are using stand-alone domains
- Projects group and Services group

Prerequisite skills

It is assumed that you are familiar with the operation of Experion system software and the plant processes which Experion controls, Microsoft Windows operating systems, Windows domains and domain controllers, and network administration tasks.

Revision history

Revision	Publication date	Description
A	February 2015	Initial release

Revision history

Related documents

- Windows Domain and Workgroup Implementation Guide
- For planning information, refer to Windows Domain and Workgroup Planning Guide
- For operation system migration information, refer the appropriate operating system-specific implementation guide Windows Domain Implementation Guide for Windows Server 2008 R2
- *Getting Started with Experion Software Guide*
- *Software Installation User's Guide*
- *Experion migration documentation*
- *Supplementary Installation Tasks Guide*
- *Server and Client Planning Guide*
- *Server and Client Configuration Guide*

2 Installing a Windows Domain Controller

Related topics

2.1 Installing the Windows Server operating system

Installing Windows Server 2003 and Windows Server 2008

If the operating system is not installed already, install the operating system. Install service packs and Windows updates as recommended for Experion. Refer to the Experion Release Notes at the following Honeywell Process Solutions website.

http://www.honeywellprocess.com

For installing the Windows Server 2008 R2 operating system, refer to the *Windows Domain Implementation Guide for Windows Server 2008 R2 guide* available on the http://www.honeywellprocess.com website.

2.2 Setting local administrator password

For Microsoft Windows Server 2003 (32-bit), you are prompted to enter the local administrator account and password when installing the operating system.

For Microsoft Windows Server 2008 Standard/Microsoft Windows Server 2008 R2, you are prompted to enter the local administrator account and password during the first log on to the Windows after the operating system installation.

Perform the following steps to change the password.

1 Log on to the server as the local Administrator

2 Press **<Ctrl> <Alt> <Delete>** and change the password, if necessary.

CAUTION

Record and store the domain Administrator password in a secure place. If you forget the password, you have to reinstall the operating system to recover the password.

Note: When a member server is promoted to a Domain Controller, the local accounts database is removed. The local admin account and password become the domain admin account. In addition, any local accounts on the server are changed to domain accounts. However, this is only true for the first Domain Controller in a domain.

2.3 System requirements for a domain controller

Component	Microsoft Windows Server 2008 R2
Computer and processor	• Minimum – 1.4 GHz (x64) • Recommended – 2GHz or faster
Memory	• Minimum – 512 MB • Recommended – 2GB or greater • Maximum – 32GB
Hard disk	• Minimum – 10GB • Recommended – 40GB or more

Attention

In virtual environments Honeywell recommends that you have at least one DC on each network level serviced by the virtual environment, this would include a domain controller on level 2.5 and each level 2 network. If the entire domain is hosted on virtual machines, you must ensure that the virtual domain is always availability. Refer to the latest version of the following documents on http://www.honeywellprocess.com for the hardware and software requirements of VM.

- HPS Virtualization Specification
- Virtualization Planning and Implementation Guide

Ensure that at least one domain controller is in real environment.

2.3.1 Choosing the right operating system for a domain controller

Choosing the operating system for a domain controller depends on your organization requirements. Experion supports domain controllers running Microsoft Windows Server 2003 (32-bit), Microsoft Windows Server 2008 Standard, and Microsoft Windows Server 2008 R2.

However, if you are installing a new domain controller, choose Microsoft Windows Server 2008 R2 as it is the recommended version. If you already have Microsoft Windows Server 2003 (32-bit) or Microsoft Windows Server 2008 Standard operating system, you can continue to use that, or choose to upgrade to Microsoft Windows Server 2008 R2.

The domain controllers for must be configured with the forest functional level and the domain functional level set at Windows Server 2003 or higher.

2.3.2 Software requirements for implementing a domain in Experion

To implement a domain in Experion, you need the following media/software.

- R431.x Experion PKS Installation media

  The following table provides information about the Experion packages and its compatibility with the supported operating systems.

Experion packages	Microsoft Windows Server 2003 (32-bit)	Microsoft Windows Server 2008 Standard	Microsoft Windows Server 2008 R2
Domain Security Policy	Supported	Supported	Supported
System Management Runtime	Not supported	Supported	Supported
Fault Tolerant Ethernet	Supported	Supported	Supported
TPS Domain Console Configuration	Supported	Supported	Supported

Experion packages	Microsoft Windows Server 2003 (32-bit)	Microsoft Windows Server 2008 Standard	Microsoft Windows Server 2008 R2
USB Storage Enable/Disable	Supported	Supported	Supported

2.4 Guidelines to upgrade Windows Server 2003 DC to Windows Server 2008/Windows Server 2008 R2 DC

Attention

Refer to the following Microsoft documentation.

http://technet.microsoft.com/en-us/library/cc731188(WS.10).aspx

This activity requires sufficient planning before execution. The following is a summary of tasks that must be performed for upgrading a Microsoft Windows Server 2003 Domain Controller to a Microsoft Windows Server 2008 Standard and Microsoft Windows Server 2008 R2 Domain Controller.

For instructions to upgrade Microsoft Windows Server 2003 Domain Controller to Microsoft Windows Server 2008 R2 Domain Controller, refer to the document *Windows Domain Implementation Guide for Windows Server 2008 R2*.

1. Prepare the domain for Microsoft Windows Server 2008 Standard Active Directory — http://technet.microsoft.com/en-us/library/cc771461(WS.10).aspx
2. Introduce a Microsoft Windows Server 2008 Standard computer as a member server in the domain.
3. Install Microsoft Windows Server 2008 Standard Domain Controller on the member server.
4. Move required roles from the old (Windows Server 2003) Domain Controller to the new Domain Controller.
5. On the old Domain Controller, perform the following tasks.
   a. Demote the Domain Controller (“http://technet.microsoft.com/en-us/library/cc740017(WS.10).aspx”)
   b. Reload (not upgrade) Microsoft Windows Server 2008 Standard operating system.
   c. Promote as peer Domain Controller
   d. Move back any of the required roles

2.5 Domain controller backup strategies

Honeywell does not have any specific recommendations for Domain Controller backup. Refer to the Microsoft documentation at the following link.

http://technet.microsoft.com/en-us/library/aa997537(EXCHG.65).aspx

2.6 Setting time and date

This is generally done as part of the operating system installation. Time is crucial to the domain and hence, the time and the time zone must be verified before promoting a server to a Domain Controller.

2.7 Configuring the TCP/IP settings

For the actual data that needs to be entered, refer to your Domain Controller Configuration Data Sheet. Note that the Domain Controllers must use static IP addresses.

For configuring the TCP/IP settings on a domain running Microsoft Windows Server 2008 R2 operating system, refer to the document *Windows Domain Implementation Guide for Windows Server 2008 R2*.

Step	Microsoft Windows Server 2003 (32-bit)	Microsoft Windows Server 2008 Standard
1	Log on to the server as the local administrator.	Log on to the server as the local administrator.
2	From the **Start** menu, right-click **My Network Places** and select **Properties**.	Choose **Start** > **Control Panel**.
3	Right-click **Local Area Connection** and select **Properties**.	Do one of the following: If you use the Control Panel Home view, under the **Network and Internet** section, click **View network status and tasks**. If you use the Classic View, click **Network and Sharing Center**.
4	Double-click **Internet Protocol**.	In the **Tasks** section, click **Manage Network Connections**.
5	Select **Use the following IP address**.	Right-click **Local Area Connection** and select **Properties**.
6	Enter the **IP address**.	Select **Internet Protocol Version 4** (TCP/IPv4) and click **Properties**. Note: Leave the IPv6 address empty.
7	Enter the **Subnet mask**.	Select **Use the following IP address**.
8	Enter the **Default gateway**.	Enter the **IP address**.
9	Select **Use the following DNS Server addresses**.	Enter the **Subnet mask**.
10	Enter the IP address of the **Preferred DNS server** (this must be local address).	Enter the **Default gateway**.
11	Enter the IP address of the **Alternate DNS server**. Note: If you are installing the first Domain Controller, when using Active Directory integrated DNS, the alternate DNS server must be left blank. Once a Peer Domain Controller running DNS is added to the domain, the alternate DNS server address can be entered. If you are installing a peer Domain Controller running DNS, the Alternate DNS server must be the root Domain Controller that runs DNS.	Select **Use the following DNS Server addresses**.
12	Click **OK**.	Enter the IP address of the **Preferred DNS server** (this must be local address).

Step	Microsoft Windows Server 2003 (32-bit)	Microsoft Windows Server 2008 Standard
13	In the **Local Area Connection Properties** dialog box, click **OK**.	Enter the IP address of the **Alternate DNS server**. Note: If you are installing the first Domain Controller, when using Active Directory integrated DNS, the alternate DNS server must be left blank. Once a Peer Domain Controller running DNS is added to the domain, the alternate DNS server address can be entered. If you are installing a peer Domain Controller running DNS, the Alternate DNS server must be the root Domain Controller that runs DNS.
14	Physically connect the network (Ethernet) cable(s), if not already connected.	Click **OK**.
15		In the **Local Area Connection Properties** dialog box, click **OK**.
16		Physically connect the network (Ethernet) cable(s), if not already connected.

2.8 Changing the computer name

Attention
This procedure MUST be completed BEFORE promoting the computer to a Domain Controller, as it would be difficult to do so later on.

This is normally done as part of the operating system installation. If necessary, you can change the computer name by performing the following steps.

For changing the computer name of a server running Microsoft Windows Server 2008 R2 operating system, refer to the document *Windows Domain Implementation Guide for Windows Server 2008 R2*.

Step	Microsoft Windows Server 2003 (32-bit)	Microsoft Windows Server 2008 Standard
1	Log on to the server as the local administrator.	Log on to the server as local administrator.
2	From the **Start** menu, right-click the **My Computer** icon and select **Properties** .	Choose **Start** > **Administrative** > **Tools** > **Server Manager**.
3	Select the **Computer Name** tab and click **Change**.	In the **Server Summary**, under **Computer Information**, click the **Change System Properties** link. The **System Properties** System Properties dialog box is displayed.
4	Change the computer name of the server.	Click the **Change** button. The **Computer Name/Domain Changes** dialog box is displayed.
5	Restart the node.	In the **Computer name** box, type the new computer and then click **OK**.
6		If a restart your computer message dialog box appears, click **OK**.
7		Click **OK** in the **System Properties** dialog box.
8		In the restart your computer message dialog box, click **Yes** to restart the computer. After the computer restarts, “an unable to locate dll” event message may be displayed. This message can be ignored. Click **OK** to continue.

Attention
It is important to restart the server after changing the name and before promoting the server to a Domain Controller.

2.9 Promoting the Windows server to root Domain Controller

Perform the following steps to begin the promotion of the standalone Windows Server 2003/2008 server machine to a root or peer Domain Controller.

1. Log on to the server as local administrator.
2. Perform the following steps to run the Microsoft application dcpromo.exe.
   a. Choose **Start** > **Run**.
      The **Run** dialog box appears.
   b. Type **dcpromo**, and click **OK**.
      The dcpromo application initiates the **Active Directory Installation Wizard**.

      Refer to the section “Install Active Directory and DNS” on page 19.

2.10 Install Active Directory and DNS

At the Active Directory installation wizard, enter the appropriate configuration to install the Active Directory for a Root Domain Controller and install DNS, if necessary.

Regarding domain naming, refer to the section “Support for DNS”.

When installing DNS on a Microsoft Windows Server 2008 Standard / Microsoft Windows Server 2008 R2, the installation wizard may display a warning stating that one of the network adapters is not set to a static IP address. This message can be ignored as long as you have verified the IPv4 IP address information as mentioned in the section “Configuring the TCP/IP settings” on page 15. The error message in this situation is based on the IPv6 IP address that is neither configured nor required to be configured.

Attention

Record and store the Directory Services Restore Mode Administrator password in a secure place. If you forget the password, authoritative restores on the domain will not be possible. This is not the same account as the Domain Administrator.

Refer to the following Microsoft documentation for detailed instructions to Install Active Directory and DNS.

- Using the Active Directory installation wizard (Microsoft Windows Server 2003 (32-bit))–

  http://technet.microsoft.com/en-us/library/cc785263(WS.10).aspx
- Using the Active Directory installation wizard (Microsoft Windows Server 2008 Standard) – WS2008

  http://technet.microsoft.com/en-us/library/cc755103(WS.10).aspx

2.11 Adding reverse lookup zone to DNS

Using the DNS management application, add a Reverse Lookup Zone.

Start > **Administrative Tools** > **DNS**.

Note: The reverse lookup zone for the domain must be a primary zone and with “Store the zone in Active Directory” selected. In addition, once this is complete, the following command must be executed from the Command prompt on each node in the domain, including the Domain Controller.

ipconfig /registerdns

Refer to the Microsoft documentation for detailed instructions to add reverse lookup zone to DNS –

- Microsoft Windows Server 2003 (32-bit)—

  http://technet.microsoft.com/en-us/library/cc783250(WS.10).aspx
- Microsoft Windows Server 2008 Standard—

  http://technet.microsoft.com/en-us/library/cc753997.aspx

2.12 Installing the Honeywell Domain Controller package

The Experion Domain Controller Security package must be installed on the Domain Controller for a process control network before migrating to Experion or installing a new Experion system. Experion also supports installation of System Management and/or FTE on the Domain Controller in some circumstances. If your Domain Controller has components from previous versions of Experion or TPS, ensure that the TPS Domain/ Console Configuration Tool is removed before proceeding further.

These instructions apply to the following domain controllers.

- Single Domain Controllers, and peer Domain Controllers running on Windows Server 2003 (32-bit), Windows Server 2008 (32-bit), and Windows Server 2008 R2 (64-bit)
- Read-Only Domain Controllers (RODC) running on Windows Server 2008 (32-bit), and Windows Server 2008 R2 (64-bit)

Attention

The Domain Controller must be up-to-date with the latest updates from Microsoft before proceeding with the following instructions.

2.12.1 Domain Controller security policies and optional component (ESIS/DVD) installation

Considerations

- This package updates domain security policies ONLY. NO OTHER software is installed.
- If the computer is a Read-Only Domain Controller (RODC), refer to Windows Domain and Workgroup Implementation Guide. For planning information, refer to Windows Domain and Workgroup Planning Guide. For operation system migration information, refer the appropriate operating system-specific implementation guide Windows Domain Implementation Guide for Windows Server 2008 R2/Windows Domain Implementation Guide for Windows Server 2012..
- Before you begin installation on a system with Windows Server 2003 (32–bit) operating system, ensure that the Windows Server 2003 Service Pack 2 is installed to install Microsoft .NET 3.5 SP1.
- Before you configure a system with Windows Server 2012 operating system as a domain controller, ensure that Microsoft .NET 3.5 is installed manually.

Prerequisites

- Ensure that a common account does not exist between ESIS and the installation node.
- If you are installing Experion on Microsoft Windows Server 2003 (32-bit) operating system, add ESIS server as a trusted source in Internet Explorer (**Tools > Internet Options > Security > Trusted Sites**).

To start ESIS-based installation

1 In the **Welcome to ESIS** page, select **OS Preparation with/without Product Install**.
When prompted for the Windows credentials for the share.
   - Type the **<Domain Name>\Username** and **Password** if you belong to a domain and if you have share permissions.
   - Type the **<ESISServer IP>\Username** and **Password** if you belong to a workgroup and if you have share permissions.

2 Select **Product Install Only** option.

Attention

To install Domain Controller packages, you must select the **Product Install Only** option. Selecting the other options does not allow you to install the Domain Controller packages.

When prompted for the Windows credentials for the share.

- Type the **<Domain Name>\Username** and **Password** if you belong to a domain and if you have share permissions.
- Type the **<ESISServer IP>\Username** and **Password** if you belong to a workgroup and if you have share permissions.

3 Click **Next**.

> **Attention**
> After clicking **Next**, if an error message **Multiple users cannot be connected to the same network share** appears, refer to the section "Troubleshooting Experion for installation failure" in the *Experion Software Installation User's Guide* for the solution.

4 To continue with the installation go to "To continue with installation" section.

To start DVD-based installation

1 Log on to the Domain Controller using an account that is a member of the "Domain Admins" group.

2 Insert the Experion PKS Installation media into the DVD drive.

3 If the **Honeywell Experion PKS Installer** screen does not appear, using Windows Explorer, go to the browser folder on the Experion PKS Installation media, and double-click **setup.exe**.
The installer is automatically detected if it is executed on a Domain Controller.

4 To continue with the installation go to" To continue with installation" section.

To continue with installation

1 The **Setup** dialog box is displayed with the message, **Do you want to install the Experion PKS domain policies on this domain controller (Installing domain policies will install no other software on this machine)? NOTE: It may not be necessary to install these policies on more than one domain controller in a domain, or on the domain controller(s) for a child domain of a domain, where these policies are installed**.

- Select **No** to go to the section *Installing optional Experion components on the Domain Controller*. This bypasses installation of the domain policies and proceeds to optional component installation.
- Select **Yes** to install the Honeywell Domain Controller group policies , user accounts, and groups (this step also creates the *DCSComServer* account). Selecting **Yes** does not install any additional software on this domain controller.

The **Honeywell Security Model - Domain Controller InstallShield Wizard** is displayed.

2 Click **Next** to begin installation.
The **License Agreement** dialog box is displayed.

3 If you accept the license agreement, select **I accept the terms in the license agreement** and click **Next**.
If you do not accept the license agreement, click **Cancel**, and proceed to the section *Installing optional Experion components on the Domain Controller*.

4 If the *DcsComServer* domain account does not exist in this domain, the **DcsComServer Password** dialog box is displayed. Enter a strong password for this account in both fields, and click **Next**.
The following page is displayed, depending upon the number of organizational units (OUs) in a domain.

If	then...
the domain contains one or more organizational units (OUs)	**Link Policies to the Domain or an Organizational Unit** page is displayed
the domain does not contain organizational units (OUs)	**Ready to Install the Program** page is displayed

5 If the **Link Policies to the Domain or an Organizational Unit** page is displayed, select one of the following options, depending upon your preferences.

If	then select the option...
you are not aware of the impact and side effects of linking domain policies to an OU	Install policies at Domain level
you want the Honeywell security domain policies to be applied to the entire domain	Install policies at Domain level
you want to associate the Honeywell security domain policies with a single organizational unit	Link policies to an Organizational Unit (OU)

Select the appropriate OU, and click **Next**.

The **Ready to Install the Program** page is displayed.

6 In the **Ready to Install the Program** dialog box, click **Install** to begin the domain controller security package installation.

The **Installing Honeywell Security Model–Domain Controller** dialog box is displayed.

7 Once the installation is complete, the **InstallShield Wizard Completed** page is displayed. Click **Finish** to proceed.

8 Proceed with section *Installing optional Experion components on the Domain Controller*.

Installing optional Experion components on the Domain Controller

1 After the completion of the Honeywell security domain policies, the **Setup** dialog box is displayed with the message, **Do you want to install optional Experion PKS components on this domain controller? WARNING: if you answer "Yes" to this question, .NET 3.5 and installer-related software will be installed on this domain controller (if not already present), as it is required for the optional components that can be installed on this machine**.

- Click **Yes** to continue installing optional components.
- Click **No** to end the installation with no software installed on this domain controller.

Attention

- Clicking **Yes** installs Microsoft .NET 3.5 SP1 on this domain controller if it is not installed, even if no optional packages are installed during the procedure.
- If Microsoft .NET 3.5 SP1 is installed during this step, the system prompts for a reboot.
- After the reboot, perform the following steps, depending upon your mode of installation.

If you are installing from	then...
ESIS	1. Log on to the Domain Controller using an account that is a member of the "Domain Admins" group. 2. Double-click **setup.exe** at the root of the ESIS repository path. The **Welcome to ESIS Tool** screen is displayed. 3. Select **Product Install Only**, and click **Next**. The **Welcome to the Honeywell Experion PKS Installation Setup** screen is displayed.
DVD	1. Log on to the Domain Controller using an account that is a member of the "Domain Admins" group. 2. The **Welcome to the Honeywell Experion PKS Installation Setup** screen is displayed. If the **Welcome to the Honeywell Experion PKS Installation Setup** screen does not appear, using Windows Explorer, go to the browser folder on the Experion PKS Installation media, and double-click **setup.exe** .

2 If a **Microsoft User Account Control** dialog box is displayed, click **Yes**.

The **Setup type of Node to install** dialog box is displayed.

3 Select **Optional Features**, and click **Next**.

The **User and License Information** dialog box is displayed.

4 Specify the customer name and company name in the **Name** and **Company Name** fields respectively. Click **Next**.

The **Feature and Options Selection** dialog box is displayed.

5 Select the **Add-on Features** check box.
Depending upon the Domain Controller type, select the required options from the list of options displayed.

Domain Controller type	Option
Read-Only Domain Controller (RODC)	Select the following options. • System Management Runtime • Fault Tolerant Ethernet (FTE) • USB Storage Enable Disable
Writable Domain Controller	Select the following options. • System Management • Fault Tolerant Ethernet (FTE) • TPS Domain Console Configuration • USB Storage Enable Disable

Attention
System Management Runtime feature is not applicable for Windows Server 2003 and Windows Server 2008 (32-bit) operating system.

Click **Next**.

The **Summary** dialog box is displayed.

6 Review the summary of the settings selected, and click **Install**.
The **Experion PKS Status Display** dialog box is displayed, indicating the feature being installed/run.

7 If the *System Management* or *FTE* optional components were installed, perform the following procedure.

a Choose **Start** > **Run**.

b Type **dcomcnfg**, and click **OK**.

c Click **Yes** on the **User Account Control** dialog box.

d In the left pane of the **Component Services** window, select **Component Services > Computers > My Computer**.

e Right-click **My Computer**, and choose **Properties** from the context menu.

f In the **My Computer Properties** dialog box, click the **COM Security** tab.

g Click **Edit Default** for **Access Permissions**.

h In the **Access Permission** dialog box, click **Add**.

i In the **Enter the object names to select** dialog box, type **LOCAL SERVICE**, and click **OK**.

j In the **Access Permission** dialog box, select **LOCAL SERVICE** and ensure that only **Local Access Allow** is selected.

k Click **OK**.

l Click **Edit Default** for **Launch and Activation Permissions**.

m In the **Launch and Activate Permission** dialog box, click **Add**.

n In the **Enter the object names to select** dialog box, type **LOCAL SERVICE**

o In the **Launch and Activate Permission** dialog box, select LOCAL SERVICE and ensure the only permission check boxes that are checked are **Local Launch Allow** and **Local Activation Allow**.

p Click **OK**.

q In the **My Computer Properties** dialog box, click **OK**.

r Close the **Component Services** window.

8 When all packages have been successfully installed, the **Install Complete** message is displayed. Click **Yes** to complete the installation.

The system restarts automatically. After restart, log on to the system.

2.13 Installing a peer Domain Controller

Prerequisites

- The default Honeywell configuration and system policies are used as defined in this document. The administrator of the Experion system can choose to configure the system using additional policies. While this is allowed, it is not the intent of this document to cover all possible configurations of policies.
- The policies and procedures defined must be used on a per node basis within a single Microsoft Windows Server 2003 (32-bit), Microsoft Windows Server 2008 Standard, or Microsoft Windows Server 2008 R2 domain. This does not preclude the use of zero administration techniques, trusted domains, or physically separate resource and account domains, but those techniques are not described here.
- The computer must already be a member server of the domain for which you want to setup a peer Domain Controller.
- Active Directory DNS must be integrated with the peer Domain Controllers too. The following are some of the DNS-related settings that you need to perform during peer Domain Controller installation:
  - The Preferred DNS server address must be the local address of the member server that will be promoted.
  - The Alternate DNS server address must be the root Domain Controller that runs DNS.
  - In the root Domain Controller, the peer Domain Controller address must be configured as the alternate DNS address.
- All steps applicable for setting up a Domain Controller are applicable for peer Domain Controllers too. The Honeywell High Security Domain package need not be loaded on peer Domain Controllers as long as it is installed on one domain controller in the domain. The optional components discussed above for domain controllers can be installed on a peer domain controller.
- If you are using “Restore from backup” option to setup a peer Domain Controller, take a backup of Domain Controller, perform the following steps.

1 Choose **Start** > **Programs** > **Accessories** > **System Tools** > **Backup**.
The **Backup or Restore Wizard** dialog box is displayed.

2 Click **Advanced Mode**.
The **Backup Utility Window** is displayed.

3 Click the **Backup** tab and then select **System State** from the left pane.

4 Click **Browse** to specify the path for the backup.

5 Click **Start Backup**.
The backup files are saved in the specified path.

Perform the following steps to implement a Peer Domain Controller.

1 Review the checklist for peer Domain Controller installation at the following link.
http://technet.microsoft.com/en-us/library/cc759620(WS.10).aspx

Ensure that you are a member of the domain admin group before proceeding.

2 Verifying DNS before Active Directory installation at the following link.
http://technet.microsoft.com/en-us/library/cc778452(WS.10).aspx

3 Refer to the procedure at the following to create a peer Domain Controller.
http://technet.microsoft.com/en-us/library/cc781792(WS.10).aspx

2.14 Installing a read only Domain Controller

If the primary domain controller is at level 3 and you do not want to maintain or administer another domain or a child domain to the DMZ Domain, it is recommended that a *Read Only Domain Controller (RODC)* be created to replicate to the primary domain controller. This reduces maintenance and security issues faced with the domain upkeep. In addition, it facilitates in maintenance of the the domain settings without imposing or having direct access to the control network.

To add a read only domain controller to the domain, you must meet the following criteria:

- The forest functional level and the domain functional level must be Windows Server 2003 or higher.
- Run **Adprep.exe** command to prepare the existing forest and domains for domain controllers that run Microsoft Windows Server 2008 Standard or Microsoft Windows Server 2008 R2 operating systems.
- Deploy at least one writable domain controller running Microsoft Windows Server 2008 Standard or Microsoft Windows Server 2008 R2 in the same domain as the RODC. In addition, ensure that the writable domain controller is also a DNS server that has registered a name server (NS) resource record for the relevant DNS zone. An RODC must replicate domain updates from a writable domain controller running Microsoft Windows Server 2008 Standard or Microsoft Windows Server 2008 R2.

To prepare the node to be an RODC

1. Install the Windows Server 2008 operating system either using the Experion PKS System Initialization media or using the Microsoft operating system media provided by your platform manufacturer.
2. After the operating system is installed, configure the network settings and add the antivirus software and any other applications to aid with security and ease of use.
3. Activate the operating system.
4. Add the *Windows Server Backup* feature using **Server Manager Interface**.
5. Take a backup of the operating system on a removable drive or DVD.
6. Add the server machine to the domain that it is going to be as RODC for.

To create an RODC

1. Log on to the machine as Domain Administrator or local Administrator.
2. Using the **Server Manager** application, add a role. In the **Select Server Roles** dialog box, click **Server Roles** from left pane. Then select **Active Directory Domain Services** in the right pane.
3. Click **Install**.
   The installation of the role service begins.
4. After installation is complete, the service and roles installed are displayed in the **Installation Results** page.
5. Click **Close**.
6. Run the **dcpromo.exe** application. Select **Start > Run > dcpromo.exe**.
   The **Welcome to the Active Directory Domain Services Install Wizard** page is displayed.
7. Select **Use Advance Mode Installation**, and select **Next**.
   The **Operating System Compatibility** page is displayed.
8. If an IP address is not properly assigned on the computer, a warning message about invalid IP address is displayed. The IP address must be corrected before continuing.
9. In the **Deployment Configuration** page, select **Existing Forest** and then select **Add a Domain Controller to An Existing Domain**. Click **Next**.
   The **Network Credentials** page is displayed.
10. If you added the RODC to the domain, the domain is automatically displayed. Otherwise, type the full DNS name of domain in box, and click **Next**.

Attention

If you are not logged in as a domain account with permissions to add to the domain, the **Alternate Credentials** is prompted for. Enter the **Administrator account** and **password**, and click **OK**.

The **Select a Domain** page is displayed.

11 Select the domain from the list. If this is a child domain, more than one domain may appear in the list. Click **Next**.

The **Select a Site** page is displayed.

12 Select the site, usually the Default first site, and click **Next**.

The **Additional Domain Controller Options** page is displayed.

13 The wizard examines the DNS configuration and attempts to determine whether any authorized DNS servers are available. Select **Read-only Domain Controller** if you want this domain controller to be a read only domain controller. From your topology requirements also determine if the **Global Catalog** and **DNS server** is required. Click **Next**.

Attention

If you are installing the DNS server service and if the computer has dynamic IP addresses, the warning message, **This computer has dynamically assigned IP address(es)** is displayed even if IPV6 is not used.

Select **Yes, the computer uses a dynamically assigned IP address** only if the IP configuration for IPV6 is **DHCP** and/or if there are two adapters and FTE is installed on the node in the future.

The **Specify the Password Replication Policy** page is displayed.

14 Select **Add** to include additional groups and accounts, and click **Next**.

The **Select Users, Computers, or Groups** page is displayed.

15 Select the specific users and groups this domain controller must replicate.

Attention

- It is recommended to have access to the Experion accounts to replicate groups such as Engineers, Operators, and Supervisors. This ensures access to the control node if the connection between the RODC and the Replication Domain Controller is interrupted.
- Select the groups and users you want to have specific access at all time. The RODC is created to give access to users when there is a problem with access, and to minimize compromise of the machine if it is not secure.

16 Once the groups and users are selected, click **OK** and click **Next**.

The **Delegation of RODC Installation and Administration** page is displayed.

17 Configure the account or group that has local administrative permissions on the RODC, and click **Next**.

The **Install from Media** page is displayed.

18 Specify the replication from the network or media and click **Next**.

- If you have low bandwidth or the slow network connections to level 3 where the Replication Domain Controller is located, select **Replicate data from media at the following location**. Perform the steps in section *Installing RODC from media*.
- Otherwise, select **Replicate data over the network from an existing Domain Controller**.

The **Source Domain Controller** page is displayed.

19 Click **Next**.

The **Location for Database, Log Files, and SYSVOL** page is displayed.

20 Review the information and best practices for domain controllers. The default location is acceptable. However, your site may have a different scheme. After setting this correctly or taking the default values, click **Next**.

The **Directory Services Restore Mode Administrator Password** page is displayed.

21 Specify and confirm password for the system to startup in *Directory Services in Restore mode*. Ensure that this password is only used in restore mode and is different from the Administrator password. Click **Next**.

The **Summary** page is displayed.

22 Review the summary of the installation settings. If you want to create more than one RODC for this domain, choose to **Export Settings** to save the data. Click **Next** to start the installation of the RODC.
The **Active Directory Domain Services Installation Wizard** is displayed. The installation begins.

23 Verify the completing the active directory installation, click **Finish**.

24 Select **Restart Now** for the prompt to restart the computer.

Installing RODC from media

1 Log into the domain controller for which the RODC is being created for.

2 Run a command window as administrator. Type **ntdsutil** verify the prompt.

```
C:\Users\Administrator>ntdsutil
ntdsutil:
```

3 In the ntdsutil prompt, type **activate instance ntds**

```
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil:
```

4 At the ntdsutil prompt, type **ifm**.

```
ifm:
```

5 Now you can create a copy of the active directory data with or without the systvol data: at the ifm prompt type create **RODC SaveFolder** (where savefolder is an empty folder where the active directory information is stored).

```
ifm: create RODC d:\RODCSaveFolder
Creating snapshot for RODC media...
Snapshot set {7f1d9367-725b-4cfd-8f2f-b361e1870dcd} generated successfully.
Snapshot {9a0ee27a-0c7a-4662-b0c7-f9e37cef4736} mounted as C:\$SNAP_201004291433
_VOLUMEC$\
Initiating DEFRAGMENTATION mode...
            Source Database:
C:\$SNAP_201004291433_VOLUMEC$\Windows\NTDS\ntds.dit
            Target Database: d:\RODCSaveFolder\Active Directory\ntds.dit
Defragmentation  Status (% complete)
0    10   20   30   40   50   60   70   80   90  100
|----|----|----|----|----|----|----|----|----|----|
..................................................
Converting Full DC IFM media to Read-only DC IFM media...
Records scanned:       3518
Records scanned:        123
Read-only DC IFM media conversion completed successfully.
got 263572 buffers
Securing  Status (% complete)
0    10   20   30   40   50   60   70   80   90  100
|----|----|----|----|----|----|----|----|----|----|
..................................................
1536 pages seen
312 blank pages seen
0 unchanged pages seen
2 unused pages zeroed
1169 used pages seen
0 pages with unknown objid
65165 nodes seen
2 flag-deleted nodes zeroed
0 flag-deleted nodes not zeroed
0 version bits reset seen
0 orphaned LVs
Snapshot {9a0ee27a-0c7a-4662-b0c7-f9e37cef4736} unmounted.
IFM media created successfully in d:\RODCSaveFolder
ifm:
```

6 After that completes copy of the directory data for the Sysvol data at the ifm prompt type **create sysvol rodc Save** folder (where SaveFolder is the location where the Sysvol data is to be written)

```
ifm: create sysvol rodc d:\sysvolsave
Creating snapshot for RODC media...
Snapshot set {49b8b14a-3a2a-43c6-865e-36a32df4f4e3} generated successfully.
Snapshot {a0344482-f32b-4bd5-83ea-8f099ea862e7} mounted as C:\$SNAP_201004291436
_VOLUMEC$\
Snapshot {a0344482-f32b-4bd5-83ea-8f099ea862e7} is already mounted.
Initiating DEFRAGMENTATION mode...
```

```
            Source Database:
C:\$SNAP_201004291436_VOLUMEC$\Windows\NTDS\ntds.dit
            Target Database: d:\sysvolsave\Active Directory\ntds.dit

    Defragmentation  Status (% complete)
0    10   20   30   40   50   60   70   80   90  100
|----|----|----|----|----|----|----|----|----|----|
.................................................
Converting Full DC IFM media to Read-only DC IFM media...
Records scanned:       3518
Records scanned:        123
Read-only DC IFM media conversion completed successfully.got 263400 buffers
    Securing  Status (% complete)
    0    10   20   30   40   50   60   70   80   90  100
    |----|----|----|----|----|----|----|----|----|----|
.................................................

1536 pages seen
312 blank pages seen
0 unchanged pages seen
2 unused pages zeroed
1169 used pages seen
0 pages with unknown objid
65165 nodes seen
2 flag-deleted nodes zeroed
0 flag-deleted nodes not zeroed
0 version bits reset seen
0 orphaned LVs
Copying SYSVOL...
Copying d:\sysvolsave\SYSVOL
Copying d:\sysvolsave\SYSVOL\domain.com
Copying d:\sysvolsave\SYSVOL\domain.com\Policies
Copying d:\sysvolsave\SYSVOL\domain.com\Policies\{24bce660-8400-458f-96
fb-4c97b5a33727}
Copying d:\sysvolsave\SYSVOL\domain.com\Policies\{24bce660-8400-458f-96
fb-4c97b5a33727}\container.ldif
Copying d:\sysvolsave\SYSVOL\domain.com\Policies\{24bce660-8400-458f-96

Copying d:\sysvolsave\SYSVOL\domain.com\scripts\ec-ws08auditpolicy-ms.c
md
Copying d:\sysvolsave\SYSVOL\domain.com\scripts\ec-ws08auditpolicy-ms.t
xt
Copying
d:\sysvolsave\SYSVOL\domain.com\scripts\linkdomaingroups.vbs
Copying d:\sysvolsave\SYSVOL\domain.com\scripts\operator.bat
Snapshot {a0344482-f32b-4bd5-83ea-8f099ea862e7} unmounted.
IFM media created successfully in d:\sysvolsave
ifm:
```

7 Once complete, at the ifm prompt, type **quit**, at the ntdsutil prompt type **quit** again.

8 Save the two directories and the files to the RODC that is going to be added to the domain.

9 On The RODC from the **Install from Media** page, select **Replicate data from media at the following location**. Type the location where the two directories were copied to the RODC return to step 18 of the Create a RODC.

3 Setting up a Windows domain environment

Related topics

“Creating Active Directory users and groups” on page 32
“Configuring Organizational Units (OUs)” on page 34
“Creating a Group Policy” on page 35

3.1 Creating Active Directory users and groups

3.1.1 Creating a user

1. Click **Start** > **All Programs** > **Administrative Tools,** and then click **Active Directory Users and Computers**.
   The **Active Directory Users and Computers** window appears.
2. In the left pane, right-click the container in which you want to create the user/computer/group.
   A pop-up menu appears.

   Tip
   You can create an account in the domain or in one of the OUs.
3. Click **New**, and then select **User**.
4. In the **New Object – User** dialog box, fill in the details of the user and click **Next**.
5. In **First name**, type the user's first name.
6. In **Initials**, type the user's initials.
7. In **Last name**, type the user's last name.
8. Modify **Full name** to add initials or reverse order of first and last names.
9. In **User logon** name, type the user logon name, click the UPN suffix in the drop-down list, and then click **Next**.
10. In **Password** and **Confirm password**, type the user's password, and then select the appropriate password options.
11. Click **OK**.

Next steps

Add new users to the appropriate domain groups, particularly the Experion groups, to grant the user privileges within the domain.

3.1.2 Creating Active Directory groups

To create Active Directory groups

1. Log on to the domain controller using an account with administrative privileges.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
   The **Active Directory Users and Computers** window opens.
3. In the console tree, right-click the folder (*Active Directory Users and Computers/domain node/folder*) in which you want to add a group.
4. Click **New** > **Group**.
   The **New Object — Group** dialog box appears.
5. Type the **Group** name.
6. Select **Group scope** and **Group type** for the group, as desired.
7. Click **OK**.
   A new group is created and appears in the details pane of the **Active Directory Users and Computers** window.

3.1.3 Changing group membership

To change group membership

1. Log on to the domain controller using an account with administrative privileges.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
   The **Active Directory Users and Computers** window opens.
3. In the console tree, browse to the folder (Active Directory Users and Computers/domain node/folder) containing the group that you want to modify.
4. Select the **Honeywell Group** that you want to modify.
5. In the details pane (right pane), right-click the group, and then click **Properties**.
6. On the **Members** tab, click **Add**.
7. Enter the Honeywell user name and then **Check Names**.
   A valid entry will have an underline.
8. Click **OK**.
9. Repeat steps until the required users are added to the group.
10. Click **OK**.

For further guidance on managing groups, refer to the following Microsoft documentation.

http://technet.microsoft.com/en-us/library/cc738263(WS.10).aspx

3.2 Configuring Organizational Units (OUs)

Attention

- These tasks can be performed only from writable domain controllers that have the **TPS Domain Console Configuration** optional package installed.
- Creating an Experion/TPS domain OU or a Console OU allows you to organize and manage plant nodes of interest from a System Management Display. An Experion Console OU provides a grouping of similar process control computers within a TPS domain OU.

3.2.1 Create a TPS Domain OU

Perform the following steps to create a TPS domain OU.

1. At the Domain Controller, with domain administrator privileges, open **Active Directory Users and Computers**.
2. Point to **New**, and then click **Organizational Unit**.
3. Type the name of the organizational unit.
4. **Right-click** the new OU and select **Properties**.
5. Select the **TPS Domain** tab, and then select the **TPS Domain** option.
6. Click **OK**.
   The OU now has the "TPS Domain" attribute.

3.2.2 Create an Experion/TPS domain OU or a console OU within a TPS domain OU

1. Click **Start** > **All Programs** > **Administrative Tools,** and then click **Active Directory Users and Computers**.
   The **Active Directory Users and Computers** window appears.
2. Refer to the procedure in section “Create a TPS Domain OU” on page 34 and create an OU within the TPS domain OU.
3. Right-click the new OU and select **Properties**.
   The Properties dialog box appears.

   Tip
   This can be performed on Domain Controllers that have had the Domain Controller Security installed.
4. Click the **TPS Domain** tab.
   The TPS Domain Properties dialog box appears.
5. Click **Console**.
6. Click **OK**.

3.3 Creating a Group Policy

You can create and link a Group Policy to a domain or one or more OUs within a domain by using the Group Policy Management Console.

To create a group policy, perform the following steps.

1. Log on to the Domain Controller using a domain administrator account.
2. Choose **Start** > **All Programs** > **Administrative Tools** > **Group Policy Management**.
3. On the User Account Control dialog box, click **Yes**.
4. In the left (navigation) pane, expand the tree and right-click **Group Policy Objects** under the required domain and select **New**.
5. Enter the policy name and click **OK**.

Refer to the following Microsoft documentation to create and link a Group Policy.

http://technet.microsoft.com/en-us/library/cc776678(WS.10).aspx

4 Integrating computers into a Windows domain

This section describes the tasks for integrating computers into an existing Windows domain.

This section does not describe how to create a Windows domain. For security-related guidelines about Windows domains and Experion, refer to the *Experion Network and Security Planning Guide*.

Related topics

"Adding a Windows domain security group to a local security group on a computer" on page 38
"Creating mutually trusted domains" on page 39
"Associating Windows domain account groups with the local account groups on a computer" on page 40

4.1 Adding a Windows domain security group to a local security group on a computer

If you require a Windows domain account to have local administrator rights complete these instructions.

Prerequisites

- You have a Windows domain controller installed and operating correctly.
- For the remaining installation instructions, if you are instructed to log on to the computer using a Windows account with local administrator rights, you can log on to the computer using a domain account that has been added the local Administrators group on this computer.
- If a Windows domain account is required to import or export Control Builder repositories, that Windows domain account must be added to the local Engineering Repository Administrator group.

To add a Windows domain account group to a local account group

1. Choose **Start**, right-click on **Computer** and choose **Manage**.
2. If prompted, click **Continue** in the **User Account Control** dialog box.
3. Expand the **Configuration** item.
4. Expand the **System Tools** item.
5. Expand the **Local Users and Groups** item.
6. Click **Groups**.
7. Double-click on the name of the local group to add the domain account. For example, double-click Administrators.
8. Click **Add** to display the **Select Users or GroupsSelect Users, Computers, or GroupsSelect Users, Computers, Service Accounts or Groups** dialog box.
9. Click **Locations** to display the **Locations** dialog box.
10. If prompted, type the user name and password of an account with permissions for the required domain.
11. Click the domain name containing the domain account and then click **OK**.
12. In the **Enter the object names to select** box, type the name of Windows domain group account.
13. Click **OK**.
14. Click **OK** to close the group account properties dialog box.

4.2 Creating mutually trusted domains

Mutually trusting domains are created by configuring the primary domain controllers on two connected domains to trust the partner domain. To set up mutually trusting domains, each domain must trust the other domain and each domain must know what other domains trust it. The process for defining these relationships is to create a trusted domain and to create a trusting domain. A trusted domain is a domain that is trusted by the domain that is being configured. A trusting domain is a domain that trusts the domain that is being configured.

Configuring mutually trusting domains is required only if the CDA-SP service (ACE) is on a different domain to an OPC server. Mutually trusting domains are created by configuring the domain controllers on two connected domains to trust the partner domain.

To set up mutually trusting domains, ensure that both domain controllers are configured using the appropriate procedure.

Attention

Creating a trust between two domains requires name resolution to be setup so that both domains can resolve the other domain name. An example of this is setting up a secondary DNS zone for the other domain.

If you are setting mutually trusted domains to support a control configuration such as the CDA-SP service (ACE) on a different domain to an OPC server, consult your nearest Honeywell representatives for additional configration requirements.

To create mutually trusted domains

1. Click **Start**, right-click on **Computer**, and then click **Manage**.
2. If prompted, click **Continue** in the **User Account Control** dialog box.
3. Expand **Roles**, and then click **Active Directory Domain Services**.
4. In the right pane, locate **Advanced Tools**. To see the advanced options, click the arrow next to **Advanced Tools**.
5. Click **AD Domains and Trusts**.
   The **Active Directory Domains and Trust** window appears.
6. Expand the **Active Directory Domains and Trust** item, right-click the local domain name, and then click **Properties**.
7. Click the **Trusts** tab.
8. Click **New Trust**.
   The **New Trust Wizard** appears.
9. In the **Trust Name** box, type the name of the other domain, and then click **Next**.
10. In the **Trust Type** box, select **External Trust for Windows 2008 to Windows 2003 and Forest Trust for Windows 2008 to Windows 2008**, and then click **Next**.
11. In the **Direction of Trust** box, select **Two-Way**, and then click **Next**.
12. In the **Sides of Trust** box, select **Both this Domain and the specified domain**, then click **Next**.
13. In the **User Name and Password** boxes, enter the credentials of domain account for the other domain, and then click **Next**.
14. In the **Outgoing Trust Authentication Level-Local Domain** page, select **Domain-wide authentication**, and then click **Next**.
15. In the **Trust Selections Complete** page, click **Next**.
16. In the **Confirm Outgoing Trust** page, select **Yes** to confirm the outgoing trust, and then click **Next**.
17. In the **Confirm Incoming Trust** page, select **Yes** to confirm the incoming trust and then click **Next**.
18. In the **Completing the New Trust Wizard** page, click **Finish**.

4.3 Associating Windows domain account groups with the local account groups on a computer

You only need to perform this procedure if you use domains. This procedure links Windows domain account groups with local account groups for computers participating in a domain and the Honeywell High Security Policy.

Prerequisites

- The computer must already be added to the domain.
- Perform this procedure on every computer in the domain where you want to implement the High Security Policy.

To link the Windows domain account groups to the Windows local account groups

1 Log on as a user with administrative privileges.

2 Click **Start** > **All Programs** > **Honeywell Experion PKS** > **System Management** > **Link Domain Groups**.

The **User Account Control** dialog box appears.

3 Click **OK**.

A dialog box appears displaying the success of the *Link Domain Groups command*.

4 Perform the following based on the success of running the *Link Domain Groups command*.

- If there are no errors, click **OK** to acknowledge the success message.
- If errors are indicated, select the **Details** checkbox.

  Information about the problems encountered appears.

After running the *Link Domain Groups command*, the Windows domain account groups are linked to the local account groups as follows.

Windows domain account group	Linked to local account group
DCS Administrators	Product Administrators
Engineers	Local Engineers
Supervisors	Local Supervisors
Operators	Local Operators
Ack View Only Usage	Local Ack View Only Users
View Only Users	Local View Only Users
DCS Domain Servers	Local Servers

5 Creating Windows Workgroup users and groups

Attention

Any accounts that need to access other computers must have the same user name and password on all computers. For more information about creating Windows Workgroup users and groups, refer to the following Microsoft documentation.

http://technet.microsoft.com/en-us/library/cc775771(WS.10).aspx

6 Reviewing security templates in domain/workgroup environment

To review security templates in domain/workgroup environment

1. Choose **Start** > **Run**, type `mmc` and click OK.
   The **Microsoft Management Console** opens.
2. If the **User Account Control** dialog box appears, click **Yes**.
3. Choose **File** > **Add/Remove Snap-in**.
   The **Add/Remove Snap-in** dialog box opens.
4. Click **Add**.
   The **Add Standalone Snap-in** dialog box opens.
5. Select **Security Templates** and click **Add**.
6. Click **OK**.
   The Security Templates snap-in is added to the console.
7. In the navigation pane, right-click **Security Templates**, and select **New Template Search Path**.
8. In the **Browse For Folder** dialog box, navigate to **Desktop** > **Computer** > **Local Disk (C:)** > **Windows** > **Security** > **Templates**, select **Templates**, and then click **OK**.
9. In the navigation pane, expand *C:\Windows\security\templates* and select **honeywellws**.
10. Review the setting in the right pane.

7 Setting up time synchronization

Related topics

“Time synchronization in a domain” on page 46
“Time synchronization in a virtual environment” on page 47

7.1 Time synchronization in a domain

The Active Directory domain is time sensitive and any time differences between domain controllers and client nodes could affect the authentication process of users and resource access. When a member server is promoted as the first domain controller in the domain, that server automatically receives all of the FSMO roles. The PDC emulator role controls time on the domain and the server holding that role becomes the authoritative time source on the domain. Any authentication process on any resource on the domain must have a clock setting that is within 5 minutes of the PDC emulator role holder. If the time difference between the machine clock and the PDC emulator role holder clock is greater than 5 minutes, the authentication process fails. Once there is peer domain controller in the domain, the PDC emulator role can be moved to any domain controller in the domain. By default, the PDC emulator role holder will use its local clock as the time source for the domain. The time source for the PDC emulator can be changed to use an external source such as hardware clock (GPS clock) or an internet time server.

In the Experion network, once a computer joins the domain, it will use the PDC role holder as the authoritative time source. If the computer had SNTP setup run on it while in a workgroup the SNTP setup settings may need to be cleared before SNTP time functions correctly on the computer.

For more information on configuring a time source for the forest, refer to the article at the following link.

http://technet.microsoft.com/en-us/library/cc794823(WS.10).aspx

Tip

For more information about time synchronization and SNTP setup, refer to the *Supplementary Installation Tasks Guide*.

7.2 Time synchronization in a virtual environment

With Experion , virtualization deployment is supported for Experion and domain controllers. When a domain controller is a virtual machine, its local clock is no longer accurate. When the PDC role holder is running in a virtual machine, this behavior could cause clock drift and invalidate access to network resources. For sites that virtualize the domain controller that holds the PDC role, the following steps must be performed on the PDC role holder.

- Do not synchronize the PDC role holder time with the vmhost.
- Force the PDC role holder to synchronize the time with an external time source either a GPS device or an internet time source. Refer to the following VMware white paper for instructions for this process.

  http://www.vmware.com/files/pdf/Virtualizing_Windows_Active_Directory.pdf

Attention
When creating a virtual domain controller, do not convert a physical domain controller to a virtual domain controller.

Tip
For more information about time synchronization in a virtual environment, refer to the Virtualization Planning and Implementation Guide.

8 Securing the operating system

Related topics

“Creating and assigning login scripts” on page 50
“Removing access to Windows Explorer and the Task Manager” on page 54
“Setting up automatic logon” on page 56
“Preventing operator shutdown” on page 57
“Disabling the lock computer option” on page 58

8.1 Creating and assigning login scripts

8.1.1 Station command line options

The following command line options may be added to the command to start the Station application in batch files or in shortcuts to tailor the environment that Station runs in.

The syntax for **Station.exe** is as follows:

```
station.exe [-stn <path to .stn file>] [-s[f][l][x][s][c]]
```

Parameter	Description
stn	Path to the Station.stn file. Do not include the path if the Station.stn file is in the same location as the Station.exe file.
-s	Startup switches
f	Disables window resizing so that Station can only operate in full screen mode and is always on top.
l	Disables window resizing so that Station can only operate in full screen mode and is always on the bottom
x	Disables the Exit menu choice
s	Disables the Setup menu choice
c	Disables the Connect menu choice

8.1.2 Locking station in full screen mode and disabling menus

You can restrict access to non-Station software on a computer by changing the Station command line.

Changing the Station command line allows you to do the following:

- Lock the Station window in full screen so that users cannot resize the window or access operating system functions and non-Station applications.
- Disable the Exit menu choice so users cannot close down this Station.
- Disable the Setup menu choice so that users cannot change the connection or display settings for this Station.
- Disable the Connect menu choice so that the users cannot attempt to connect to a different server and disconnect from the current server.

By default, access to Intranet and Internet sites are disabled on Station. For information on enabling full or restricted access via Station's SafeBrowse feature, refer to the section “Customizing Station - Web Access tab, Connection properties” in the *Server and Client Configuration Guide*.

8.1.3 Creating a Station startup batch file

For operators to access Station on a secure computer, create a batch file that enables the Station to start automatically when the operator logs on to the computer.

To create the batch file

1. For domain account scripts, log on to the domain controller with a domain administrator account.
2. Use a text editor such as Notepad, to create the following batch file.

Attention

If you use Signon Manager and Electronic Signatures, you must use the **–sl** option so that Station is in full-screen mode but always on the bottom so that the Signon Manager and Electronic Signatures dialog boxes appear on top of Station.

```
rem Run signon.exe only if you are using Sigon Manager

cd /d "%hwinstallpath%\Signon Manager"

start signon.exe
rem ******************************************
rem change to station directory
rem ******************************************

cd /d "%hwinstallpath%\Experion PKS\Client\Station"

rem ******************************************
rem the following line need only be included
rem if you are on the Server PC
rem and also using automatic logon.
rem It delays Station startup to let the
rem Server start completely first.
rem ******************************************
sleep 70
rem ******************************************
rem start station with "full screen lock" and always on top
rem and all 'Station" menu options inactive.
rem stnsetup.stn is optional, delete if not
rem required.
rem ******************************************
start station.exe “C:\ProgramData\Honeywell\Experion PKS\Client\Station\sntsetup.stn” -sslxc
```

WARNING

Do not add a network path to the ‘path’ environment variable.

3 Save the file according to the locations specified in one of the following sections.

- Assigning logon scripts to domain groups and users using group policy.
- Assigning logon scripts to individual domain accounts.
- Assigning logon scripts to local accounts.

8.1.4 Assigning logon scripts to domain groups and users using group policy

This procedure demonstrates how to assign the *Operator_Start.bat* logon script to all domain users that are members of the Operators global group.

For a Microsoft Windows Server 2003 domain controller, the Group Policy Management Console must be installed first. On Microsoft Windows Server 2008 R2/Microsoft Windows Server 2008 R2, it is installed by default.

To assign logon scripts to domain groups and users using group policy

1 Log on to the domain controller using a domain administrator account.

2 Place the *Operator_Start.bat* script in the following path — %SystemRoot%\SYSVOL\Domain\Scripts.

3 Choose **Start** > **All Programs** > **Administrative Tools** > **Group Policy Management**.

4 Click **Yes** on the **User Account Control** dialog box.

5 In the left pane (navigation pane), expand the tree, right-click **Group Policy Objects** under the required domain, and then click **New**.

6 Type the new policy name as **Operator Startup Policy**, and then click **OK**.

7 Right-click the new policy in the navigation pane, and then click **Edit**.

8 In the navigation pane of the **Group Policy Management Editor**, expand **User Configuration > Policies > Windows Settings**, and then click **Scripts (Logon/Logoff)**.

9 In the right pane, double-click **Logon**.

10 In the **Logon Properties** dialog box, click **Add**.

11 In the **Script Name** field, type *Operator_Start.bat* and type required script parameters in the **Script Parameters** field, then click **OK**.

12 In the **Logon Properties** dialog box, click **OK**.

13 Close the **Group Policy Object Editor** window.

14 In the right pane of the **Group Policy Management** window, click the **Details** tab and in the **GPO Status** list, select **Computer Configuration Settings Disabled**.

15 In the navigation pane, drag the new policy to the domain (or OU) to which this policy should apply to.

16 If you want to link the GPO to the selected location, click **OK**.

17 In the navigation pane, expand **Group Policy Objects > Operator Startup Policy** .

18 In the right pane, remove the users/groups listed under the **Security Filtering**, and then click **Add** to add the required groups (or individual users).

19 When the group policies are next pushed to the computers in the domain, this startup script applies to all operator logon.

8.1.5 Assigning logon scripts to individual domain accounts

Perform the following steps to specify the batch file as a logon script for domain accounts.

1 Log on to the domain controller using a domain administrator account.

2 Choose **Start > Control Panel > System and Maintenance > Administrative Tools > Active Directory Users and Computers**.

3 Place the Operator_Start.bat script in **%SystemRoot%\SYSVOL\domain\scripts**.

4 In the tree view, select **Users** to display the list of users in the domain.

5 Right-click the account name to which the Logon Script must be assigned, and then click **Properties**.

6 On the **Profile** tab, type Operator_Start.bat in the **Logon script** box.

7 Click **OK**.

8 Close **Active Directory Users and Computers**.

8.1.6 Assigning logon scripts to local accounts

Assigning logon scripts to local accounts

1 Log on to the local machine using a domain or local administrator account.

2 If the local computer does not have a NetLogon share, create a directory to be used for the share (for example %SystemRoot%\NetLogon), and share the directory using the name “NetLogon”.

3 Place the Operator_start.bat file in `\\<computername>\NetLogon`, or use the local directory path that is shared as NetLogon.

4 Choose **Start > Control Panel > System and Maintenance > Administrative Tools > Computer Management**.

5 Select **Local Users and Groups** > **Users**.

6 Double-click the user account that you want to modify.
The **Properties** dialog box is displayed.

7 Click the **Profile** tab, and in **Logon Script** box, type `Operator_Start.bat`.

8 Click **Apply**.

9 Click **OK** to close the **Properties** dialog box.

10 Close **Computer Management**.

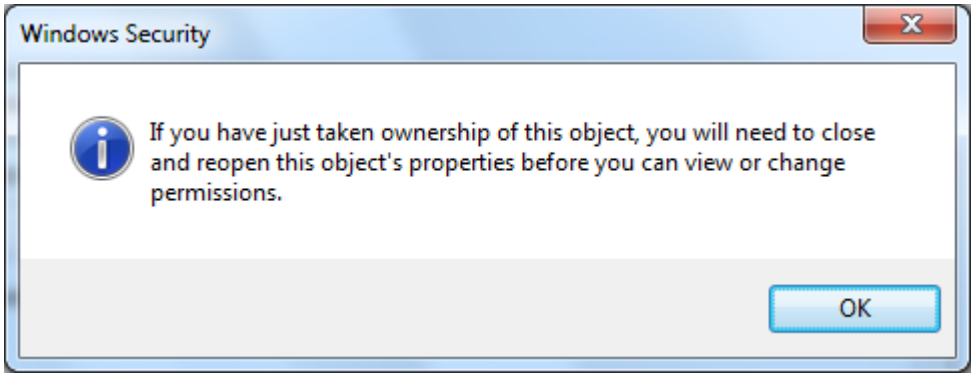
8.2 Removing access to Windows Explorer and the Task Manager

This procedure applies to computers in a workgroup environment. In a domain environment, this is automatically taken care through the **Honeywell Operational Roles GPO** settings.

You can prevent operators from accessing applications through Task Manager, Windows Explorer, and Internet Explorer by removing access to Task Manager, Windows Explorer, and Internet Explorer.

To remove access to Windows Explorer and Task Manager

1. In Windows Explorer, navigate to the **%windir%\System32** directory.
2. Perform the following steps only if your operating system is Windows 7 or Windows Server 2008.
   a. Right-click taskmgr.exe, choose **Properties** and click the **Security** tab.
   b. In the **Security** tab, click **Advanced**.
      The **Advanced Security Settings** dialog box appears.
   c. In the **Advanced Security Settings** dialog box, click the **Owner** tab.
   d. Click **Edit**.
   e. Click **Yes/Continue** if the **User Account Control** dialog box appears.
   f. In the **Change owner to** list, select **Administrators**, and click **OK**.
   g. Click **OK** in the **Security** tab.
      The **Windows Security** dialog box appears with the following message:



   h. Click **OK** in the **Windows Security** dialog box.
   i. Click **OK** to close the **Properties** dialog box.
3. Right-click taskmgr.exe, choose **Properties** and click the **Security** tab.
4. In the **Security** tab, click **Edit**.
5. Click **Yes/Continue** if the **User Account Control** dialog box appears.
6. In the **Security** tab, click **Add**.
   The **Select Users, Computers, or Groups** dialog box appears.
7. Click **Advanced**.
   The **Common Queries** tab appears within the **Select Users, Computers, Service Accounts, or Groups** dialog box.
8. Click **Find Now**.
   The **Search Results** section displays a list of users and groups in the domain.
9. Select the user or the group for which you want to remove/restrict access to Task Manager.
10. If there are additional groups or users that must be restricted, hold down the **CTRL** key while clicking each additional user/group.
11. Click **OK** in the **Common Queries** tab.

12 Click **OK** in the **Select Users, Computers, or Groups** dialog box.
The selected user(s) and group(s) are listed in the **Security** tab, in the **Group or user names** section.

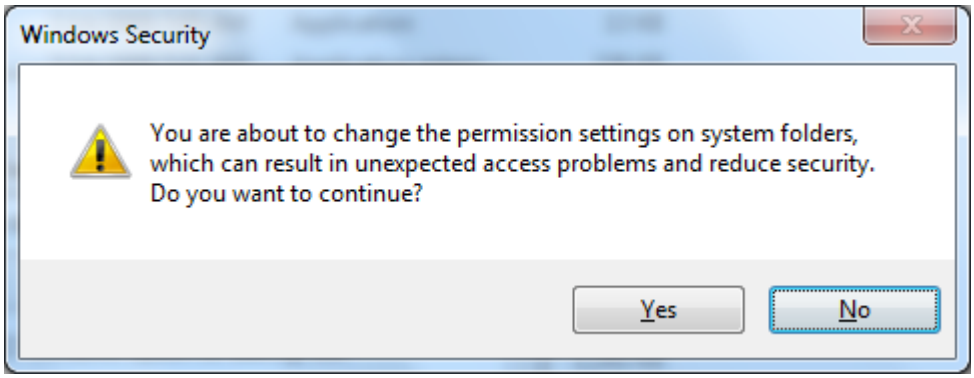
13 For each user or group that you added to the **Group or user names** section, perform the following:

a Click the name in the **Group or user names** list.

b In the **Permissions for** dialog box, click the checkbox in the Deny column next to **Read & Execute/ Allow**.

14 When all necessary users/groups are denied the access to execute, click **OK**.

a On systems with Windows 7 and Windows Server 2008 operating systems, the **Windows Security** dialog box appears with the following message:



b Click **Yes** in the **Windows Security** dialog box.

c Click **Yes**, if the same message appears.

15 Click **OK** to close the **Properties** dialog box.

16 Repeat the above steps for **Windows Explorer**.

a Choose **Start > Run**, and type **%windir%**
The **Windows** folder appears.

b Locate **explorer.exe**, and continue with step 1.

17 Repeat the above steps for **Internet Explorer**.

a Choose **Start > Run**, and type **%programfiles%**
The **Program Files** folder appears.

b In the **Internet Explorer** folder, locate **iexplore.exe**, and continue with step 1.

8.3 Setting up automatic logon

If you want Windows to start automatically without the operator entering a Windows password, you can set up automatic logon. If you set up automatic logon, the computer always logs on with the same user name and password.

Attention

- Computers must be configured individually for auto-logon in a domain or workgroup.
- Automatic logon can be useful in a Plant environment but you must use it with a very restrictive user account. It should not be used with user accounts with administrative privileges.
- If you set up automatic logon for a computer, to log on as an Administrator, you need to press the Shift key to prevent automatic logon.
- After following the procedures for automatic logon, automatic logon is set the first time after any restart. To get the computer to automatic logon after each restart and each logoff, you must set the registry value of ForceAutoLogon = 1 in the same key.

8.3.1 Setting up automatic logon in a domain

CAUTION

- Editing Windows registry can cause serious problems, if modified incorrectly. To recover from the problem, you might have to reinstall the operating system. As a best practice, ensure that you take a back up of the Windows registry before making any changes.
- This mechanism of changing the password is a security risk since a clear text password would be visible in the registry entry.

To set up an automatic logon in a domain, edit the following registry entries.

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key:
- DefaultUserName = the user account name
- DefaultPassword = the password for that account
- DefaultDomainName = computer name for local accounts or domain name for domain accounts
- AutoAdminLogon = 1

8.3.2 Setting up automatic logon in a workgroup

1. Choose **Start > Run**.
2. In the **Run** dialog box, type `control userpasswords2`, and then click **OK**.
3. Select the user account, and then clear the **Users must enter a user name and password to use this computer** check box.
4. Click **Apply**.
5. In the **Automatically Log On** dialog box, enter the password for the selected account and confirm to add the password to the system.
6. In the **Automatically Log On** dialog box, click **OK**.
7. In the **User Accounts** dialog box, click **OK**.
8. If automatic logon does not work when Windows is restarted, it is because the password was entered incorrectly. Repeat the above steps to correct the issue after the account and password are checked for correctness.

8.4 Preventing operator shutdown

This procedure applies to computers in a workgroup environment. In a domain environment, this is automatically taken care through the **Honeywell Operational Roles GPO** settings.

Product Administrators, Engineers, and Supervisors can shut down a computer in several ways.

- From the Start menu.
- By pressing CTRL+ALT+DEL.
- At the logon screen.

To prevent Product Administrators, Engineers and Supervisors from shutting down the computer, you must change the local policies and edit the registry.

To change the local policies to prevent shut down by selected users

1. Choose **Start > Settings > Control Panel > System and Maintenance > Administrative Tools > Local Security Policy**.
2. In the navigation pane, choose **Local Policies > Security Options**.
3. Select **Local Policies > User Rights Assignment**.
4. Double-click **Shutdown the system**.

   The **Shut down the system Properties** dialog box opens. Typical settings will include Administrators, Backup Operators, Product Administrators, Local Supervisors, and Local Engineers.
5. Remove any users or groups that must not be able to shut down the system.
6. Add any additional users or groups that must able to shut down the system.
7. Click **OK** to close the **Shut down the system Properties** dialog box.
8. Close the **Local Security Policy** window.

To prevent shut down from logon screen

1. Choose **Start > All programs > Administrative Tools > Local Security Policy**.
2. In the navigation pane, select **Local Policies > Security Options**.
3. In the right pane, double-click **Shutdown: Allow system to be shut down without having to log on**.
4. Select **Disabled** and click **OK**.
5. Close the **Local Security Policy** window.

8.5 Disabling the lock computer option

This procedure applies to computers in a workgroup environment. In a domain environment, this is automatically taken care through the **Honeywell Operational Roles GPO** settings.

Product Administrators, Engineers and Supervisors can lock a computer in several ways.

- From the Start menu.
- By pressing CTRL+ALT+DEL.
- At the logon screen.

To prevent Product Administrators, Engineers and Supervisors from locking the computer, you need to change the local policies and edit the registry.

1. Choose **Start > Run**, type mmc and click **OK**.
2. On the User Account Control dialog box, click **Yes**.
3. In the **Console Root** window, select **File > Add/Remove Snap-in**.
4. In the **Add or Remove Snap-ins** dialog box, select **Group Policy Object Editor**, click **Add**.
5. In the **Select Group Policy Object** dialog box, click **Finish**.
6. In the **Add or Remove Snap-ins** dialog box, click **OK**.
7. In the Console Root windows navigation pane, select **Local Computer Policy > User Configuration > Administrative Templates > System > Ctrl + Alt + Del Options**.
8. In the right pane, double-click **Remove Lock Computer**.
9. In the **Remove Lock Computer** dialog box, click Enabled, and then click **Apply**.
10. Press CTRL+ALT+DEL to verify that **Lock Computer** option is disabled. Click **Cancel**.
11. Click **OK** to close the **Disable Lock Computer Properties** dialog box.

9 Managing domains

Related topics

“Managing domain group policy” on page 60
“Creating mutually trusted domains” on page 39
“Renaming a domain controller” on page 63
“Removing a domain controller” on page 64

9.1 Managing domain group policy

Overview

The Group Policy Management Console (GPMC) is the primary tool that Microsoft provides for managing group policies. This tool is an optional feature on Microsoft Windows Server 2008 R2 and Microsoft Windows Server 2008 R2, and is a free download from Microsoft for Microsoft Windows Server 2003, Microsoft Windows 7 Professional, and Microsoft Windows XP. Detailed information about using GPMC is available from Microsoft at http://technet.microsoft.com/en-us/library/cc783034(WS.10).aspx.

Edit a Group Policy

Attention

You must not modify the Experion group policies, as each update to Experion overwrites these policies, eliminating any changes you have made. To change policy settings, create a new Group Policy Object (GPO), add only the settings you need to change, and link the policy such that the new settings override the Experion setting. Warning: Be cautious while overriding Experion policy settings as it may affect the operation of Experion.

To edit a group policy, choose **Administrative Tools > Group Policy Management**, locate the policy to be edited under **Forest > Domains ><<your domain>>Group Policy Objects**, and then right-click and select **Edit**.

For more information, refer to the following Microsoft documentation-

http://technet.microsoft.com/en-us/library/cc759123(WS.10).aspx.

Copy a group policy

A copy operation is used for transferring settings from an existing Group Policy object in Active Directory into a new GPO. The new GPO is given a Globally Unique Identifier (GUID) and is unlinked. You can copy GPOs in the same domain, another domain in the same forest, or a domain in another forest. However, if you want to copy GPOs across domains, ensure that trust is mutually established between the domains. You can use the GPMC to copy GPOs. To understand more about copying GPOs, refer to the following Microsoft documentation — http://technet.microsoft.com/en-us/library/cc785936(WS.10).aspx.

To copy a group policy

1. Open **Administrative Tools > Group Policy Management**.
2. Find the policy to be copied under **Forest > Domains** > <<your domain>> **Group Policy Objects** , right-click and select **Copy**.
3. Right-click **Group Policy Objects**, click **Paste**, and then rename the copied policy as appropriate.
   For more information on copying a group policy, refer to the following Microsoft documentation: http://technet.microsoft.com/en-us/library/cc758287(WS.10).aspx

Move a group policy from the default domain to OUs

1. Open **Administrative Tools > Group Policy Management**, find the policy to be moved under **Forest > Domains > [your domain]**.
2. To unlink the GPO from the domain, right-click the GPO under the domain and choose **Delete**.

   Attention

   When unlinking a GPO, do NOT delete the object from the Group Policy Objects, as this deletes the GPO. Deleting the GPO from under the domain (or an OU) deletes the link to the object, and not the object itself.

3. Link the GPO to the OU as follows:
   a. Right-click the OU to which the policy should be linked, and then click **Link and Existing GPO**.
   b. In the **Select GPO** dialog box, select the policy to link and click **OK**.

Tip

For more information about working with group policies, refer to the following Microsoft documentation.

http://technet.microsoft.com/en-us/library/cc783034(WS.10).aspx

9.2 Creating mutually trusted domains

Mutually trusting domains are created by configuring the primary domain controllers on two connected domains to trust the partner domain. To set up mutually trusting domains, each domain must trust the other domain and each domain must know what other domains trust it. The process for defining these relationships is to create a trusted domain and to create a trusting domain. A trusted domain is a domain that is trusted by the domain that is being configured. A trusting domain is a domain that trusts the domain that is being configured.

Configuring mutually trusting domains is required only if the CDA-SP service (ACE) is on a different domain to an OPC server. Mutually trusting domains are created by configuring the domain controllers on two connected domains to trust the partner domain.

To set up mutually trusting domains, ensure that both domain controllers are configured using the appropriate procedure.

Attention

Creating a trust between two domains requires name resolution to be setup so that both domains can resolve the other domain name. An example of this is setting up a secondary DNS zone for the other domain.

If you are setting mutually trusted domains to support a control configuration such as the CDA-SP service (ACE) on a different domain to an OPC server, consult your nearest Honeywell representatives for additional configration requirements.

To create mutually trusted domains

1. Click **Start**, right-click on **Computer**, and then click **Manage**.
2. If prompted, click **Continue** in the **User Account Control** dialog box.
3. Expand **Roles**, and then click **Active Directory Domain Services**.
4. In the right pane, locate **Advanced Tools**. To see the advanced options, click the arrow next to **Advanced Tools**.
5. Click **AD Domains and Trusts**.
   The **Active Directory Domains and Trust** window appears.
6. Expand the **Active Directory Domains and Trust** item, right-click the local domain name, and then click **Properties**.
7. Click the **Trusts** tab.
8. Click **New Trust**.
   The **New Trust Wizard** appears.
9. In the **Trust Name** box, type the name of the other domain, and then click **Next**.
10. In the **Trust Type** box, select **External Trust for Windows 2008 to Windows 2003 and Forest Trust for Windows 2008 to Windows 2008**, and then click **Next**.
11. In the **Direction of Trust** box, select **Two-Way**, and then click **Next**.
12. In the **Sides of Trust** box, select **Both this Domain and the specified domain**, then click **Next**.
13. In the **User Name and Password** boxes, enter the credentials of domain account for the other domain, and then click **Next**.
14. In the **Outgoing Trust Authentication Level-Local Domain** page, select **Domain-wide authentication**, and then click **Next**.
15. In the **Trust Selections Complete** page, click **Next**.
16. In the **Confirm Outgoing Trust** page, select **Yes** to confirm the outgoing trust, and then click **Next**.
17. In the **Confirm Incoming Trust** page, select **Yes** to confirm the incoming trust and then click **Next**.
18. In the **Completing the New Trust Wizard** page, click **Finish**.

9.3 Renaming a domain controller

You can rename a domain controller for the following reasons.

- To restructure your network for organizational and business needs
- To make management and administrative control easier

Renaming must be done without interruptions to the domain controller. The recommended practice for renaming a domain controller without interruption to clients is to use the **Netdom** tool. However, there would be a temporary interruption when the domain controller is restarted after a rename.

Tip

For more information about renaming a domain controller, refer to the following Microsoft documentation:

http://technet.microsoft.com/en-us/library/cc782761(WS.10).aspx

9.4 Removing a domain controller

Removing a domain controller implies removing the domain controller role on the server and removing the domain controller from the domain. This task is referred to as demoting a domain controller. For detailed instructions about demoting a domain controller, refer to the section “Demoting a domain controller” in the *Windows Domain Implementation Guide for Microsoft Windows Server 2008 R2*.

For more information about demoting a domain controller, refer to the following Microsoft documentation at http://technet.microsoft.com/en-us/library/cc740017(WS.10).aspx

CAUTION

- If the domain has only one domain controller, removing a domain leads to permanent loss of data (like User, Groups, and Accounts) contained in the domain. Hence, exercise caution before taking up this activity.
- As long as the domain has multiple domain controllers, no data loss should happen. Before performing this task, ensure the following:
  - If this domain controller is a GC server, ensure that another GC server is available to the users.
  - Transfer any of the operation master roles held by the domain controller to another domain controller.

10 Enabling or disabling USB-connected storage devices on Experion systems

Related topics

“Introduction” on page 66
“Installation of USB Storage Enable Disable feature using Experion PKS Installation media” on page 68
“Managing the USB Storage Enable Disable feature” on page 72

10.1 Introduction

Starting with Experion R410, an administrator can enable or disable the use of USB-connected storage devices, such as flash drive, floppy disk, CD/DVD on the Experion systems in domain or workgroup environments. However, use of other types of USB devices such as keyboards, mouse, finger print readers, and smart cards are not affected. This facility includes three type of applications that is optionally installed using the Experion PKS Installation media.

The **USB Storage Enable Disable** feature installs a set of components as detailed in the following table.

Domain/ Workgroup	Type of administration	Type of tool	Implementation	Components installed
Workgroup	Local	Local USB Control tool	Local USB Control tool is installed on each machine in a workgroup for enabling or disable use of USB-enabled devices For more information about Local USB Control tool, refer to the "Managing the USB Storage Enable Disable feature using Local USB Control tool" on page 72 procedure.	Local USB Control tool
Workgroup	Central	NA	NA	NA
Domain	Local	Local USB Control tool	Local USB Control tool is installed on each machine in a domain for enabling or disable use of USB-enabled devices For more information about Local USB Control tool, refer to the "Managing the USB Storage Enable Disable feature using Local USB Control tool" on page 72 procedure.	Local USB Control tool
Domain	Central	Manage Domain USB Policies tool	Manage Domain USB Policies tool is installed on writable domain controller. The policy files are installed from the Experion PKS Installation media on the writable domain controller. The writeable domain controller installs the policy files on each node in the domain including the RODC according to the enable or disable action. For more information about Manage Domain USB Policies tool, refer to the "Managing USB Storage Enable Disable feature using the Manage Domain USB Policies tool(individual computer management method)" on page 73 procedure.	Two policy files (Honeywell USB Storage Disable Policy and Honeywell USB Storage Enable Policy) and the Manage Domain USB Policies tool.

		Microsoft Group Policy Management Console tool	Microsoft Group Policy Management Console tool is installed on writable domain controller. This tool is available on any Windows-based system. The policy files are installed from the Experion PKS Installation media on the writable domain controller. The writeable domain controller installs the policy files on each node in the domain including the RODC according to the enable or disable action. For more information about Microsoft Group Policy Management Console tool, refer to the “Managing USB Storage Enable Disable feature using the Microsoft Group Policy Management Console tool(domain or Organization Unit (OU) management method)” on page 74 procedure.	Two policy files (Honeywell USB Storage Disable Policy and Honeywell USB Storage Enable Policy) and the Microsoft Group Policy Management Console tool.

10.2 Installation of USB Storage Enable Disable feature using Experion PKS Installation media

The USB Storage Enable Disable feature installs a default set of components depending on the node type, when installed from the Experion PKS Installation media.

Node type	Components installed
Writable domain controller	• Manage Domain USB Policies tool • Policy files • Local USB Control tool
• Non-domain controller • Read-only domain controller (RODC)	Local USB Control tool

Related topics

"Installation methods" on page 68
"Installation of USB Storage Enable Disable feature on non-domain controllers" on page 69
"Installation of USB Storage Enable Disable feature on domain controllers" on page 71

10.2.1 Installation methods

To start the installation for ESIS-based installations from a USB drive

1. Insert the USB pen drive or removable hard drive into the system.
2. Browse to the ESIS repository location in the USB pen drive/removable hard drive.
3. Double-click **setup.exe** at the root of the ESIS repository path.
4. On the **ESIS Welcome** screen, select **Product Installation**, if not already selected.

To start installation for ESIS-based installation from network share

1. Type `\\<ESISserver IP>\<ShareName>` in the Windows **Run** dialog box (choose Start > Run) to connect to the ESIS repository.
2. Press **ENTER**.
3. If prompted for Windows credentials, perform the following:
   a. Type the **<Domain Name>\Username** and **Password** if you belong to a domain and if you have share permissions.
   b. Type the**<ESISServer IP>\Username** and **Password** if you belong to a workgroup and if you have share permissions.
   c. Clear the **Remember Password** check box.

   Attention
   Ensure that you have same login (either domain or workgroup) for both ESIS and the migrated nodes.
4. Double-click the **setup.exe** at the root of the `\<ShareName>.`
5. If prompted for user account control, click **Allow**.
6. If you are prompted for the Windows credentials, perform the following:
   a. Type the **<Domain Name>\Username** and **Password** if you belong to a domain and if you have share permissions.
   b. Type the **<ESISServer IP>\Username** and **Password** if you belong to a domain and if you have share permissions.

c Clear the **Remember Password** check box.

> **Attention**
> If you enter incorrect credentials, an error occurs after the first reboot of Experion installation or migration. Then, you have to enter the correct credentials to connect to the ESIS share.

7 On the **ESIS Welcome** screen, select **Product Installation**, if not already selected.

To start installation from Experion PKS Installation media

1 Insert the Experion PKS Installation media into the DVD drive.

2 If the **Honeywell Experion PKS Installer** screen does not appear, using Windows Explorer, go to the browser folder on the Experion PKS Installation media, and double-click the **cdbrowse.exe** file.

10.2.2 Installation of USB Storage Enable Disable feature on non-domain controllers

To install USB Storage Enable Disable feature along with Experion installation

1 On the **Honeywell Experion PKS Installer** page, click **Install/Migrate Experion PKS** to begin installation.
The **Welcome to the Honeywell Experion PKS Installation Setup** wizard is displayed.

2 Read the information on the page, and click **Next**.
The **Experion PKS Dialog manager** is displayed.

3 Select **Install Clean** and click **Next**.
The **License Agreement** page is displayed.

4 Read the license terms carefully before accepting the terms in the license agreement and then select **I accept the terms in the License agreement**. Click **Next**.
The **Setup type of Node to install** page is displayed.

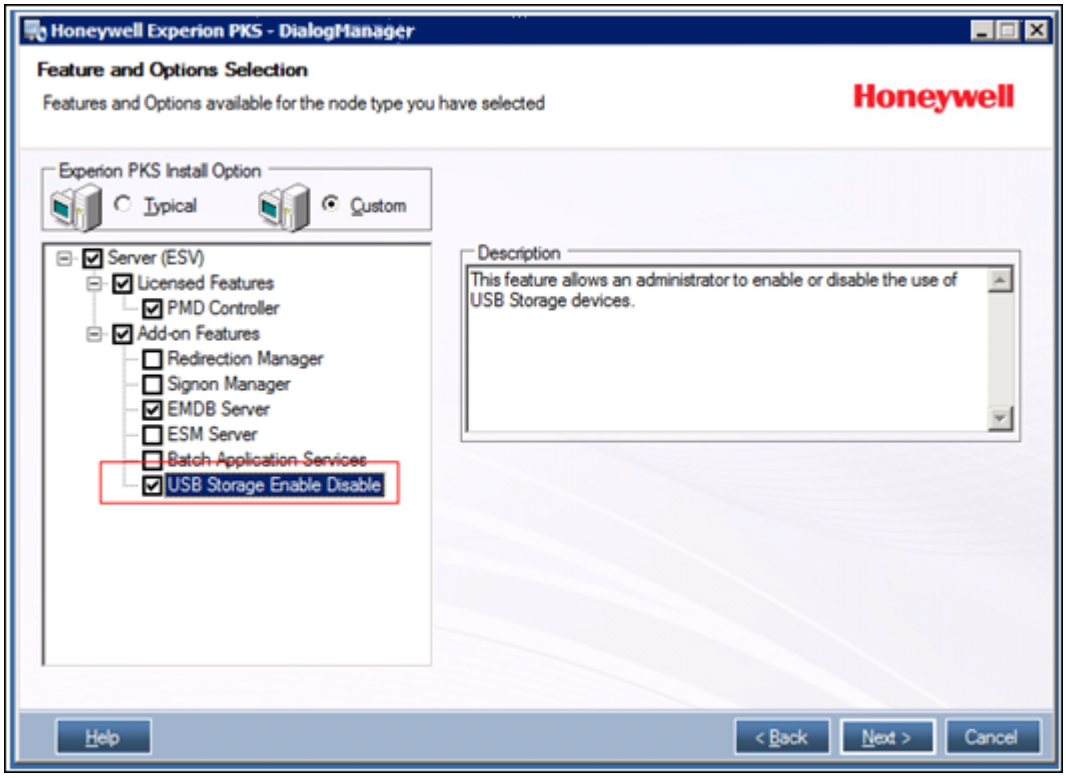
5 Click **Next**.
The **User and License Information** page is displayed.

6 Specify the customer name and company name in the **Name**, **Company Name**,**System Number** and , **Authorization** fields respectively and click **Next**.
The **Installation Path(s) Selection** page is displayed.

7 Click **Next**.
The **Experion Network Selection** page is displayed.

8 Click **Next**.
The **FTE Bootp and NTP IP Address Configuration** page is displayed.

9 Click **Next**.
The **Feature and Options Selection** page is displayed.



10 In the **Feature and Options Selection** page, select the **USB Storage Enable Disable** check box, and click **Next**.

11 Follow the on-screen instructions, and complete the Experion installation.

On completion of Experion installation, the **USB Storage Enable Disable** feature is installed.

To install USB Storage Enable Disable feature after Experion installation

1 On the **Honeywell Experion PKS Installer** page, click **Install/Migrate Experion PKS** to begin installation.

Attention

- Click **Yes** if a **User Account Control** page is displayed.
- If **Honeywell Experion PKS Installer** screen does not appear, using Windows Explorer browse to the drive (or folder) and run **setup.exe** at the root of the media to start the Installer

The **Welcome to the Honeywell Experion PKS Installation Setup** wizard is displayed.

2 Click **Yes** to continue installation of Experion.

The **License Agreement** page is displayed.

3 Read the license terms carefully before accepting the terms in the license agreement and then select **I accept the terms in the License agreement**. Click **Next**.

The **Setup type of Node to install** page is displayed.

4 Select **Optional Features** and click **Next**.

The **User and License Information** page is displayed.

5 Specify the customer name and company name in the **Name** and **Company Name** fields respectively, and click **Next**.

The **Installation Path(s) Selection** page is displayed.

6 Click **Next**.

The **Feature and Options Selection** page is displayed.

7 In the **Feature and Options Selection** page, select the **USB Storage Enable Disable** option, and click **Next**.

8 Follow the on-screen instructions, and complete the Experion installation.
The **Summary** page is displayed which lists the options selected for installation.

9 Click **Install**.
The **Status Display** page is displayed.

10 After installation is complete, click **Yes** to restart the node.

10.2.3 Installation of USB Storage Enable Disable feature on domain controllers

1 On the **Honeywell Experion PKS Installer** page, click **Install/Migrate Experion PKS** to begin installation.
The **Setup** dialog box is displayed, prompting for domain policies installation.

2 Click **Yes** to install Experion domain policies. Follow the on-screen instructions to complete the installation.
After the installation is complete, the **Setup** dialog box is displayed again, prompting for .NET 3.5 installation.

3 Click **Yes** to install .NET 3.5 on the domain controller.
After the installation completes, the **Welcome to the Honeywell Experion PKS Installation Setup Wizard** is displayed.

4 Click **Next** to continue installation of Experion.
The **License Agreement** page is displayed.

5 Read the license terms carefully before accepting the terms in the license agreement and then select **I accept the terms in the License agreement**. Click **Next**.
The **Setup type of Node to install** page is displayed.

6 Select **Optional Features**, and click **Next**.
The **User and License Information** page is displayed.

7 Specify the customer name and company name in the **Name** and **Company Name** fields respectively.

> **Attention**
> Do not enter "&" (ampersand) in the **Name** and **Company Name** fields.

8 Click **Next**.
The **Features and Options Selection** page is displayed.

9 In the **Features and Options Selection** page, select the **USB Storage Enable Disable** option, and click **Next**.
The **Experion PKS Software Installation Settings** page is displayed.

10 Review the summary of the settings you have selected in the installation page and click **Install**.
The **Experion PKS Status Display** page is displayed, where the status of the **USB Storage Enable Disable** feature is shown in the left pane.

11 After the installation is complete, the **Install Complete** message is displayed. Click **OK** to restart the system.

10.3 Managing the USB Storage Enable Disable feature

Related topics

"Managing the USB Storage Enable Disable feature using Local USB Control tool" on page 72

"Managing USB Storage Enable Disable feature using the Manage Domain USB Policies tool(individual computer management method)" on page 73

"Managing USB Storage Enable Disable feature using the Microsoft Group Policy Management Console tool(domain or Organization Unit (OU) management method)" on page 74

10.3.1 Managing the USB Storage Enable Disable feature using Local USB Control tool

Prerequisites

- You must logon as *local administrator* or *domain administrator* to use this tool.
- A reboot is NOT required to complete the configuration.
- The disable of USB storage devices is effective only when there are no USB storage devices plugged in. If there are such devices plugged in at the time that disable is configured, the disable does not become effective until all such storage devices are removed.
- If a USB storage device is plugged in at the time that the configuration is changed to enable, the device must be removed and reinserted before it starts working.
- If this Local USB Control tool is used on a machine that is controlled by the domain policies (central), this tool changes the configuration immediately, but the domain policy reasserts itself at the next policy refresh opportunity.

To enable USB-connected storage devices

1 Choose **All Programs** > **Honeywell Experion PKS** > **System Management** > **Local USB Control**.
The **Local USB Control** dialog box is displayed.

2 Select the **Allow use of USB storage devices on this computer** option to enable the use of USB Storage devices on the computer.

3 Click **Apply**, and then click **OK**.
The USB storage devices are enabled on this computer.

To disable use of USB storage devices

1 Choose **All Programs** > **Honeywell Experion PKS** > **System Management** > **Local USB Control**.
The **Local USB Control** dialog box is displayed.

2 Clear the **Allow use of USB storage devices on this computer** option to disable the use of USB Storage devices on the computer.

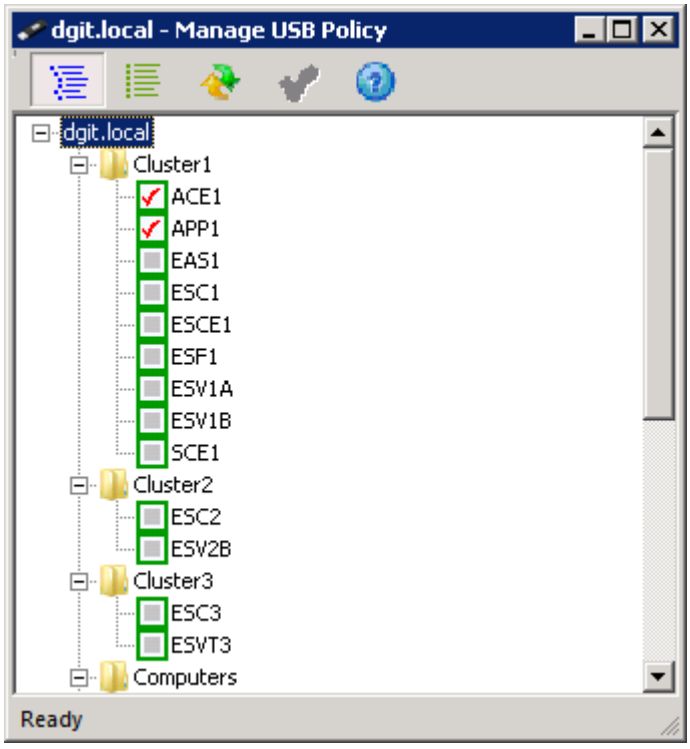
3 Click **Apply**, and then click **OK**.
The USB storage devices are disabled on this computer.

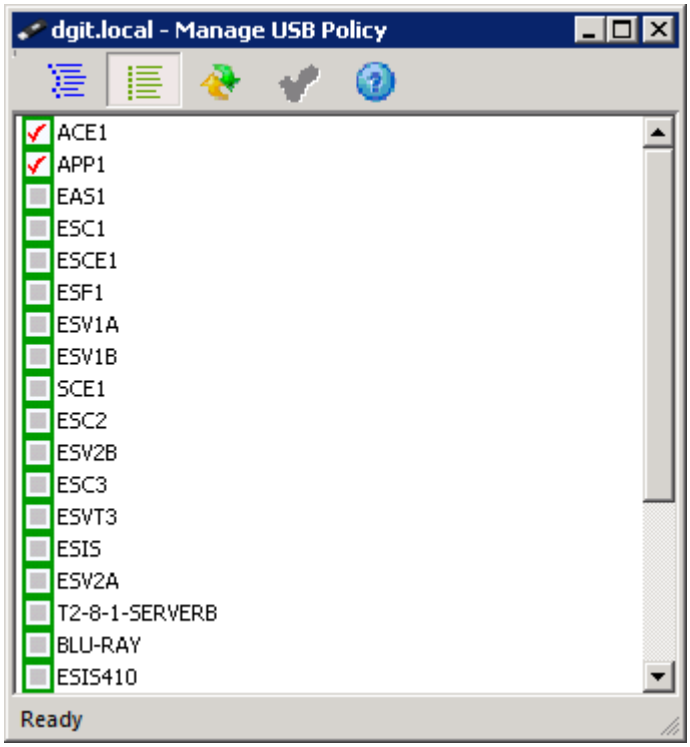
10.3.2 Managing USB Storage Enable Disable feature using the Manage Domain USB Policies tool(individual computer management method)

To enable or disable USB Storage Enable Disable feature using the Manage Domain USB Policies tool

1 Choose **Start** > **All Programs** > **Honeywell Experion PKS** > **System Management** > **Manage Domain USB Policies**.
The **Manage USB Policy** page is displayed.

2 The **Manage USB Policy** page is displayed in one of the following formats.

Format	Description
	Computers grouped as per the organization unit. This list includes all the computers in the domain but are grouped according to the organization unit they belong to.

Format	Description
	Computers organized in alphabetical order. This list includes all the computer in the domain.

3 Perform one of the following to apply **Honeywell USB Storage Enable/Disable Policy** on your computer.

Option	Procedure
To apply Honeywell USB Storage Enable Policy to a node.	1. Select the check box next to the required computer(s). 2. Click **Refresh**. The **Honeywell USB Storage Enable Policy** is applied and the Apply check mark appears for the selected computer(s).
To apply Honeywell USB Storage Disable Policy to a node.	1. Clear the check box next to the required computer. 2. Click **Refresh**. The **Honeywell USB Storage Disable Policy** is applied and the Apply check mark appears for the selected computer(s).

Changes that are not yet applied are indicated by showing the computer name in bold text .

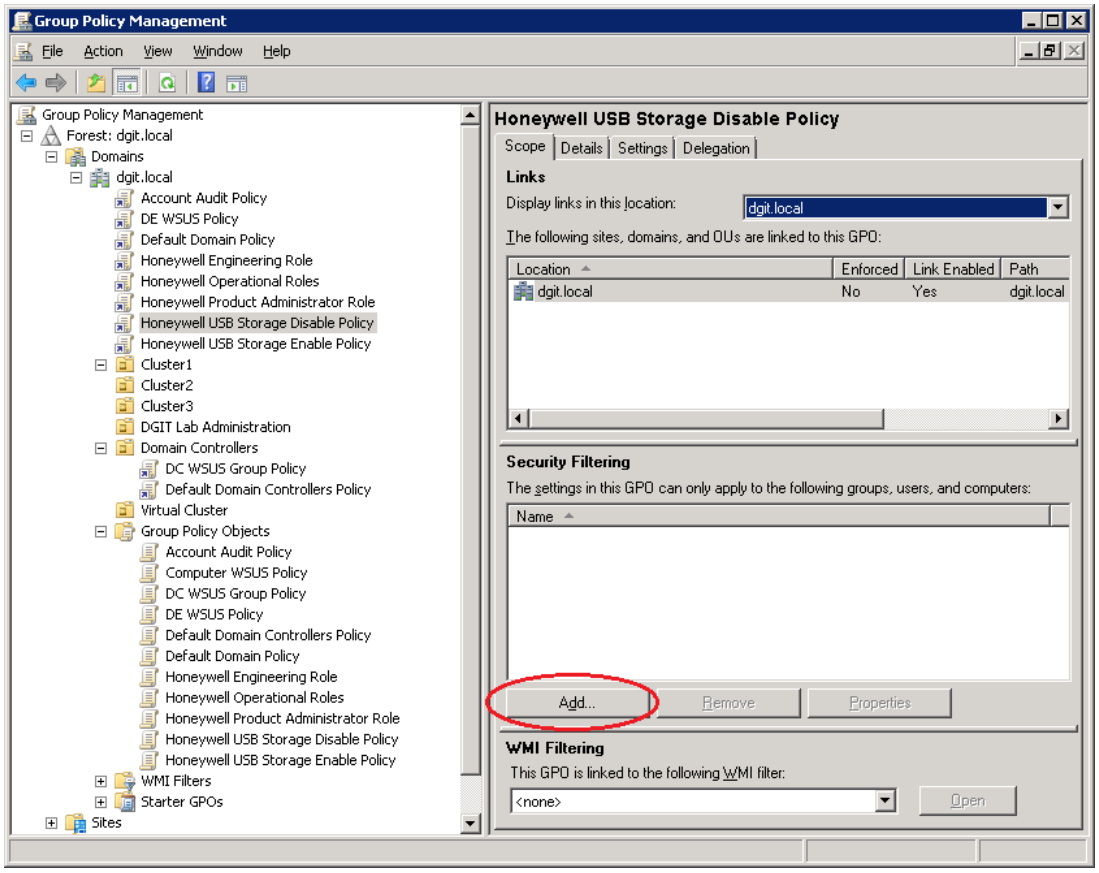
10.3.3 Managing USB Storage Enable Disable feature using the Microsoft Group Policy Management Console tool(domain or Organization Unit (OU) management method)

Considerations

Do not apply both policies to the same computer or computers as the results are inconsistent.

To disable or enable all computers in the domain

1 Choose **Start > Run**, type **gpmc.msc**, and click **OK**.
The **Group Policy Management** page is displayed.



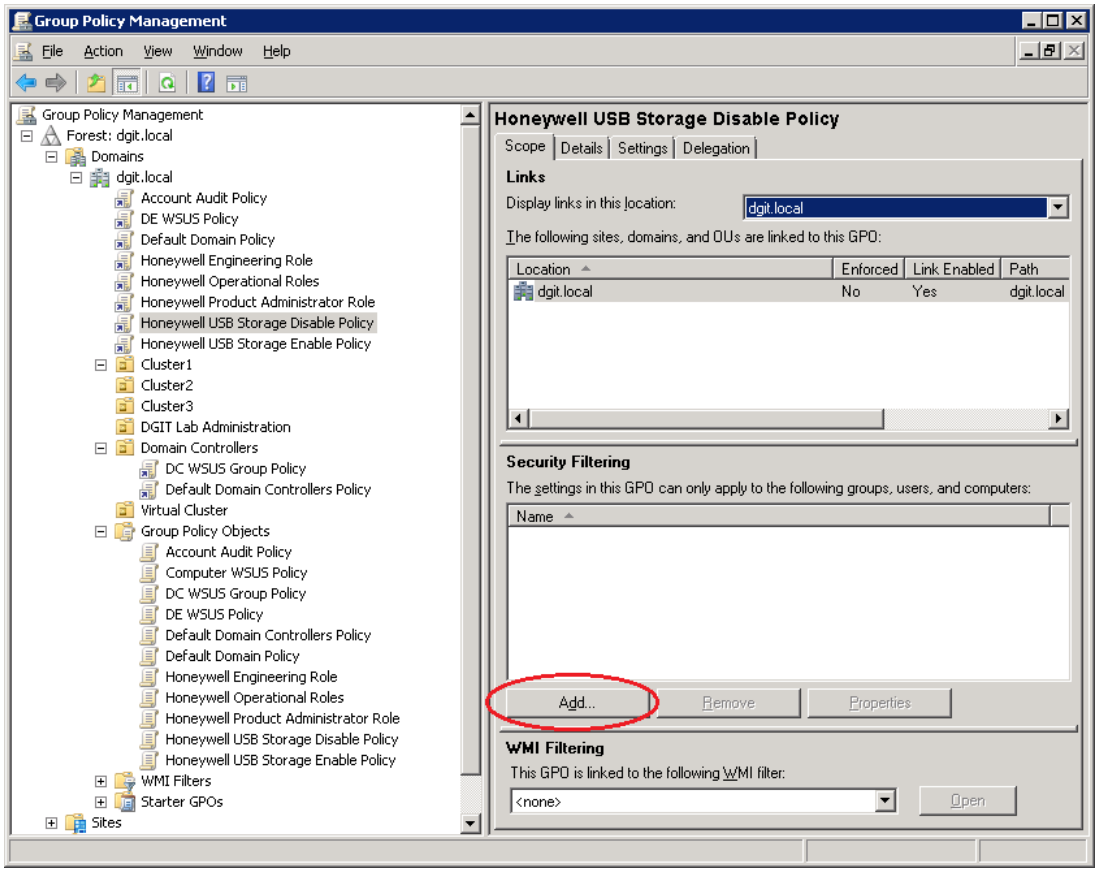
2 Perform one of the following procedures.

Option	Description
To enable USB storage devices	1. Select **Honeywell USB Storage Enable Policy** in the left pane. 2. In the **Security Filtering** list, click **Add**, and add the list of authenticated users to the security filtering list. **Attention** Do not apply both policies to the same computer or computers as the results are inconsistent.
To disable USB storage devices	1. Select **Honeywell USB Storage Disable Policy** in the left pane. 2. In the **Security Filtering** list, click **Add**, and add the list of authenticated users to the security filtering list. The next reboot, gpupdate or policy refresh interval makes the policy effective on each computer in the domain.

3 The next system restarts, **gpupdate** command or policy refresh interval makes the policy effective on each computer in the domain.

To disable or enable all computers in organizational units (OU)

1 Choose **Start > Run**, type **gpmc.msc**, and click **OK**.
The **Group Policy Management** page is displayed.



2 Click the domain name. For example, dgit.local.

3 In the right pane, where a list of policies linked at the domain level is displayed, click one of the Honeywell USB policies and then CTRL+Click on the other Honeywell USB policy.

Both the policies are highlighted.

4 Right-click one of the highlighted policies, and select **Delete** from the menu.

A message, **Do you want to delete these links?** is displayed.

5 Click **OK**.

The policies continue to show in the list of **Group Policy Objects** in the left pane, but not directly under the domain or any of the OUs.

6 With the **Group Policy Objects** list in the left pane expanded (click the + beside that title if necessary), click on the policy you want to apply on an OU.

7 Drag that policy to an OU or container in the left pane.

A message, **Do you want to link the GPOs that you have selected to this organizational unit?** is displayed.

8 Click **OK**.

9 Repeat this procedure for each OU you want to apply the policy to.

Attention

- You can apply the USB enable policy to some OUs, the USB disable to other OUs, and neither policy to yet other OUs.
- DO NOT apply both USB policies to the same OU, either directly or inherited from a containing OU.

10 After the USB policies are linked to the required OUs, apply the following procedure to both policies:

a Select the policy from the list under **Group Policy Objects** in the left pane.

b Ensure that the **Security Filtering** list on the **Scope** tab in the right pane is empty.

c Click the **Add** option, and add **Authenticated Users**.

The **Security Filtering** list now shows the entry, **Authenticated Users**.

11 After the procedure is complete for each policy being applied, restart the system. The **gpupdate** command or policy refresh interval enables/disables the policy on each computer in the linked OUs.

11 Advanced Domain administration

Related topics

“Managing security” on page 80
“DNS Recommendations for large FTE networks” on page 81

11.1 Managing security

Tip

Refer to the chapter, “Configuring System Security” in the *Experion Server and Client Configuration Guide*. Additionally, you can refer to the *Appendix* in this document.

11.2 DNS Recommendations for large FTE networks

Related topics

“Overview” on page 81
“Recommendation” on page 81

11.2.1 Overview

There are numerous DNS design strategies based on the location and layout of network resources. This section only addresses the network design recommendations for large FTE networks. In small network implementations, having one or two domain controllers running DNS will satisfy most of the network design goals. When implementing a large FTE network, especially with multiple level 2 FTE communities that communicate with a common level 3 network, the layout of DNS could affect name resolution across the entire network.

11.2.2 Recommendation

In a large FTE network, the major design goal is to minimize network traffic that needs to be routed to the level 3 network while at the same time ensuring name resolution to the local network in which the domain controller resides. To help minimize DNS traffic, there should be at least one domain controller running DNS on each level 2 FTE community and at least one domain controller running DNS on the level 3 network.

The preferred DNS server on each domain controller should be its local IP address. The alternate DNS server on each domain controller in each level 2 FTE community should be the IP address of the level 3 domain controller that is running DNS.

The computer nodes on each level 2 FTE community should have their preferred DNS server and their alternate DNS server set to the same IP addresses as the domain controller for that level 2 FTE community. This will isolate the majority of DNS traffic and domain authentication to the local domain controller in each level 2 FTE community.

Another configuration aspect that needs to be addressed is that of reverse lookup zone configuration for this type of network design. It is assumed that each level 2 FTE community and the level 3 network will have different IP networks. To ensure that reverse lookup (PTR) records are created for each host in each IP network, the initial reverse lookup zone should be larger than the single IP network.

In the following network example, all of the IP networks share a common network identifier, in this case 172.21.x.x. In this situation, the reverse lookup zone should reference 172.21 as the network ID when creating the reverse lookup zone. This will allow all of the level 2 and level 3 hosts to be contained in a single reverse lookup zone.

Level	Network
3	172.21.1.x
2	172.21.2.x
2	172.21.3.x

12 Troubleshooting Windows domain and workgroup

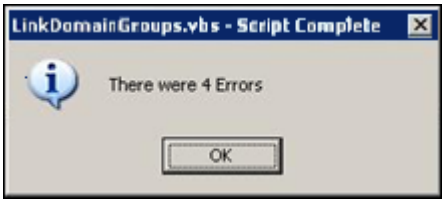
Related topics

“Backward compatibility of TPS, Experion releases and Domain Controller security” on page 84
“Troubleshooting group policy objects” on page 86

12.1 Backward compatibility of TPS, Experion releases and Domain Controller security

The following section describes an issue about differences in security groups between Experion R3xx and TPS releases and Experion R4xx.

This issue occurs in domains that contain Experion R3xx or TPS computers where the domain controller was initialized with the Experion R4xx "Honeywell Security Model – Domain Security" installed, but was not upgraded from a TPS or Experion R3xx version of that package.

Error Indication	In the specific environment noted, the "LinkDomainGroups.vbs" script running on a TPS or Experion R3xx node displays multiple error messages, **Unable to add Global Group to Local Group**. The issue results from several global groups used in TPS and Experion R3xx becoming obsolete in Experion R400.1. If only the R4xx domain security package is installed in this domain, these obsolete groups are not created, and errors result from running *LinkDomainGroups.vbs* on nodes version earlier than Experion R400. If a TPS or earlier version of the Experion domain security package was installed before upgrading the domain for Experion R4xx, the obsolete groups exist in the domain and these errors do not occur.
Cause	After *LinkDomainGroups.vbs* is started on a TPS or Experion R3xx node, four error dialogs are displayed, one at a time, with the error message, **Unable to add Global Group to Local Group**. The contents of each dialog differ in the names of the groups displayed, but are similar to the following:  In addition, the following message is displayed. 

Solution	Perform the following procedure to manually add the security groups referenced by TPS or Experion R3xx to the domain.
	1. On the domain controller, using an account that is a member of "Domain Admins".
	a. Open a Microsoft Windows command (CMD) window. This needs to be started using "Run as administrator" on Windows Server 2008 or later.
	b. Execute the following 5 commands at the command prompt.
	`net group "ER Admins" /add /comment:"Built-in Honeywell Legacy Group"`
	`net group "Point Builders" /add /comment:"Built-in Honeywell Legacy Group"`
	`net group "Intimate Users" /add /comment:"Built-in Honeywell Legacy Group"`
	`net group "Continuous Ctrls" /add /comment:"Built-in Honeywell Legacy Group"`
	`net group "Programs" /add /comment:"Built-in Honeywell Legacy Group"`
	2. On the node(s) where the error was encountered, log on using an account with domain administrator privilege, rerun the *LinkDomainGroups.vbs* script.

12.2 Troubleshooting group policy objects

12.2.1 Overview

When applying multiple GPOs against a domain object, the actual results on the domain object may not meet the required goals. In such a situation, you can use Microsoft tools to troubleshoot the interaction of multiple GPOs on a specific object. These tools can be run from a domain controller or from the client nodes exhibiting the issue.

- **Resultant Set of Policy** (RSoP) tool
- Using `gpupdate` and `gpresult`

12.2.2 Running the Resultant Set of Policy (RSoP)

The RSoP tool can be run on the client node in logging mode. When the RSoP is run on a domain controller, it can be run in logging mode or in planning mode. Logging mode displays the GPO information currently applied to the node while planning mode can simulate how a specific object will have GPOs applied to it.

To run the RSoP tool in planning mode on a domain controller

1. Log on to a domain controller with domain administrative privileges.
2. Choose **Start > Run**, type `mmc`, and then click **OK**.
   The Microsoft Management Console opens.
3. If the **User Account Control** dialog box appears, click **Yes**.
4. Choose **File > Add/Remove Snap-in**.
   The **Add/Remove Snap-in** dialog box appears.
5. Click **Add**.
   The **Add Standalone Snap-in** dialog box appears.
6. Select **Resultant Set of Policy**, and then click **Add**.
7. Click **OK**.
   The **Resultant Set of Policy snap-in** is added to the console.
8. In the left pane, right-click **Resultant Set of Policy**, and then select **Generate RSoP data**.
   The **Resultant Set of Policy Wizard** appears.
9. Click **Next**.
10. In the **Mode selection** dialog box, choose **Planning Mode**, and then click **Next**.
11. In the **User and Computer selection** dialog box, change the user information to **User** and the computer information to **Computer**.
12. Under **User**, click **Browse**.
13. Enter the required user name (that is, operator), and then click **Check Names**.
    If the domain user exists, it will be underlined.
14. Click **OK**.
15. Under **Computer**, click **Browse**.
    If the computer exists, it will be underlined.
16. Click **OK**.
17. Select **Skip to final page of this wizard with collecting additional data**, and then click **Next**.
18. To start the simulation, click **Next**.

19 To view the results of the simulation, click **Finish**.

12.2.3 Using gpupdate and gpresult

gpupdate

When making changes to group policies, it may be necessary to apply the changes immediately without waiting for the default update interval to elapse. The update interval for domain members is 90 minutes, and for domain controllers, the interval is 5 minutes. Gpupdate is a command line utility that is used to force an update change on local computers.

The following are some examples of how to use gpupdate:

- gpupdate with no switches will update both computer and user policies on the local machine. Note that this will reapply policy settings that are changed.
- gpupdate /force using the force switch will reapply all policy settings

A complete list of switches is outlined in the following article.

http://technet.microsoft.com/en-us/library/cc739112(WS.10).aspx

Gpupdate can also be executed remotely through the use of psexec.exe from Sysinternals. For more information, see the following article.

http://support.microsoft.com/kb/556027

Note that this is listed as a suggestion but has not been qualified by Honeywell.

gpresult

gpresult is a command line utility that displays the currently enforced policies on a computer. The utility can be run either locally or remotely. The gpresult tool displays the RSoP for the last logged on user on the machine. The following are some examples of using gpresult.

- gpresult with no switches will display the local RSoP data for the currently logged in user.
- gpresult /s computername where computername is the name of the computer, displays the current RSoP that is enforced on the remote computer with the currently logged in user.

A complete list of switches is outlined in the following article.

http://technet.microsoft.com/en-us/library/cc756960(WS.10).aspx

13 Appendix

Related topics

“Experion domain group policy settings” on page 90
“Security Model specific permissions” on page 143

13.1 Experion domain group policy settings

Policy settings related to Operating System releases		Applicable operating system	Description
Path::Setting	**Affected roles**		
\Control Panel::Prohibit access to the Control Pane	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Disables all Control Panel programs and prevents Control.exe (the program file for Control Panel) from starting. This setting also removes Control Panel from the Start menu and Control Panel folder from Windows Explorer. If users try to select a Control Panel item from the Properties item on a shortcut menu, a message appears explaining that a setting prevents the action.
\Control Panel\Add or Remove Programs::Go directly to Components Wizard	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from using Add or Remove Programs to configure installed services. This setting removes the "Set up services" section of the Add/Remove Windows Components page. The "Set up services" section lists system services that have not been configured and offers users easy access to the configuration tools. If you disable this setting or do not configure it, "Set up services" appears only when there are no configured system services. If you enable this setting, "Set up services" never appears. This setting does not prevent users from using other methods to configure services. **Note:** When "Set up services" does not appear, clicking the Add/Remove Windows Components button starts the Windows Component Wizard immediately. This is because, the only option remaining on the Add/Remove Windows Components page starts the wizard, that option is selected automatically, and the page is bypassed. To remove "Set up services" and prevent the Windows Component Wizard from starting, enable the "Hide Add/ Remove Windows Components page" setting. If the "Hide Add/Remove Windows Components page" setting is enabled, this setting is ignored.

\Control Panel\Add or Remove Programs::Hide Add New Programs page	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes the Add New Programs button from the Add or Remove Programs bar. As a result, users cannot view or change the attached page. The Add New Programs button lets users install programs published or assigned by a system administrator. If you disable this setting or do not configure it, the Add New Programs button is available to all users. This setting does not prevent users from using other tools and methods to install programs.
\Control Panel\Add or Remove Programs::Hide Add/Remove Windows Components page	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes the Add/Remove Windows Components button from the Add or Remove Programs bar. As a result, users cannot view or change the associated page. The Add/Remove Windows Components button lets users configure installed services and use the Windows Component Wizard to add, remove, and configure components of Windows from the installation files. If you disable this setting or do not configure it, the Add/ Remove Windows Components button is available to all users. This setting does not prevent users from using other tools and methods to configure services, add, or remove program components. However, this setting blocks user access to the Windows Component Wizard.
\Control Panel\Add or Remove Programs::Hide Change or Remove Programs page	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes the Change or Remove Programs button from the Add or Remove Programs bar. As a result, users cannot view or change the attached page. The Change or Remove Programs button lets users uninstall, repair, add, or remove features of installed programs. If you disable this setting or do not configure it, the Change or Remove Programs page is available to all users. This setting does not prevent users from using other tools and methods to delete or uninstall programs.
\Control Panel\Add or Remove Programs::"Hide the ""Add a program from CD-ROM or floppy disk"" option"	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes the "Add a program from CD-ROM or floppy disk" section from the Add New Programs page. This prevents users from using Add or Remove Programs to install programs from removable media. If you disable this setting or do not configure it, the "Add a program from CD-ROM or floppy disk" option is available to all users. This setting does not prevent users from using other tools and methods to add or remove program components. **Note:** If the "Hide Add New Programs page" setting is enabled, this setting is ignored. In addition, if the "Prevent removable media source for any install" setting (located in User Configuration\Administrative Templates\Windows Components\Windows Installer) is enabled, users cannot add programs from removable media, regardless of this setting.

\Control Panel\Add or Remove Programs::"Hide the ""Add programs from Microsoft"" option"	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes the "Add programs from Microsoft" section from the Add New Programs page. This setting prevents users from using Add or Remove Programs to connect to Windows Update. If you disable this setting or do not configure it, "Add programs from Microsoft" is available to all users. This setting does not prevent users from using other tools and methods to connect to Windows Update. **Note:** If the "Hide Add New Programs page" setting is enabled, this setting is ignored.
\Control Panel\Add or Remove Programs::"Hide the ""Add programs from your network"" option"	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from viewing or installing published programs. This setting removes the "Add programs from your network" section from the Add New Programs page. The "Add programs from your network" section lists published programs and provides an easy way to install them. Published programs are those programs that the system administrator has explicitly made available to the user with a tool such as Windows Installer. Typically, system administrators publish programs to notify users that the programs are available, to recommend their use, or to enable users to install them without having to search for installation files. If you enable this setting, users cannot tell which programs have been published by the system administrator, and they cannot use Add or Remove Programs to install published programs. However, they can still install programs by using other methods, and view and install assigned (partially installed) programs that are offered on the desktop or on the Start menu. If you disable this setting or do not configure it, "Add programs from your network" is available to all users. **Note:** If the "Hide Add New Programs page" setting is enabled, this setting is ignored.
\Control Panel\Add or Remove Programs::Remove Add or Remove Programs	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from using Add or Remove Programs. This setting removes Add or Remove Programs from Control Panel and removes the Add or Remove Programs item from menus. Add or Remove Programs lets users install, uninstall, repair, add, and remove features and components of Windows and a wide variety of Windows programs. Programs published or assigned to the user appear in Add or Remove Programs. If you disable this setting or do not configure it, Add or Remove Programs is available to all users. When enabled, this setting takes precedence over the other settings in this folder. This setting does not prevent users from using other tools and methods to install or uninstall programs.

\Control Panel\Add or Remove Programs::Remove Support Information	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes links to the Support Info dialog box from programs on the Change or Remove Programs page. Programs listed on the Change or Remove Programs page can include a "Click here for support information" hyperlink. When clicked, the hyperlink opens a dialog box that displays troubleshooting information, including a link to the installation files and data that users need to obtain product support, such as the Product ID and version number of the program. The dialog box also includes a hyperlink to support information on the Internet, such as the Microsoft Product Support Services Web page. If you disable this setting or do not configure it, the Support Info hyperlink appears. **Note:** Not all programs provide a support information hyperlink.
\Control Panel \Display::Disable the Display Control Panel	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	Disables Display in Control Panel. If you enable this setting, Display in Control Panel does not run. When users try to start Display, a message appears explaining that a setting prevents the action. Also, see the "Prohibit access to the Control Panel" (User Configuration\Administrative Templates\Control Panel) and "Remove programs on Settings menu" (User Configuration\Administrative Templates\Start Menu & Taskbar) settings.
\Control Panel \Display::Hide Appearance and Themes tab	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	Removes the Appearance and Themes tabs from Display in Control Panel. When this setting is enabled, it removes the desktop color selection option from the Desktop tab. This setting prevents users from using Control Panel to change the colors or color scheme of the desktop and windows. If this setting is disabled or not configured, the Appearance and Themes tabs are available in Display in Control Panel.
\Control Panel \Display::Hide Desktop tab	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	Removes the Desktop tab from Display in Control Panel. This setting prevents users from using Control Panel to change the pattern and wallpaper on the desktop. Enabling this setting also prevents the user from customizing the desktop by changing icons or adding new Web content through Control Panel.

\Control Panel \Display::Hide Screen Saver tab	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	Removes the Screen Saver tab from Display in Control Panel. This setting prevents users from using Control Panel to add, configure, or change the screen saver on the computer.
\Control Panel \Display::Hide Settings tab	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the Settings tab from Display in Control Panel. This setting prevents users from using Control Panel to add, configure, or change the display settings on the computer.
\Control Panel \Display::Prevent changing wallpaper	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	Prevents users from adding or changing the background design of the desktop. By default, users can use the Desktop tab of Display in Control Panel to add a background design (wallpaper) to their desktop. If you enable this setting, the Desktop tab still appears, but all options on the tab are disabled. To remove the Desktop tab, use the "Hide Desktop tab" setting. To specify wallpaper for a group, use the "Desktop Wallpaper" setting. **Note:** You must also enable the "Desktop Wallpaper" setting to prevent users from changing the desktop wallpaper. Refer to KB article: Q327998 for more information. Also, see the "Allow only bitmapped wallpaper" setting.

\Control Panel \Display::Screen Saver	Operational Roles is disabled	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	Enables desktop screen savers. If you disable this setting, screen savers do not run. In addition, this setting disables the Screen Saver section of the Screen Saver tab in Display in Control Panel. As a result, users cannot change the screen saver options. If you do not configure it, this setting has no effect on the system. If you enable it, a screen saver runs, provided the following two conditions hold: First, a valid screensaver on the client is specified through the "Screensaver executable name" setting or through Control Panel on the client computer. Second, the screensaver timeout is set to a nonzero value through the setting or Control Panel. Also, see the "Hide Screen Saver tab" setting.
\Control Panel\Display \Desktop Themes::Prevent selection of windows and buttons styles	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from changing the visual style of the windows and buttons displayed on their screens. When enabled, this setting disables the "Windows and buttons" drop-down list on the Appearance tab in Display Properties.
\Control Panel\Display \Desktop Themes::Prohibit selection of font size	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from changing the size of the font in the windows and buttons displayed on their screens. If this setting is enabled, the "Font size" drop-down list on the Appearance tab in Display Properties is disabled. If you disable or do not configure this setting, a user may change the font size using the "Font size" drop-down list on the Appearance tab.
\Control Panel\Display \Desktop Themes::Prohibit Theme color selection	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	This setting forces the theme color to be the default color scheme. If you enable this setting, a user cannot change the color scheme of the current desktop theme. If you disable or do not configure this setting, a user may change the color scheme of the current desktop theme.
\Control Panel\Display \Desktop Themes::Remove Theme option	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	This setting effects the Themes tab that controls the overall appearance of windows. It is accessed through the Display icon in Control Panel. Using the options under the Themes tab, users can configure the theme for their desktop. If you enable this setting, it removes the Themes tab. If you disable or do not configure this setting, there is no effect. **Note:** If you enable this setting but do not set a theme, the theme defaults to whatever the user previously set.

\Control Panel \Personalization::Enable screen saver	Operational Roles is disabled	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Enables desktop screen savers. If you disable this setting, screen savers do not run. In addition, this setting disables the Screen Saver section of the Screen Saver dialog in the Personalization or Display Control Panel. As a result, users cannot change the screen saver options. If you do not configure it, this setting has no effect on the system. If you enable it, a screen saver runs, provided the following two conditions hold: First, a valid screen saver on the client is specified through the "Screen Saver executable name" setting or through Control Panel on the client computer. Second, the screen saver timeout is set to a nonzero value through the setting or Control Panel. Also, see the "Prevent changing Screen Saver" setting.
\Control Panel \Personalization::Prevent changing color scheme	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This setting forces the theme color scheme to be the default color scheme. If you enable this setting, a user cannot change the color scheme of the current desktop theme. If you disable or do not configure this setting, a user may change the color scheme of the current desktop theme. For Windows 7 and later, use the "Prevent changing window color and appearance" setting.
\Control Panel \Personalization::Prevent changing desktop background	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from adding or changing the background design of the desktop. By default, users can use the Desktop Background page in the Personalization or Display Control Panel to add a background design (wallpaper) to their desktop. If you enable this setting, none of the Desktop Background settings can be changed by the user. To specify wallpaper for a group, use the "Desktop Wallpaper" setting. **Note:** You must also enable the "Desktop Wallpaper" setting to prevent users from changing the desktop wallpaper. Refer to KB article: Q327998 for more information. Also, see the "Allow only bitmapped wallpaper" setting.

\Control Panel \Personalization::Prevent changing desktop icons	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from changing the desktop icons. By default, users can use the Desktop Icon Settings dialog in the Personalization or Display Control Panel to show, hide, or change the desktop icons. If you enable this setting, none of the desktop icons can be changed by the user. For systems prior to Windows Vista, this setting also hides the Desktop tab in the Display Control Panel
\Control Panel \Personalization::Prevent changing mouse pointers	Operational Roles	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from changing the mouse pointers. By default, users can use the Pointers tab in the Mouse Control Panel to add, remove, or change the mouse pointers. If you enable this setting, none of the mouse pointer scheme settings can be changed by the user
\Control Panel \Personalization::Prevent changing screen saver	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents the Screen Saver dialog from opening in the Personalization or Display Control Panel. This setting prevents users from using Control Panel to add, configure, or change the screen saver on the computer. It does not prevent a screen saver from running
\Control Panel \Personalization::Prevent changing sounds	Operational Roles	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from changing the sound scheme. By default, users can use the Sounds tab in the Sound Control Panel to add, remove, or change the system Sound Scheme. If you enable this setting, none of the Sound Scheme settings can be changed by the user

\Control Panel \Personalization::Prevent changing theme	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	This setting disables the theme gallery in the Personalization Control Panel. If you enable this setting, users cannot change or save a theme. Elements of a theme such as the desktop background, window color, sounds, and screen saver can still be changed (unless policies are set to turn them off). If you disable or do not configure this setting, there is no effect. **Note:** If you enable this setting but do not specify a theme using the "load a specific theme" setting, the theme defaults to whatever the user previously set or the system default
\Control Panel \Personalization::Prevent changing visual style for windows and buttons	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users or applications from changing the visual style of the windows and buttons displayed on their screens. When enabled on Windows XP, this setting disables the "Windows and buttons" drop-down list on the Appearance tab in Display Properties. When enabled on Windows XP and later systems, this setting prevents users and applications from changing the visual style through the command line. Also, a user may not apply a different visual style when changing themes
\Control Panel \Personalization::Prevent changing window color and appearance	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Disables the Window Color page in the Personalization Control Panel, or the Color Scheme dialog in the Display Control Panel on systems where the Personalization feature is not available. This setting prevents users from using Control Panel to change the glass color, system colors, or color scheme of the desktop and windows. If this setting is disabled or not configured, the Window Color page or Color Scheme dialog is available in the Personalization or Display Control Panel. For systems prior to Windows Vista, this setting hides the Appearance and Themes tabs in the in Display in Control Panel
\Control Panel \Personalization::Prohibit selection of visual style font size	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from changing the size of the font in the windows and buttons displayed on their screens. If this setting is enabled, the "Font size" drop-down list on the Appearance tab in Display Properties is disabled. If you disable or do not configure this setting, a user may change the font size using the "Font size" drop-down list on the Appearance tab

\Control Panel \Printers::Browse the network to find printers	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Allows users to use the Add Printer Wizard to search the network for shared printers. If you enable this setting or do not configure it, when users choose to add a network printer by selecting the "A network printer, or a printer attached to another computer" radio button on Add Printer Wizard's page 2, and also check the "Connect to this printer (or to browse for a printer, select this option and click Next)" radio button on Add Printer Wizard's page 3, and do not specify a printer name in the adjacent "Name" edit box, then Add Printer Wizard displays the list of shared printers on the network and invites to choose a printer from the shown list. If you disable this setting, the network printer browse page is removed from within the Add Printer Wizard, and users cannot search the network but must type a printer name. **Note:** This setting affects the Add Printer Wizard only. It does not prevent users from using other programs to search for shared printers or to connect to network printers.
\Control Panel \Printers::Prevent addition of printers	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from using familiar methods to add local and network printers. This setting removes the Add Printer option from the Start menu. (To find the Add Printer option, click Start, click Printers, and then click Add Printer.) This setting also removes Add Printer from the Printers folder in Control Panel. In addition, users cannot add printers by dragging a printer icon into the Printers folder. If they try, a message appears explaining that the setting prevents the action. However, this setting does not prevent users from using the Add Hardware Wizard to add a printer. Nor does it prevent users from running other programs to add printers. This setting does not delete printers that users have already added. However, if users have not added a printer when this setting is applied, they cannot print. **Note:** You can use printer permissions to restrict the use of printers without specifying a setting. In the Printers folder, right-click a printer, click Properties, and then click the Security tab. If this policy is disabled, or not configured, users can add printers using the methods described above

\Control Panel \Printers::Prevent deletion of printers	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from deleting local and network printers. If a user tries to delete a printer, such as by using the Delete option in Printers in Control Panel, a message appears explaining that a setting prevents the action. This setting does not prevent users from running other programs to delete a printer. If this policy is disabled, or not configured, users can delete printers using the methods described previously
\Control Panel \Programs::"Hide ""Get Programs"" page"	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from viewing or installing published programs from the network. This setting prevents users from accessing the "Get Programs" page from the Programs Control Panel in Category View, Programs and Features in Classic View and the "Install a program from the network" task. The "Get Programs" page lists published programs and provides an easy way to install them. Published programs are those programs that the system administrator has explicitly made available to the user with a tool such as Windows Installer. Typically, system administrators publish programs to notify users of their availability, to recommend their use, or to enable users to install them without having to search for installation files. If this setting is enabled, users cannot view the programs that have been published by the system administrator, and they cannot use the "Get Programs" page to install published programs. Enabling this feature does not prevent users from installing programs by using other methods. Users will still be able to view and installed assigned (partially installed) programs that are offered on the desktop or on the Start menu. If this setting is disabled or is not configured, the "Install a program from the network" task to the "Get Programs" page will be available to all users. **Note:** If the "Hide Programs Control Panel" setting is enabled, this setting is ignored

\Control Panel \Programs::"Hide ""Installed Updates"" page"	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This setting prevents users from accessing "Installed Updates" page from the "View installed updates" task. "Installed Updates," allows users to view and uninstall updates currently installed on the computer. The updates are often downloaded directly from Windows Update or from various program publishers. If this setting is disabled or not configured, the "View installed updates" task and the "Installed Updates" page will be available to all users. This setting does not prevent users from using other tools and methods to install or uninstall programs
\Control Panel \Programs::"Hide ""Programs and Features"" page"	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This setting prevents users from accessing "Programs and Features" to view, uninstall, change, or repair programs that are currently installed on the computer. If this setting is disabled or not configured, "Programs and Features" will be available to all users. This setting does not prevent users from using other tools and methods to view or uninstall programs. It also does not prevent users from linking to related Programs Control Panel Features including Windows Features, Get Programs, or Windows Marketplace
\Control Panel \Programs::"Hide ""Set Program Access and Computer Defaults"" page"	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This setting removes the Set Program Access and Defaults page from the Programs Control Panel. As a result, users cannot view or change the associated page. The Set Program Access and Computer Defaults page allows administrators to specify default programs for certain activities, such as Web browsing or sending e-mail, as well as specify the programs that are accessible from the Start menu, desktop, and other locations. If this setting is disabled or not configured, the Set Program Access and Defaults button is available to all users. This setting does not prevent users from using other tools and methods to change program access or defaults. This setting does not prevent the Default Programs icon from appearing on the Start menu
\Control Panel \Programs::Hide "Windows Features"	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This setting prevents users from accessing the "Turn Windows features on or off" task from the Programs Control Panel in Category View, Programs and Features in Classic View, and Get Programs. As a result, users cannot view, enable, or disable various Windows features and services. If this setting is disabled or is not configured, the "Turn Windows features on or off" task will be available to all users. This setting does not prevent users from using other tools and methods to configure services or enable or disable program components

\Control Panel \Programs::Hide "Windows Marketplace"	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This setting prevents users from access the "Get new programs from Windows Marketplace" task from the Programs Control Panel in Category View, Programs and Features in Classic View, and Get Programs. Windows Marketplace allows users to purchase and/or download various programs to their computer for installation. Enabling this feature does not prevent users from navigating to Windows Marketplace using other methods. If this feature is disabled or is not configured, the "Get new programs from Windows Marketplace" task link will be available to all users. **Note:** If the "Hide Programs control Panel" setting is enabled, this setting is ignored
\Control Panel \Programs::Hide the Programs Control Panel	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This setting prevents users from using the Programs Control Panel in Category View and Programs and Features in Classic View. The Programs Control Panel allows users to uninstall, change, and repair programs, enable and disable Windows Features, set program defaults, view installed updates, and purchase software from Windows Marketplace. Programs published or assigned to the user by the system administrator also appear in the Programs Control Panel. If this setting is disabled or not configured, the Programs Control Panel in Category View and Programs and Features in Classic View will be available to all users. When enabled, this setting takes precedence over the other settings in this folder. This setting does not prevent users from using other tools and methods to install or uninstall programs.
\Control Panel\Regional and Language Options::Hide Regional and Language Options administrative options	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This policy removes the Administrative options from the Regional and Language Options control panel. Administrative options include interfaces for setting system locale and copying settings to the default user. This policy does not, however, prevent an administrator or another application from changing these values programmatically. The policy is used only to simplify the Regional Options control panel. If the policy is Enabled, then the user will not be able to see the Administrative options. If the policy is Disabled or Not Configured, then the user will see the Administrative options. Note that even if a user can see the Administrative options, other policies may prevent them from modifying the values.

\Control Panel\Regional and Language Options::Hide the geographic location option	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This policy removes the option to change the user's geographical location (GeoID) from the Language and Regional Options control panel. This does not, however, prevent the user or an application from changing the GeoID programmatically. The policy is used only to simplify the Regional Options control panel. If the policy is Enabled, then the user will not see the option to change the user geographical location (GeoID). If the policy is Disabled or Not Configured, then the user will see the option for changing the user location (GeoID). Note that even if a user can see the GeoID Option, the "Disallow changing of geographical location" option may prevent them from actually changing their current geographical location.
\Control Panel\Regional and Language Options::Hide the select language group options	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This policy removes the option to change the user's menus and dialogs (UI) language from the Language and Regional Options control panel. This does not, however, prevent the user or an application from changing the UI language programmatically. The policy is used only to simplify the Regional Options control panel. If the policy is Enabled, then the user will not see the option for changing the UI language. If the policy is Disabled or Not Configured, then the user will see the option for changing the UI language. Note that even if a user can see the option to change the UI language, other policies may prevent them from changing their UI language.
\Control Panel\Regional and Language Options::Hide user locale selection and customization options	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This policy removes the regional formats interface from the Regional and Language Options control panel. This does not, however, prevent the user or an application from changing their user locale or user overrides programmatically. The policy is only used to simplify the Regional Options control panel. If the policy is Enabled, then the user will not see the regional formats options. If the policy is Disabled or Not Configured, then the user will see the regional formats options for changing and customizing the user locale.
\Desktop::Do not add shares of recently opened documents to Network Locations	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Remote shared folders are not added to Network Locations whenever you open a document in the shared folder. If you disable this setting or do not configure it, when you open a document in a remote shared folder, the system adds a connection to the shared folder to Network Locations. If you enable this setting, shared folders are not added to Network Locations automatically when you open a document in the shared folder.

\Desktop::Don't save settings at exit	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from saving certain changes to the desktop. If you enable this setting, users can change the desktop, but some changes, such as the position of open windows or the size and position of the taskbar, are not saved when users log off. However, shortcuts placed on the desktop are always saved
\Desktop::Hide and disable all items on the desktop	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes icons, shortcuts, and other default and user-defined items from the desktop, including Briefcase, Recycle Bin, Computer, and Network Locations. Removing icons and shortcuts does not prevent the user from using another method to start the programs or opening the items they represent. Also, see "Items displayed in Places Bar" in User Configuration\Administrative Templates\Windows Components\Common Open File Dialog to remove the Desktop icon from the Places Bar. This will help prevent users from saving data to the Desktop
\Desktop::Hide Internet Explorer icon on desktop	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the Internet Explorer icon from the desktop and from the Quick Launch bar on the taskbar. This setting does not prevent the user from starting Internet Explorer by using other methods

\Desktop::Hide Network Locations icon on desktop	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the Network Locations icon from the desktop. This setting only affects the desktop icon. It does not prevent users from connecting to the network or browsing for shared computers on the network. **Note:** In operating systems earlier than Microsoft Windows Vista, this policy applies to the My Network Places icon
\Desktop::"Prevent adding, dragging, dropping and closing the Taskbar's toolbars"	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from manipulating desktop toolbars. If you enable this setting, users cannot add or remove toolbars from the desktop. In addition, users cannot drag toolbars on to or off of docked toolbars. **Note:** If users have added or removed toolbars, this setting prevents them from restoring the default configuration. **Tip** To view the toolbars that can be added to the desktop, right-click a docked toolbar (such as the taskbar beside the Start button), and point to "Toolbars." Also, see the "Prohibit adjusting desktop toolbars" setting
\Desktop::Prohibit adjusting desktop toolbars	Operational Roles, Engineering Role, and Product Administrator Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from adjusting the length of desktop toolbars. In addition, users cannot reposition items or toolbars on docked toolbars. This setting does not prevent users from adding or removing toolbars on the desktop. **Note:** If users have adjusted their toolbars, this setting prevents them from restoring the default configuration. Also, see the "Prevent adding, dragging, dropping and closing the Taskbar's toolbars" setting.

\Desktop::Prohibit User from manually redirecting Profile Folders	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from changing the path to their profile folders. By default, a user can change the location of their individual profile folders like Documents, Music etc. by typing a new path in the Locations tab of the folder's Properties dialog box. If you enable this setting, users are unable to type a new location in the Target box
\Desktop::Remove Computer icon on the desktop	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	If you enable this setting, Computer is hidden on the desktop, the new Start menu, the Explorer folder tree pane, and the Explorer Web views. If the user manages to navigate to Computer, the folder will be empty. If you enable this setting, Computer is hidden on the desktop, the new Start menu, the Explorer folder tree pane, and the Explorer Web views. If the user manages to navigate to Computer, the folder will be empty If you disable this setting, Computer is displayed as usual, appearing as normal on the desktop, Start menu, folder tree pane, and Web views, unless restricted by another setting. If you do not configure this setting, the default is to display Computer as usual. **Note:** In operating systems earlier than Microsoft Windows Vista, this policy applies to the My Computer icon. Hiding Computer and its contents does not hide the contents of the child folders of Computer. For example, if the users navigate into one of their hard drives, they see all of their folders and files there, even if this setting is enabled.
\Desktop::Remove My Documents icon on the desktop	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes most occurrences of the My Documents icon. This setting removes the My Documents icon from the desktop, from Windows Explorer, from programs that use the Windows Explorer windows, and from the standard Open dialog box. This setting does not prevent the user from using other methods to gain access to the contents of the My Documents folder. This setting does not remove the My Documents icon from the Start menu. To do so, use the "Remove My Documents icon from Start Menu" setting. **Note:** To make changes to this setting effective, you must log off from and log back on to Windows.

\Desktop::Remove Properties from the Recycle Bin context menu	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes the Properties option from the Recycle Bin shortcut menu. If you enable this setting, the Properties option will not be present when the user right-clicks on Recycle Bin or opens Recycle Bin and then clicks File. Likewise, Alt-Enter does nothing when Recycle Bin is selected. If you disable or do not configure this setting, the Properties option is displayed as usual.
\Desktop::Remove the Desktop Cleanup Wizard	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from using the Desktop Cleanup Wizard. If you enable this setting, the Desktop Cleanup wizard does not automatically run on a user's workstation every 60 days. The user will also not be able to access the Desktop Cleanup Wizard. If you disable this setting or do not configure it, the default behavior of the Desktop Clean Wizard running every 60 days occurs. **Note:** When this setting is not enabled, users can run the Desktop Cleanup Wizard, or have it run automatically every 60 days from Display, by clicking the Desktop tab and then clicking the Customize Desktop button.
\Desktop\Active Directory::Hide Active Directory folder	Operational Roles		Hides the Active Directory folder in Network Locations. The Active Directory folder displays Active Directory objects in a browse window. If you enable this setting, the Active Directory folder does not appear in the Network Locations folder. If you disable this setting or do not configure it, the Active Directory folder appears in the Network Locations folder. This setting is designed to let users search Active Directory but not tempt them to casually browse Active Directory.
\Desktop\Desktop::Disable Active Desktop	Operational Roles, Engineering Role and Product Administrator Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Disables Active Desktop and prevents users from enabling it. This setting prevents users from trying to enable or disable Active Desktop while a policy controls it. If you disable this setting or do not configure it, Active Desktop is disabled by default, but users can enable it. **Note:** If both the "Enable Active Desktop" setting and the "Disable Active Desktop" setting are enabled, the "Disable Active Desktop" setting is ignored. If the "Turn on Classic Shell" setting (in User Configuration \Administrative Templates\Windows Components \Windows Explorer) is enabled, Active Desktop is disabled, and both these policies are ignored.
\Desktop\Desktop::Prohibit changes	Operational Roles, Engineering Role and Product Administrator Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents the user from enabling or disabling Active Desktop or changing the Active Desktop configuration. This is a comprehensive setting that locks down the configuration you establish by using other policies in this folder. This setting removes the Web tab from Display in Control Panel. As a result, users cannot enable or disable Active Desktop. If Active Desktop is already enabled, users cannot add, remove, or edit Web content or disable, lock, or synchronize Active Desktop components.

\Network\Network Connections::Prohibit access to the New Connection Wizard	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Determines whether users can use the New Connection Wizard, which creates new network connections. If you enable this setting (and enable the "Enable Network Connections settings for Administrators" setting), the Make New Connection icon does not appear in the Start Menu on in the Network Connections folder. As a result, users (including administrators) cannot start the New Connection Wizard. Important: If the "Enable Network Connections settings for Administrators" is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers. If you disable this setting or do not configure it, the Make New Connection icon appears in the Start menu and in the Network Connections folder for all users. Clicking the Make New Connection icon starts the New Connection Wizard. **Note:** Changing this setting from Enabled to Not Configured does not restore the Make New Connection icon until the user logs off or on. When other changes to this setting are applied, the icon does not appear or disappear in the Network Connections folder until the folder is refreshed. This setting does not prevent users from using other programs, such as Internet Explorer, to bypass this setting.
\Network\Windows Connect Now::Prohibit Access of the Windows Connect Now wizards	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This policy setting prohibits access to Windows Connect Now (WCN) wizards. If this policy setting is enabled, the wizards are disabled and users will have no access to any of the wizard tasks. All the configuration related tasks, including ‘Set up a wireless router or access point’ and ‘Add a wireless device’, will be disabled. If this policy is disabled or not configured, users will have access to the wizard tasks; including ‘Set up a wireless router or access point’ and ‘Add a wireless device’. The default for this policy setting allows users to access all WCN wizards.

\Start Menu and Taskbar::Add Logoff to the Start Menu	Operational Roles, Engineering Role and Product Administrator Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	This policy only applies to the classic version of the start menu and does not affect the new style start menu. Adds the "Log Off <username>" item to the Start menu and prevents users from removing it. If you enable this setting, the Log Off <username> item appears in the Start menu. This setting also removes the Display Logoff item from Start Menu Options. As a result, users cannot remove the Log Off <username> item from the Start Menu. If you disable this setting or do not configure it, users can use the Display Logoff item to add and remove the Log Off item. This setting affects the Start menu only. It does not affect the Log Off item on the Windows Security dialog box that appears when you press Ctrl+Alt+Del. **Note:** To add or remove the Log Off item on a computer, click Start, click Settings, click Taskbar and Start Menu, click the Start Menu Options tab, and then, in the Start Menu Settings box, click Display Logoff. Also, see "Remove Logoff" in *User Configuration \Administrative Templates\System\Logon/Logoff*.
\Start Menu and Taskbar::Change Start Menu power button	Operational Roles, Engineering Role, and Product Administrator Role are logged off	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Set the default action of the power button on the Start menu. If you enable this setting, the Start Menu will set the power button to the chosen action, and not let the user change this action. If you set the button to either Sleep or Hibernate, and that state is not supported on a computer, then the button will fall back to Shut Down. If you disable or do not configure this setting, the Start Menu power button will be set to Shut Down by default, and the user can change this setting to another action.

\Start Menu and Taskbar::Clear history of recently opened documents on exit	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Clear history of recently opened documents on exit. If you enable this setting, the system deletes shortcuts to recently used document files when the user logs off. As a result, the Recent Items menu on the Start menu is always empty when the user logs on. In addition, recently and frequently used items in the Jump Lists off of programs in the Start Menu and Taskbar will be cleared when the user logs off. If you disable or do not configure this setting, the system retains document shortcuts, and when a user logs on, the Recent Items menu and the Jump Lists appear just as it did when the user logged off. **Note:** The system saves document shortcuts in the user profile in the *System-drive*\Users*User-name**Recent folder*. Also, see the "Remove Recent Items menu from Start Menu" and "Do not keep history of recently opened documents" policies in this folder. The system only uses this setting when neither of these related settings are selected. This setting does not clear the list of recent files that Windows programs display at the bottom of the File menu. See the "Do not keep history of recently opened documents" setting. This policy setting also does not hide document shortcuts displayed in the Open dialog box. See the "Hide the dropdown list of recent files" setting. This policy also does not clear items that the user may have pinned to the Jump Lists, or Tasks that the application has provided for their menu. See the "Do not allow pinning items in Jump Lists" setting.
\Start Menu and Taskbar::Do not allow pinning items in Jump Lists	Operational Roles	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this setting, users cannot pin files, folders, websites, or other items to their Jump Lists in the Start Menu and Taskbar. Users also cannot unpin existing items pinned to their Jump Lists. Existing items already pinned to their Jump Lists will continue to show. If you disable this setting or do not configure it, users can pin files, folders, websites, and other items to a program's Jump List so that the items is always present in this menu.

\Start Menu and Taskbar::Do not keep history of recently opened documents	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents the operating system and installed programs from creating and displaying shortcuts to recently opened documents. If you enable this setting, the system and Windows programs do not create shortcuts to documents opened while the setting is in effect. In addition, they retain but do not display existing document shortcuts. The system empties the Recent Items menu on the Start menu, and Windows programs do not display shortcuts at the bottom of the File menu. In addition, the Jump Lists off of programs in the Start Menu and Taskbar do not show lists of recently or frequently used files, folders, or websites. If you disable or do not configure this setting, the system will store and display shortcuts to recently and frequently used files, folders, and websites. **Note:** The system saves document shortcuts in the user profile in the *System-drive*\Users*User-name**Recent folder*. Also, see the "Remove Recent Items menu from Start Menu" and "Clear history of recently opened documents on exit" policies in this folder. If you enable this setting but do not enable the "Remove Recent Items menu from Start Menu" setting, the Recent Items menu appears on the Start menu, but it is empty. If you enable this setting, but then later disable it or set it to Not Configured, the document shortcuts saved before the setting was enabled reappear in the Recent Items menu and program File menus, and Jump Lists. This setting does not hide or prevent the user from pinning files, folders, or websites to the Jump Lists. See the "Do not allow pinning items in Jump Lists" setting. This policy also does not hide Tasks that the application has provided for their Jump List. This setting does not hide document shortcuts displayed in the Open dialog box. See the "Hide the dropdown list of recent files" setting. **Note:**It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.
\Start Menu and Taskbar::Lock all taskbar settings	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents the user from making any changes to the taskbar settings through the Taskbar Properties dialog. If you enable this setting the user cannot access the taskbar control panel. The user is also unable to resize, move or rearrange toolbars on their taskbar. If you disable or do not configure this setting the user will be able to set any taskbar setting that is not disallowed by another policy setting.

\Start Menu and Taskbar::Prevent changes to Taskbar and Start Menu Settings	Operational Roles and Engineering Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the Taskbar and Start Menu item from Settings on the Start menu. This setting also prevents the user from opening the Taskbar Properties dialog box. If the user right-clicks the taskbar and then clicks Properties, a message appears explaining that a setting prevents the action.
\Start Menu and Taskbar::Prevent grouping of taskbar items	Operational Roles and Engineering Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	This setting affects the taskbar buttons used to switch between running programs. Taskbar grouping consolidates similar applications when there is no room on the taskbar. It kicks in when the user's taskbar is full. If you enable this setting, it prevents the taskbar from grouping items that share the same program name. By default, this setting is always enabled. If you disable or do not configure it, items on the taskbar that share the same program are grouped together. The users have the option to disable grouping if they choose.
\Start Menu and Taskbar::Prevent users from adding or removing toolbars	Operational Roles and Engineering Role	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from adding or removing toolbars. If you enable this policy setting the user will not be allowed to add or remove any toolbars to the taskbar. Applications will not be able to add toolbars either. If you disable or do not configure this policy setting, the users and applications will be able to add toolbars to the taskbar.
\Start Menu and Taskbar::Prevent users from moving taskbar to another screen dock location	Operational Roles and Engineering Role	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from moving taskbar to another screen dock location. If you enable this policy setting the user will not be able to drag their taskbar to another side of the monitor(s). If you disable or do not configure this policy setting the user may be able to drag their taskbar to other sides of the monitor unless disallowed by another policy setting.

\Start Menu and Taskbar::Prevent users from rearranging toolbars	Operational Roles and Engineering Role	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from rearranging toolbars. If you enable this setting the user will not be able to drag or drop toolbars to the taskbar. If you disable or do not configure this policy setting, users will be able to rearrange the toolbars on the taskbar.
\Start Menu and Taskbar::Prevent users from resizing the taskbar	Operational Roles and Engineering Role	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevent users from resizing the taskbar. If you enable this policy setting the user will not be able to resize their taskbar to be any other size. If you disable or do not configure this policy setting, the user will be able to resize their taskbar to be any other size unless disallowed by another setting.
\Start Menu and Taskbar::Remove access to the context menus for the taskbar	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Hides the menus that appear when you right-click the taskbar and items on the taskbar, such as the Start button, the clock, and the taskbar buttons. This setting does not prevent users from using other methods to issue the commands that appear on these menus.
\Start Menu and Taskbar::Remove All Programs list from the Start menu	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	If you enable this setting, the "All Programs" item is removed from the simple Start menu. If you disable this setting or do not configure it, the "All Programs" item remains on the simple Start menu.

\Start Menu and Taskbar::"Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands"	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This policy setting prevents users from performing the following commands from the Start menu or Windows Security screen: Shut Down, Restart, Sleep, and Hibernate. This policy setting does not prevent users from running Windows-based programs that perform these functions. If you enable this policy setting, the Power button and the Shut Down, Restart, Sleep, and Hibernate commands are removed from the Start menu. The Power button is also removed from the Windows Security screen, which appears when you press *CTRL+ALT+DELETE*. If you disable or do not configure this policy setting, the Power button and the Shut Down, Restart, Sleep, and Hibernate commands are available on the Start menu. The Power button on the Windows Security screen is also available. **Note:** Third-party programs certified as compatible with Microsoft Windows Vista, Windows XP SP2, Windows XP SP1, Windows XP, or Windows 2000 Professional are required to support this policy setting.
\Start Menu and Taskbar::Remove Balloon Tips on Start Menu items	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Hides pop-up text on the Start menu and in the notification area. When you hold the cursor over an item on the Start menu or in the notification area, the system displays pop-up text providing additional information about the object. If you enable this setting, some of this pop-up text is not displayed. The pop-up text affected by this setting includes "Click here to begin" on the Start button, "Where have all my programs gone" on the Start menu, and "Where have my icons gone" in the notification area. If you disable this setting or do not configure it, all pop-up text is displayed on the Start menu and in the notification area.
\Start Menu and Taskbar::Remove common program groups from Start Menu	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes items in the All Users profile from the Programs menu on the Start menu. By default, the Programs menu contains items from the All Users profile and items from the user's profile. If you enable this setting, only items in the user's profile appear in the Programs menu. **Tip** To see the Program menu items in the All Users profile, on the system drive, go to `ProgramData\Microsoft\Windows\Start Menu\Programs`.

\Start Menu and Taskbar::Remove Default Programs link from the Start menu.	Operational Roles and Engineering Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes the Default Programs link from the Start menu. Clicking the Default Programs link from the Start menu opens the Default Programs control panel and provides administrators the ability to specify default programs for certain activities, such as Web browsing or sending e-mail, as well as which programs are accessible from the Start menu, desktop, and other locations. **Note:** This setting does not prevent the Set Default Programs for This Computer option from appearing in the Default Programs control panel.
\Start Menu and Taskbar::Remove Documents icon from Start Menu	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the Documents icon from the Start menu and its submenus. This setting only removes the icon. It does not prevent the user from using other methods to gain access to the contents of the Documents folder. **Note:** To make changes to this setting effective, you must log off and then log on. Also, see the "Remove Documents icon on the desktop" setting.
\Start Menu and Taskbar::Remove Downloads link from Start Menu	Operational Roles and Engineering Role	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this policy the start menu will not show a link to the Downloads folder.
\Start Menu and Taskbar::Remove drag-and-drop and context menus on the Start Menu	Operational Roles and Engineering Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from using the drag-and-drop method to reorder or remove items on the Start menu. In addition, it removes shortcut menus from the Start menu. If you disable this setting or do not configure it, users can remove or reorder Start menu items by dragging and dropping the item. They can display shortcut menus by right-clicking a Start menu item. This setting does not prevent users from using other methods of customizing the Start menu or performing the tasks available from the shortcut menus. Also, see the "Prevent changes to Taskbar and Start Menu Settings" and the "Remove access to the context menus for taskbar" settings.

\Start Menu and Taskbar::Remove Favorites menu from Start Menu	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from adding the Favorites menu to the Start menu or classic Start menu. If you enable this setting, the Display Favorites item does not appear in the Advanced Start menu options box. If you disable or do not configure this setting, the Display Favorite item is available. **Note:** The Favorites menu does not appear on the Start menu by default. To display the Favorites menu, right-click Start, click Properties, and then click Customize. If you are using Start menu, click the Advanced tab, and then, under Start menu items, click the Favorites menu. If you are using the classic Start menu, click Display Favorites under Advanced Start menu options. The items that appear in the Favorites menu when you install Windows are preconfigured by the system to appeal to most users. However, users can add and remove items from this menu, and system administrators can create a customized Favorites menu for a user group. This setting only affects the Start menu. The Favorites item still appears in Windows Explorer and in Internet Explorer.
\Start Menu and Taskbar::Remove frequent programs list from the Start Menu	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this setting, the frequently used programs list is removed from the Start menu. If you disable this setting or do not configure it, the frequently used programs list remains on the simple Start menu.
\Start Menu and Taskbar::Remove Games link from Start Menu	Operational Roles, Engineering Role, and Product Administrator Role	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this policy the start menu will not show a link to the Games folder. If you disable or do not configure this policy, the start menu will show a link to the Games folder, unless the user chooses to remove it in the start menu control panel.

\Start Menu and Taskbar::Remove Help menu from Start Menu	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the Help command from the Start menu. This setting only affects the Start menu. It does not remove the Help menu from Windows Explorer and does not prevent users from running Help.
\Start Menu and Taskbar::Remove Homegroup link from Start Menu	Operational Roles, Engineering Role, and Product Administrator Role	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this policy the Start menu will not show a link to Homegroup. It also removes the homegroup item from the Start Menu options. As a result, users cannot add the homegroup link to the Start Menu. If you disable or do not configure this policy, users can use the Start Menu options to add or remove the homegroup link from the Start Menu.
\Start Menu and Taskbar::Remove links and access to Windows Update	Operational Roles, Engineering Role, and Product Administrator Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from connecting to the Windows Update Web site. This setting blocks user access to the Windows Update Web site at http://windowsupdate.microsoft.com. In addition, the setting removes the Windows Update hyperlink from the Start menu and from the Tools menu in Internet Explorer. Windows Update, the online extension of Windows, offers software updates to keep a user's system up-to-date. The Windows Update Product Catalog determines any system files, security fixes, and Microsoft updates that user's need and shows the newest versions available for download. Also, see the "Hide the "Add programs from Microsoft" option" setting.

\Start Menu and Taskbar::Remove Music icon from Start Menu	Operational Roles, Engineering Role, and Product Administrator Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the Music icon from the Start Menu.
\Start Menu and Taskbar::Remove Network Connections from Start Menu	Operational Roles, Engineering Role, and Product Administrator Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	Prevents users from running Network Connections. This setting prevents the Network Connections folder from opening. This setting also removes Network Connections from Settings on the Start menu. Network Connections still appears in Control Panel and in Windows Explorer, but if users try to start it, a message appears explaining that a setting prevents the action. Also, see the "Disable programs on Settings menu" and "Disable Control Panel" settings and the settings in the Network Connections folder (Computer Configuration and User Configuration\Administrative Templates \Network\Network Connections).
\Start Menu and Taskbar::Remove Network icon from Start Menu	Operational Roles .	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the Network icon from the Start Menu.

\Start Menu and Taskbar::Remove Pictures icon from Start Menu	Operational Roles, Engineering Role, and Product Administrator Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the Pictures icon from the Start Menu.
\Start Menu and Taskbar::Remove pinned programs from the Taskbar	Operational Roles .	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this setting, pinned programs are prevented from being shown on the Taskbar. Users cannot pin programs to the Taskbar. If you disable this setting or do not configure it, users can pin programs so that the program shortcuts stay on the Taskbar.
\Start Menu and Taskbar::Remove pinned programs list from the Start Menu	Operational Roles .	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this setting, the "Pinned Programs" list is removed from the Start menu. Users cannot pin programs to the Start menu. In Windows XP and Windows Vista, the Internet and email checkboxes are removed from the 'Customize Start Menu' dialog. If you disable this setting or do not configure it, the "Pinned Programs" list remains on the Start menu. Users can pin and unpin programs in the Start Menu.

\Start Menu and Taskbar::Remove programs on Settings menu	Operational Roles and Engineering Role .	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents Control Panel, Printers, and Network Connections from running. This setting removes the Control Panel, Printers, and Network and Connection folders from Settings on the Start menu, and from Computer and Windows Explorer. It also prevents the programs represented by these folders (such as Control.exe) from running. However, users can still start Control Panel items by using other methods, such as right-clicking the desktop to start Display or right-clicking Computer to start System. Also, see the "Disable Control Panel," "Disable Display in Control Panel," and "Remove Network Connections from Start Menu" settings.
\Start Menu and Taskbar::Remove Recent Items menu from Start Menu	Operational Roles .	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the Recent Items menu from the Start menu. Removes the Documents menu from the classic Start menu. The Recent Items menu contains links to the non-program files that users have most recently opened. It appears so that users can easily reopen their documents. If you enable this setting, the system saves document shortcuts but does not display the Recent Items menu in the Start Menu, and users cannot turn the menu on. If you later disable the setting, so that the Recent Items menu appears in the Start Menu, the document shortcuts saved before the setting was enabled and while it was in effect, appear in the Recent Items menu. When the setting is disabled, the Recent Items menu appears in the Start Menu, and users cannot remove it. If the setting is not configured, users can turn the Recent Items menu on and off. **Note:** This setting does not prevent Windows programs from displaying shortcuts to recently opened documents. See the "Do not keep history of recently opened documents" setting. This setting also does not hide document shortcuts displayed in the Open dialog box. See the "Hide the dropdown list of recent files" setting.
\Start Menu and Taskbar::Remove Recorded TV link from Start Menu	Operational Roles, Engineering Role, and Product Administrator Role .	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this policy the start menu will not show a link to the Recorded TV library.

\Start Menu and Taskbar::Remove Run menu from Start Menu	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Allows you to remove the Run command from the Start menu, Internet Explorer, and Task Manager. If you enable this setting, the following changes occur. 1. The Run command is removed from the Start menu. 2. The New Task (Run) command is removed from Task Manager. 3. The user will be blocked from entering the following into the Internet Explorer Address Bar: • A UNC path: \\<*server*>\<*share*> • Accessing local drives: e.g., C: • Accessing local folders: e.g., \temp> Also, users with extended keyboards will no longer be able to display the Run dialog box by pressing the Application key (the key with the Windows logo) + R.
\Start Menu and Taskbar::Remove Search Computer link	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	If you enable this policy, the "See all results" link will not be shown when the user performs a search in the start menu search box. If you disable or do not configure this policy, the "See all results" link will be shown when the user performs a search in the start menu search box.
\Start Menu and Taskbar::Remove Search link from Start Menu	Operational Roles		Removes the Search link from the Start menu, and disables some Windows Explorer search elements. Note that this does not remove the search box from the new style Start menu. This setting removes the Search item from the Start menu and from the shortcut menu that appears when you right-click the Start menu. In addition, the system does not respond when users press the Application key (the key with the Windows logo)+ F. In Windows Explorer, the Search item still appears on the Standard buttons toolbar, but the system does not respond when the user presses Ctrl+F. In addition, Search does not appear in the shortcut menu when you right-click an icon representing a drive or a folder. This setting affects the specified user interface elements only. It does not affect Internet Explorer and does not prevent the user from using other methods to search. **Note:** This setting also prevents the user from using the F3 key.
\Start Menu and Taskbar::Remove See More Results / Search Everywhere link	Operational Roles	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this policy, a "See more results" / "Search Everywhere" link will not be shown when the user performs a search in the start menu search box. If you disable or do not configure this policy, a "See more results" link will be shown when the user performs a search in the start menu search box. If a 3rd party protocol handler is installed, a "Search Everywhere" link will be shown instead of the "See more results" link.

\Start Menu and Taskbar::"Remove the ""Undock PC"" button from the Start Menu"	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this setting, the "Undock PC" button is removed from the simple Start Menu, and your PC cannot be undocked. If you disable this setting or do not configure it, the "Undock PC" button remains on the simple Start menu, and your PC can be undocked.
\Start Menu and Taskbar::Remove the Action Center icon	Operational Roles and Engineering Role	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents the Action Center in the system control area from being displayed. If you enable this setting, the Action Center icon will not be displayed in the system notification area. If you disable or do not configure this setting, the Action Center icon will be displayed in the system notification area.
\Start Menu and Taskbar::Remove the battery meter	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents the battery meter in the system control area from being displayed. If you enable this setting, the battery meter will not be displayed in the system notification area. If you disable or do not configure this setting, the battery meter will be displayed in the system notification area.
\Start Menu and Taskbar::Remove user folder link from Start Menu	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this policy the start menu will not show a link to the user's storage folder. If you disable or do not configure this policy, the start menu will display a link, unless the user chooses to remove it in the start menu control panel.

\Start Menu and Taskbar::Remove user's folders from the Start Menu	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Hides all folders on the user-specific (top) section of the Start menu. Other items appear, but folders are hidden. This setting is designed for use with redirected folders. Redirected folders appear on the main (bottom) section of the Start menu. However, the original, user-specific version of the folder still appears on the top section of the Start menu. Because the appearance of two folders with the same name might confuse users, you can use this setting to hide user-specific folders. Note that this setting hides all user-specific folders, not just those associated with redirected folders. If you enable this setting, no folders appear on the top section of the Start menu. If users add folders to the Start Menu directory in their user profiles, the folders appear in the directory but not on the Start menu. If you disable this setting or do not configured it, Windows 2000 Professional and Windows XP Professional display folders on both sections of the Start menu.
\Start Menu and Taskbar::Remove Videos link from Start Menu	Operational Roles	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this policy the start menu will not show a link to the Videos library.
\Start Menu and Taskbar::Show QuickLaunch on Taskbar	Operational Roles is disabled	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	This policy setting controls whether the QuickLaunch bar is displayed in the Taskbar. If you enable this policy setting, the QuickLaunch bar will be visible and cannot be turned off. If you disable this policy setting, the QuickLaunch bar will be hidden and cannot be turned on. If you do not configure this policy setting, then users will be able to turn the QuickLaunch bar on and off.
\Start Menu and Taskbar::Turn off feature advertisement balloon notifications	Operational Roles	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this setting, certain notification balloons that are marked as feature advertisements will not be shown. If you disable this setting or do not configure it, feature advertisement balloons will be shown.

\Start Menu and Taskbar::Turn off personalized menus	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	Disables personalized menus. Windows personalizes long menus by moving recently used items to the top of the menu and hiding items that have not been used recently. Users can display the hidden items by clicking an arrow to extend the menu. If you enable this setting, the system does not personalize menus. All menu items appear and remain in standard order. In addition, this setting removes the "Use Personalized Menus" option so users do not try to change the setting while a setting is in effect. **Note:** Personalized menus require user tracking. If you enable the "Turn off user tracking" setting, the system disables user tracking and personalized menus and ignores this setting. **Tip** To Turn off personalized menus without specifying a setting, click Start, click Settings, click Taskbar and Start Menu, and then, on the General tab, clear the "Use Personalized Menus" option.
\Start Menu and Taskbar::Turn off user tracking	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	If you disable or do not configure this setting, the system tracks the programs that the user runs. The system uses this information to customize Windows features, such as showing frequently used programs in the Start Menu. If you enable this setting, the system does not track the programs that the user runs, and does not display frequently used programs in the Start Menu. Also, see these related settings: "Remove frequent programs list from the Start Menu" and "Turn off personalized menus." This setting does not prevent users from pinning programs to the Start Menu or Taskbar. See the "Remove pinned programs list from the Start Menu" and "Do not allow pinning programs to the Taskbar" settings.

\System: Don’t display the Getting Started welcome screen at logon	Operational Roles, Engineering Role, and Product Administrator Role		Suppresses the welcome screen. This setting hides the welcome screen that is displayed on Windows 2000 Professional each time the user logs on. Users can still display the welcome screen by selecting it on the Start menu or by typing "Welcome" in the Run dialog box. This setting applies only to Windows 2000 Professional. It does not affect the "Configure Your Server on a Windows 2000 Server" screen on Windows 2000 Server. **Note:** This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. **Tip** To display the welcome screen, click Start, point to Programs, point to Accessories, point to System Tools, and then click "Getting Started." To suppress the welcome screen without specifying a setting, clear the "Show this screen at startup" check box on the welcome screen.
\System::Prevent access to registry editing tools	Operational Roles and Engineering Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Disables the Windows registry editor Regedit.exe. If this setting is enabled and the user tries to start a registry editor, a message appears explaining that a setting prevents the action. To prevent users from using other administrative tools, use the "Run only specified Windows applications" setting.
Disable regedit from running silently	No Operational Roles and Engineering Role.		

\System::Prevent access to the command prompt	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from running the interactive command prompt, Cmd.exe. This setting also determines whether batch files (.cmd and .bat) can run on the computer. If you enable this setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action. **Note:** Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.
Disable the command prompt script processing also	No Operational Roles.		
\System\Ctrl+Alt+Del Options::Remove Lock Computer	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from locking the system. While locked, the desktop is hidden and the system cannot be used. Only the user who locked the system or the system administrator can unlock it. **Tip** To lock a computer without configuring a setting, press *Ctrl+Alt+Delete*, and then click **Lock Computer**.
\System\Ctrl+Alt+Del Options::Remove Task Manager	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from starting Task Manager (Taskmgr.exe). If this setting is enabled and users try to start Task Manager, a message appears explaining that a policy prevents the action. Task Manager lets users start and stop programs; monitor the performance of their computers; view and monitor all programs running on their computers, including system services; find the executable names of programs; and change the priority of the process in which programs run.

\System\Internet Communication Management\Internet Communication settings::Turn off Help Experience Improvement Program	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Specifies whether users can participate in the Help Experience Improvement program. The Help Experience Improvement program collects information about how customers use Windows Help so that Microsoft can improve it. If this setting is enabled, this policy prevents users from participating in the Help Experience Improvement program. If this setting is disabled or not configured, users will be able to turn on the Help Experience Improvement program feature from the Help and Support settings page.
\System\Internet Communication Management\Internet Communication settings::Turn off Help Ratings	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Specifies whether users can provide ratings for Help content. If this setting is enabled, this policy setting prevents ratings controls from being added to Help content. If this setting is disabled or not configured, a rating control will be added to Help topics. Users can use the control to provide feedback on the quality and usefulness of the Help and Support content.
\System\Internet Communication Management\Internet Communication settings::Turn off the Windows Messenger Customer Experience Improvement Program	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Specifies whether Windows Messenger collects anonymous information about how Windows Messenger software and service is used. With the Customer Experience Improvement program, users can allow Microsoft to collect anonymous information about how the product is used. This information is used to improve the product in future releases. If you enable this setting, Windows Messenger will not collect usage information and the user settings to enable the collection of usage information will not be shown. If you disable this setting, Windows Messenger will collect anonymous usage information and the setting will not be shown. If you do not configure this setting, users will have the choice to opt-in and allow information to be collected.
\System\Internet Communication Management\Internet Communication settings::Turn off Windows Online	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Specifies whether users can search and view content from Windows Online in Help and Support. Windows Online provides the most up-to-date Help content for Windows. If this setting is enabled, users will be prevented from accessing online assistance content from Windows Online. If this setting is disabled or not configured, users will be able to access online assistance if they have a connection to the Internet and have not disabled Windows Online from the Help and Support Options page.

\System\Performance Control Panel::Turn off access to the OEM and Microsoft branding section	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes access to the performance center control panel OEM and Microsoft branding links. If you enable this setting, the OEM and Microsoft web links within the performance control panel page will not be displayed. The administrative tools will not be affected. If you disable or do not configure this setting, the performance center control panel OEM and Microsoft branding links will be displayed to the user.
\System\Performance Control Panel::Turn off access to the performance center core section	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes access to the performance center control panel page. If you enable this setting, some settings within the performance control panel page will not be displayed. The administrative tools will not be affected. If you disable or do not configure this setting, the performance center control panel core section will be displayed to the user.
\System\Performance Control Panel::Turn off access to the solutions to performance problems section	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes access to the performance center control panel solutions to performance problems. If you enable this setting, the solutions and issue section within the performance control panel page will not be displayed. The administrative tools will not be affected. If you disable or do not configure this setting, the performance center control panel solutions to performance problems section will be displayed to the user.

\Windows Components \AutoPlay Policies::Turn off Autoplay	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Turns off the Autoplay feature. Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media start immediately. Prior to XP SP2, Autoplay is disabled by default on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives. Starting with XP SP2, Autoplay is enabled for removable drives as well, including ZIP drives and some USB Mass Storage devices. If you enable this setting, you can disable Autoplay on CD-ROM and removable media drives, or disable Autoplay on all drives. This setting disables Autoplay on additional types of drives. You cannot use this setting to enable Autoplay on drives on which it is disabled by default. **Note:** This setting appears in both the Computer Configuration and User Configuration folders. If the settings conflict, the setting in Computer Configuration takes precedence over the setting in User Configuration.
Turn off Autoplay on:	Operational Roles are for all drives		
\Windows Components \AutoPlay Policies::Turn off Autoplay for non-volume devices	Operational Roles	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If this policy is enabled, autoplay will not be enabled for non-volume devices like MTP devices. If you disable or not configure this policy, autoplay will continue to be enabled for non-volume devices.
\Windows Components \Desktop Gadgets::Turn off desktop gadgets	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This policy setting allows you to turn off desktop gadgets. Gadgets are small applets that display information or utilities on the desktop. If you enable this setting, desktop gadgets will be turned off. If you disable or do not configure this setting, desktop gadgets will be turned on. The default is for desktop gadgets to be turned on.

\Windows Components \Microsoft Management Console::Restrict the user from entering author mode	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from entering author mode. This setting prevents users from opening the Microsoft Management Console (MMC) in author mode, explicitly opening console files in author mode, and opening any console files that open in author mode by default. As a result, users cannot create console files or add or remove snap-ins. In addition, because they cannot open author-mode console files, they cannot use the tools that the files contain. This setting permits users to open MMC user-mode console files, such as those on the Administrative Tools menu in Windows 2000 Server family or Windows Server 2003 family. However, users cannot open a blank MMC console window on the Start menu. (To open the MMC, click Start, click Run, and type mmc.) Users also cannot open a blank MMC console window from a command prompt. If you disable this setting or do not configure it, users can enter author mode and open author-mode console files.
\Windows Components \Microsoft Management Console\Restricted/ Permitted snap-ins::Server Manager	Operational Roles is disabled	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Permits or prohibits use of this snap-in. If you enable this setting, the snap-in is permitted. If you disable the setting, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited. • If "Restrict users to the explicitly permitted list of snap-ins" is enabled, users cannot use any snap-in except those explicitly permitted. To permit explicit use of this snap-in, enable this setting. If this setting is not configured (or disabled), this snap-in is prohibited. • If "Restrict users to the explicitly permitted list of snap-ins" is disabled or not configured, users can use any snap-in except those explicitly prohibited. To prohibit explicit use of this snap-in, disable this setting. If this setting is not configured (or enabled), the snap-in is permitted. When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. In addition, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.

\Windows Components \Task Scheduler::Hide Advanced Properties Checkbox in Add Scheduled Task Wizard	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	This setting removes the "Open advanced properties for this task when I click Finish" checkbox from the last page of the Scheduled Task Wizard. This policy is only designed to simplify task creation for beginning users. The checkbox, when checked, instructs Task Scheduler to open the newly created task's property sheet automatically upon completion of the "Add Scheduled Task" wizard. The task's property sheet allows users to change task characteristics such as, the program the task runs, details of its schedule, idle time and power management settings, and its security context. Beginning users will often not be interested or confused by having the property sheet displayed automatically. Note that the checkbox is not checked by default even if this setting is Disabled or Not Configured. **Note:** This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
\Windows Components \Task Scheduler::Hide Property Pages	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from viewing and changing the properties of an existing task. This setting removes the Properties item from the File menu in Scheduled Tasks and from the shortcut menu that appears when you right-click a task. As a result, users cannot change any properties of a task. They can only see the properties that appear in Detail view and in the task preview. This setting prevents users from viewing and changing characteristics such as the program the task runs, its schedule details, idle time and power management settings, and its security context. **Note:**This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. **Tip** This setting affects existing tasks only. To prevent users from changing the properties of newly created tasks, use the "Remove Advanced Menu" setting.
\Windows Components \Task Scheduler::Prevent Task Run or End	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from starting and stopping tasks manually. This setting removes the Run and End Task items from the shortcut menu that appears when you right-click a task. As a result, users cannot start tasks manually or force tasks to end before they are finished. **Note:** This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

\Windows Components \Task Scheduler::Prohibit Browse	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Limits newly scheduled to items on the user's Start menu, and prevents the user from changing the scheduled program for existing tasks. This setting removes the Browse button from the Schedule Task Wizard and from the Task tab of the properties dialog box for a task. In addition, users cannot edit the "Run" box or the "Start in" box that determine the program and path for a task. As a result, when users create a task, they must select a program from the list in the Scheduled Task Wizard, which displays only the tasks that appear on the Start menu and its submenus. Once a task is created, users cannot change the program a task runs. **Important:** This setting does not prevent users from creating a new task by pasting or dragging any program into the Scheduled Tasks folder. To prevent this action, use the "Prohibit Drag-and-Drop" setting. **Note:** This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
\Windows Components \Task Scheduler::Prohibit Drag-and-Drop	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from adding or removing tasks by moving or copying programs in the Scheduled Tasks folder. This setting disables the Cut, Copy, Paste, and Paste Shortcut items on the shortcut menu and the Edit menu in Scheduled Tasks. It also disables the drag-and-drop features of the Scheduled Tasks folder. As a result, users cannot add new scheduled tasks by dragging, moving, or copying a document or program into the Scheduled tasks folder. This setting does not prevent users from using other methods to create new tasks, and it does not prevent users from deleting tasks. **Note:** This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.
\Windows Components \Task Scheduler::Prohibit New Task Creation	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from creating new tasks. This setting removes the Add Scheduled Task item that starts the New Task Wizard. In addition, the system does not respond when users try to move, paste, or drag programs or documents into the Scheduled Tasks folder. **Note:** This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. **Important:** This setting does not prevent administrators of a computer from using At.exe to create new tasks or prevent administrators from submitting tasks from remote computers.

\Windows Components \Task Scheduler::Prohibit Task Deletion	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from deleting tasks from the Scheduled Tasks folder. This setting removes the Delete command from the Edit menu in the Scheduled Tasks folder and from the menu that appears when you right-click a task. In addition, the system does not respond when users try to cut or drag a task from the Scheduled Tasks folder. **Note:** This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration. **Important:** This setting does not prevent administrators of a computer from using At.exe to delete tasks.
\Windows Components \Windows Anytime Upgrade::Prevent Windows Anytime Upgrade from running.	Operational Roles	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	By default Windows Anytime Upgrade is available for all administrators. If you enable this policy setting, Windows Anytime Upgrade will not run. If you disable this policy setting or set it to Not Configured, Windows Anytime Upgrade will run.
\Windows Components \Windows Explorer::Do not display the Welcome Center at user logon	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	This policy setting prevents the display of the Welcome Center at user logon. If you enable this policy setting, the Welcome Center will not be displayed at user logon. The user will be able to access the Welcome Center using the Control Panel or Start menu. If you disable or do not configure this policy setting, the Welcome Center will be displayed at user logon.
\Windows Components \Windows Explorer::Hide these specified drives in My Computer	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the icons representing selected hard drives from My Computer and Windows Explorer. In addition, the drive letters representing the selected drives do not appear in the standard Open dialog box. To use this setting, select a drive or combination of drives in the drop-down list. To display all drives, disable this setting or select the "Do not restrict drives" option in the drop-down list. **Note:** This setting removes the drive icons. Users can still gain access to drive contents by using other methods, such as by typing the path to a directory on the drive in the Map Network Drive dialog box, in the Run dialog box, or in a command window. In addition, this setting does not prevent users from using programs to access these drives or their contents. In addition, it does not prevent users from using the Disk Management snap-in to view and change drive characteristics. Also, see the "Prevent access to drives from My Computer" setting. It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.
Pick one of the following combinations	Operational Roles restrict all drives		

\Windows Components \Windows Explorer::Hides the Manage item on the Windows Explorer context menu	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the Manage item from the Windows Explorer shortcut menu. This shortcut menu appears when you right-click Windows Explorer or My Computer. The Manage item opens Computer Management (Compmgmt.msc), a console tool that includes many of the primary Windows administrative tools, such as Event Viewer, Device Manager, and Disk Management. You must be an administrator to use many of the features of these tools. This setting does not remove the Computer Management item from the Start menu (Start, Programs, Administrative Tools, Computer Management), nor does it prevent users from using other methods to start Computer Management. **Tip** To hide all shortcut menus, use the "Remove Windows Explorer's default context menu" setting.
\Windows Components \Windows Explorer::No Computers Near Me in Network Locations	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes computers in the user's workgroup and domain from lists of network resources in Windows Explorer and Network Locations. If you enable this setting, the system removes the "Computers Near Me" option and the icons representing nearby computers from Network Locations. This setting also removes these icons from the Map Network Drive browser. This setting does not prevent users from connecting to computers in their workgroup or domain by other commonly used methods, such as typing the share name in the Run dialog box or the Map Network Drive dialog box. To remove network computers from lists of network resources, use the "No Entire Network in Network Locations" setting.
\Windows Components \Windows Explorer::No Entire Network in Network Locations	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes all computers outside of the user's workgroup or local domain from lists of network resources in Windows Explorer and Network Locations. If you enable this setting, the system removes the Entire Network option and the icons representing networked computers from Network Locations and from the browser associated with the Map Network Drive option. This setting does not prevent users from viewing or connecting to computers in their workgroup or domain. It also does not prevent users from connecting to remote computers by other commonly used methods, such as by typing the share name in the Run dialog box or the Map Network Drive dialog box. To remove computers in the user's workgroup or domain from lists of network resources, use the "No Computers Near Me in Network Locations" setting. **Note:** It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.

\Windows Components \Windows Explorer::Prevent access to drives from My	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from using My Computer to gain access to the content of selected drives. If you enable this setting, users can browse the directory structure of the selected drives in My Computer or Windows Explorer, but they cannot open folders and access the contents. In addition, they cannot use the Run dialog box or the Map Network Drive dialog box to view the directories on these drives. To use this setting, select a drive or combination of drives from the drop-down list. To allow access to all drive directories, disable this setting or select the "Do not restrict drives" option from the drop-down list. **Note:** The icons representing the specified drives still appear in My Computer, but if users double-click the icons, a message appears explaining that a setting prevents the action. In addition, this setting does not prevent users from using programs to access local and network drives. In addition, it does not prevent them from using the Disk Management snap-in to view and change drive characteristics. Also, see the "Hide these specified drives in My Computer" setting.
Pick one of the following combinations	Operational Roles restrict all drives		
\Windows Components \Windows Explorer::Prevent users from adding files to the root of their Users Files folder.	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This policy setting allows administrators to prevent users from adding new items such as files or folders to the root of their Users Files folder in Windows Explorer. If you enable this policy setting, users will no longer be able to add new items such as files or folders to the root of their Users Files folder in Windows Explorer. If you disable or do not configure this policy setting, users will be able to add new items such as files or folders to the root of their Users Files folder in Windows Explorer. **Note:** Enabling this policy setting does not prevent the user from being able to add new items such as files and folders to their actual file system profile folder at %userprofile%.

\Windows Components \Windows Explorer::Remove "Map Network Drive" and "Disconnect Network Drive"	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from using Windows Explorer or Network Locations to map or disconnect network drives. If you enable this setting, the system removes the Map Network Drive and Disconnect Network Drive commands from the toolbar and Tools menus in Windows Explorer and Network Locations and from menus that appear when you right-click the Windows Explorer or Network Locations icons. This setting does not prevent users from connecting to another computer by typing the name of a shared folder in the Run dialog box. **Note:** This setting was documented incorrectly on the Explain tab in Group Policy for Windows 2000. The Explain tab states incorrectly that this setting prevents users from connecting and disconnecting drives. It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting.
\Windows Components \Windows Explorer::Remove CD Burning features	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Windows Explorer allows you to create and modify re-writable CDs if you have a CD writer connected to your PC. If you enable this setting, all features in the Windows Explorer that allow you to use your CD writer are removed. If you disable or do not configure this setting, users are able to use the Windows Explorer CD burning features. **Note:** This setting does not prevent users from using third-party applications to create or modify CDs using a CD writer.
\Windows Components \Windows Explorer::Remove DFS tab	Operational Roles and Engineering Role	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the DFS tab from Windows Explorer. This setting removes the DFS tab from Windows Explorer and from other programs that use the Windows Explorer browser, such as My Computer. As a result, users cannot use this tab to view or change the properties of the Distributed File System (DFS) shares available from their computer. This setting does not prevent users from using other methods to configure DFS.

\Windows Components \Windows Explorer::Remove File menu from Windows Explorer	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the File menu from My Computer and Windows Explorer. This setting does not prevent users from using other methods to perform tasks available on the File menu.
\Windows Components \Windows Explorer::Remove Hardware tab	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes the Hardware tab. This setting removes the Hardware tab from Mouse, Keyboard, and Sounds and Audio Devices in Control Panel. It also removes the Hardware tab from the Properties dialog box for all local drives, including hard drives, floppy disk drives, and CD-ROM drives. As a result, users cannot use the Hardware tab to view or change the device list or device properties, or use the Troubleshoot button to resolve problems with the device.
\Windows Components \Windows Explorer::Remove Search button from Windows Explorer	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes the Search button from the Windows Explorer toolbar. This setting removes the Search button from the Standard Buttons toolbar that appears in Windows Explorer and other programs that use the Windows Explorer window, such as My Computer and Network Locations. It does not remove the Search button or affect any search features of Internet browser windows, such as the Internet Explorer window. This setting does not affect the Search items on the Windows Explorer shortcut menu or on the Start menu. To remove Search from the Start menu, use the "Remove Search menu from Start menu" setting (in User Configuration\Administrative Templates\Start Menu and Taskbar). To hide all shortcut menus, use the "Remove Windows Explorer's default context menu" setting.

\Windows Components \Windows Explorer::Remove Security tab	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes the Security tab from Windows Explorer. If you enable this setting, users opening the Properties dialog box for all file system objects, including folders, files, shortcuts, and drives, will not be able to access the Security tab. As a result, users will be able to neither change the security settings nor view a list of all users that have access to the resource in question. If you disable or do not configure this setting, users will be able to access the security tab.
\Windows Components \Windows Explorer::Remove Shared Documents from My Computer	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Removes the Shared Documents folder from My Computer. When a Windows client is in a workgroup, a Shared Documents icon appears in the Windows Explorer Web view under "Other Places" and also under "Files Stored on This Computer" in My Computer. Using this policy setting, you can choose not to have these items displayed. If you enable this setting, the Shared Documents folder is not displayed in the Web view or in My Computer. If you disable or do not configure this setting, the Shared Documents folder is displayed in Web view and also in My Computer when the client is part of a workgroup. **Note:** The ability to remove the Shared Documents folder via Group Policy is only available on Windows XP Professional
\Windows Components \Windows Explorer::"Remove the Search the Internet ""Search again"" link"	Operational Roles	Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	If you enable this policy, the "Internet" "Search again" link will not be shown when the user performs a search in the Explorer window. If you disable this policy, there will be an "Internet" "Search again" link when the user performs a search in the Explorer window. This button launches a search in the default browser with the search terms. If you do not configure this policy (default), there will be an "Internet" link when the user performs a search in the Explorer window.
\Windows Components \Windows Explorer::Remove UI to change keyboard navigation indicator setting	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Disables the "Hide keyboard navigation indicators until I use the ALT key" option in Display in Control Panel. When this Display Properties option is selected, the underlining that indicates a keyboard shortcut character (hot key) does not appear on menus until you press ALT. Effects, such as transitory underlines, are designed to enhance the user's experience but might be confusing or distracting to some users.
\Windows Components \Windows Explorer::Remove UI to change menu animation setting	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents users from selecting the option to animate the movement of windows, menus, and lists. If you enable this setting, the "Use transition effects for menus and tooltips" option in Display in Control Panel is disabled. Effects, such as animation, are designed to enhance the user's experience but might be confusing or distracting to some users.

\Windows Components \Windows Explorer::Remove Windows Explorer's default context menu	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Removes shortcut menus from the desktop and Windows Explorer. Shortcut menus appear when you right-click an item. If you enable this setting, menus do not appear when you right-click the desktop or when you right-click the items in Windows Explorer. This setting does not prevent users from using other methods to issue commands available on the shortcut menus.
\Windows Components \Windows Explorer::Turn on Classic Shell	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard	This setting allows an administrator to revert specific Windows Shell behavior to classic Shell behavior. If you enable this setting, users cannot configure their system to open items by single-clicking (such as in Mouse in Control Panel). As a result, the user interface looks and operates like the interface for Windows NT 4.0, and users cannot restore the new features. Enabling this policy will also turn off the preview pane and set the folder options for Windows explorer to Use classic folders view and disable the user's ability to change these options. If you disable or not configure this policy, the default Windows explorer behavior is applied to the user. **Note:** In operating systems earlier than Windows Vista, enabling this policy will also disable the Active Desktop and Web view. This setting will also take precedence over the "Enable Active Desktop" setting. If both policies are enabled, Active Desktop is disabled. In addition, see the "Disable Active Desktop" setting in User Configuration\Administrative Templates\Desktop \Active Desktop and the "Remove the Folder Options menu item from the Tools menu" setting in User Configuration\Administrative Templates\Windows Components\Windows Explorer.

\Windows Components \Windows Installer::Prevent removable media source for any install	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Prevents users from installing programs from removable media. If a user tries to install a program from removable media, such as CD-ROMs, floppy disks, and DVDs, a message appears, stating that the feature cannot be found. This setting applies even when the installation is running in the user's security context. If you disable this setting or do not configure it, users can install from removable media when the installation is running in their own security context, but only system administrators can use removable media when an installation is running with elevated system privileges, such as installations offered on the desktop or in Add or Remove Programs. Also, see the "Enable user to use media source while elevated setting" in *Computer Configuration \Administrative Templates\WindowsComponents \Windows Installer*. Also, see the "Hide the 'Add a program from CD-ROM or floppy disk' option" setting in *User Configuration \Administrative Templates\Control Panel\Add or Remove Programs*.
\Windows Components \Windows Mail::Turn off Windows Mail application	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Denies or allows access to the Windows Mail application. If you enable this setting, access to the Windows Mail application is denied. If you disable or do not configure this setting, access to the Windows Mail application is allowed.
\Windows Components \Windows Media Center::Do not allow Windows Media Center to run	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Specifies whether Windows Media Center can run. If you enable this setting, Windows Media Center will not run. If you disable or do not configure this setting, Windows Media Center can be run.

\Windows Components \Windows Media Player::Prevent CD and DVD Media Information Retrieval	Operational Roles		Prevents media information for CDs and DVDs from being retrieved from the Internet. This policy prevents the Player from automatically obtaining media information from the Internet for CDs and DVDs played by users. In addition, the Retrieve media information for CDs and DVDs from the Internet check box on the Privacy Options tab in the first use dialog box and on the Privacy tab in the Player are not selected and are not available. When this policy is not configured or disabled, users can change the setting of the Retrieve media information for CDs and DVDs from the Internet check box.
\Windows Components \Windows Media Player::Prevent Music File Media Information Retrieval	Operational Roles		Prevents media information for music files from being retrieved from the Internet. This policy prevents the Player from automatically obtaining media information for music files such as Windows Media Audio (WMA) and MP3 files from the Internet. In addition, the Update my music files (WMA and MP3 files) by retrieving missing media information from the Internet check box in the first use dialog box and on the Privacy and Media Library tabs in the Player are not selected and are not available. When this policy is not configured or disabled, users can change the setting of the Update my music files (WMA and MP3 files) by retrieving missing media information from the Internet check box.
\Windows Components \Windows Media Player::Prevent Radio Station Preset Retrieval	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit)	Prevents radio station presets from being retrieved from the Internet. This policy prevents the Player from automatically retrieving radio station presets from the Internet and displaying them in Media Library. In addition, presets that exist before the policy is configured will not be updated, and presets a user adds will not be displayed. When this policy is not configured or disabled, the Player automatically retrieves radio station presets from the Internet.

\Windows Components \Windows Messenger::Do not automatically start Windows Messenger initially	Operational Roles	Microsoft Windows XP/ Microsoft Windows Server 2003 (32-bit), Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Windows Messenger is automatically loaded and running when a user logs on to a Windows XP computer. You can use this setting to stop Windows Messenger from automatically being run at logon. If you enable this setting, Windows Messenger will not be loaded automatically when a user logs on. If you disable or do not configure this setting, the Windows Messenger will be loaded automatically at logon. **Note:** This setting simply prevents Windows Messenger from running initially. If the user invokes and uses Windows Messenger from that point on, Windows Messenger will be loaded. The user can also configure this behavior on the Preferences tab on the Tools menu in the Windows Messenger user interface. If you do not want users to use Windows Messenger, enable the "Do not allow Windows Messenger to run" setting This setting is available under both Computer Configuration and User Configuration. If both are present, the Computer Configuration version of this setting takes precedence
\Windows Components \Windows Sidebar::Turn off Windows Sidebar	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	Windows Sidebar is a feature that allows the use of gadgets, which are small applets that may display information or utilities to the user. If you enable this setting, Windows Sidebar will be turned off. If you disable or do not configure this setting, Windows Sidebar will be turned on. The default is for Windows Sidebar to be turned on.
\Windows Components \Windows SideShow::Turn off Windows SideShow	Operational Roles	Microsoft Windows Vista/Microsoft Windows Server 2008 Standard, Microsoft Windows 7 Professional (32-bit)/ Microsoft Windows Server 2008 R2	This policy setting turns off Windows SideShow. If you enable this policy setting, the Windows SideShow Control Panel will be disabled and data from Windows SideShow-compatible gadgets (applications) will not be sent to connected devices. If you disable or do not configure this policy setting, Windows SideShow is on by default.

13.2 Security Model specific permissions

Part of the installation of the Common Security Model is to set up permissions on some keys in the registry and directories in the file system. In addition, it installs a base set of files, with defined permissions, that act as proxy access control lists (ACLs) for Experion objects and functions that do not have an integral Windows ACL.

[Registry Permissions]	Permission for	Scope	
		Key	Subkey
HKLM\SOFTWARE\Honeywell (add)	Product Admins	RW	Full
HKLM\SOFTWARE\Honeywell \ProgramData (add)	Product Admins	Full	Full
	Engineer	RW	Full
	Supervisor	RW	Full
	Operator	RW	Full
	Ack View	RW	Full
	View Only	RW	Full
HKLM\SOFTWARE\Honeywell \EngineeringData (set)	Engineer	RW	Full
	Windows Admin	Full	Full
	Windows Users	R	R
	SYSTEM	Full	Full
	Creator Owner		Full
HKLM\software\Microsoft\MSDTC (add - legacy)	Product Admins	RW	RW
	Local Servers	RW	RW
HKLM\software\Clients\Mail (add - legacy)	Product Admins	RW	RW
	Local Servers	RW	RW
HKLM\SYSTEM\CurrentControlSet \Control\SecurePipeServers\winreg (add)	Local Servers	R	R
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Perflib (add)	Product Admins	R	R
	Local Servers	R	R
HKLM\Software\Microsoft\Windows NT\CurrentVersion\WbemPerf (add)	Product Admins	R	R
	Local Servers	R	R

[Registry Permissions]	Permission for	Scope		
[Directories]		Folder	Subfolders	Files
%HwProgramData% (set)	Product Admins	RWX	Full	Full
	Engineer	RWX	Full	Full
	Supervisor	RWX	Full	Full
	Operator	RWX	Full	Full
	Ack View	RWX	Full	Full
	View Only	RWX	Full	Full
	Windows Admin	Full	Full	Full
	Windows Users	RX	RX	RX

	SYSTEM	Full	Full	Full
%HwEngineeringData% (set)	Engineer	Engineer	Full	Full
	Windows Admin	Full	Full	Full
	Windows Users	RX	RX	RX
	SYSTEM	Full	Full	Full
	Creator Owner		Full	Full
%HwProductConfig% (set)	Product Admins	RWX	Full	Full
	Windows Admin	Full	Full	Full
	Windows Users	RX	RX	RX
	SYSTEM	Full	Full	Full
	Creator Owner		Full	Full
%HwSecurityPath% (set)	Product Admins	Full	Full	RW
	Windows Admin	Full	Full	RW
	Windows Users	RX	RX	R
	SYSTEM	Full	Full	RW
	Creator Owner		Full	RW

[File System Permissions]	**Permission for**	Scope
[Proxy Files]		**Files**
%HwSecurityPath%\tpn_priority_two (add)	Engineer	RX
	Supervisor	RX
	Operator	RX
%HwSecurityPath%\tpn_priority_three (add)	Engineer	RX
	Supervisor	RX
	Operator	RX
%HwSecurityPath%\tpn_priority_four (add)	Engineer	RX
	Supervisor	RX
	Operator	RX
%HwSecurityPath%\tpn_priority_five (add)	Engineer	RX
	Supervisor	RX
	Operator	RX
%HwSecurityPath%\tpn_priority_six (add)	Engineer	RX
	Supervisor	RX
	Operator	RX
%HwSecurityPath% \tpn_priority_seven (add)	Engineer	RX
	Supervisor	RX
	Operator	RX
%HwSecurityPath%\tpn_priority_eight (add)	Engineer	RX
	Supervisor	RX
	Operator	RX
%HwSecurityPath%\tpn_priority_nine (add)	Engineer	RX
	Supervisor	RX

	Operator	RX
%HwSecurityPath%\tpn_priority_ten (add)	Engineer	RX
	Supervisor	RX
	Operator	RX
%HwSecurityPath%\product admin (add)	Product Admins	RX
%HwSecurityPath%\engineer (add)	Engineer	RX
%HwSecurityPath%\supervisor (add)	Engineer	RX
	Supervisor	RX
%HwSecurityPath%\operator (add)	Engineer	RX
	Supervisor	RX
	Operator	RX
%HwSecurityPath%\AckUser (add)	Engineer	RX
	Supervisor	RX
	Operator	RX
	Ack View	RX
%HwSecurityPath%\view only (add)	Engineer	RX
	Supervisor	RX
	Operator	RX
	Ack View	RX
	View Only	RX
%HwSecurityPath%\program (add)	Engineer	RX
%HwSecurityPath%\continuous control (add)	Engineer	RX
%HwSecurityPath%\checkpoint (add)	Product Admins	RX
	Engineer	RX
	Supervisor	RX
	Operator	RX
	Ack View	RX
	View Only	RX
%HwSecurityPath%\start (add)	Product Admins	RX
	Engineer	RX
	Supervisor	RX
	Operator	RX
	Ack View	RX
	View Only	RX
%HwSecurityPath%\shutdown (add)	Product Admins	RX
	Engineer	RX
	Supervisor	RX
%HwSecurityPath%\shutdownforce (add)	Product Admins	RX
	Engineer	RX
	Supervisor	RX

In the preceding table, strings between percent signs (%) represent system environment variables that may vary based on installation conditions. The default values for these are:

- .....%HwProgramData% *C:\ProgramData\Honeywell*
- .....%HwEngineeringData% *C:\ProgramData\Honeywell\EngineeringData*
- .....%HwProductConfig% *C:\ProgramData\Honeywell\ProductConfig*
- .....%HwSecurityPath%*C:\ProgramData\Honeywell\ProductConfig\Security*

13.2.1 Local policy settings

The local policy settings are applied through the SECEDIT.EXE command, using a template that is installed by the Workstation Security package.

In the following table, cells with (*) symbol indicate default settings that were modified for Experion per operating system. Cells with (**) indicate settings on Experion that differ between Windows 7 and Windows server 2008/2008 R2.

Local Policy Settings	Windows 7 for Experion	Windows 7 defaults	Windows server 2008/2008 R2 for Experion	Windows server 2008/2008 R2 defaults
[System Access]				
MinimumPasswordAge	0	0	0	0
MaximumPasswordAge	-1	42(*)	-1	42(*)
MinimumPasswordLength	0	0	0	0
PasswordComplexity	0(**)	0	1(**)	1
PasswordHistorySize	10	0(*)	10	0(*)
LockoutBadCount	0	0	0	0
RequireLogonToChangePassword	0	0	0	0
ForceLogoffWhenHourExpire	0	0	0	0
NewAdministratorName	Administrator	Administrator	Administrator	Administrator
NewGuestName	Guest	Guest	Guest	Guest
ClearTextPassword	0	0	0	0
LSAAnonymousNameLookup	0	0	0	0
EnableAdminAccount	0(**)	0	1(**)	1
EnableGuestAccount	0	0	0	0
[Event Audit]				
AuditSystemEvents	0	0	0	0
AuditLogonEvents	2	0(*)	2	0(*)
AuditObjectAccess	0	0	0	0
AuditPrivilegeUse	0	0	0	0
AuditPolicyChange	3	0(*)	3	0(*)
AuditAccountManage	0	0	0	0

Local Policy Settings	Windows 7 for Experion	Windows 7 defaults	Windows server 2008/2008 R2 for Experion	Windows server 2008/2008 R2 defaults
AuditProcessTracking	0	0	0	0
AuditDSAccess	0	0	0	0
AuditAccountLogon	2	0(*)	2	0(*)
[Registry Values]				
HKLM\software \microsoft\Ole \EnableDCOM	"Y"	"Y"	"Y"	"Y"
HKLM\software \microsoft\Ole \LegacyAuthentication Level	2	(*)	2	(*)
HKLM\software \microsoft\Ole \LegacyImpersonation Level	3	2	3	2
HKLM\software \microsoft\windows \currentversion \policies\system \HideFastUserSwitching	1	(*)	1	(*)
HKLM\software \microsoft\windows \currentversion \policies\system \LogonType	0	(*)	0	(*)
HKLM\SOFTWARE \Microsoft\Windows \Windows Error Reporting \LocalDumps \DumpCount	10	(*)	10	(*)
HKLM\SOFTWARE \Microsoft\Windows \Windows Error Reporting \LocalDumps \DumpFolder	"%HwProgramData% \Experion PKS \CrashDump	(*)	"%HwProgramData% \Experion PKS \CrashDump"	(*)
HKLM\SOFTWARE \Microsoft\Windows \Windows Error Reporting \LocalDumps \DumpType	2	(*)	2	(*)
HKLM\Software \Microsoft\Windows NT\CurrentVersion \Setup \RecoveryConsole \SecurityLevel	0	0	0	0

Local Policy Settings	Windows 7 for Experion	Windows 7 defaults	Windows server 2008/2008 R2 for Experion	Windows server 2008/2008 R2 defaults
HKLM\Software \Microsoft\Windows NT\CurrentVersion \Setup \RecoveryConsole \SetCommand	0	0	0	0
HKLM\Software \Microsoft\Windows NT\CurrentVersion \Winlogon \AllocateCDRoms	“0”	(*)	“0”	(*)
HKLM\Software \Microsoft\Windows NT\CurrentVersion \Winlogon \AllocateDASD	“0”	(*)	“0”	(*)
HKLM\Software \Microsoft\Windows NT\CurrentVersion \Winlogon \AllocateFloppies	“1”	(*)	“1”	(*)
HKLM\Software \Microsoft\Windows NT\CurrentVersion \Winlogon \CachedLogonsCount	“10”	“10”	“10”	“25”(*)
HKLM\Software \Microsoft\Windows NT\CurrentVersion \Winlogon \ForceUnlockLogon	0	0	0	0
HKLM\Software \Microsoft\Windows NT\CurrentVersion \Winlogon \PasswordExpiryWarning	5(**)	5	14(**)	14
HKLM\Software \Microsoft\Windows NT\CurrentVersion \Winlogon \ScRemoveOption	“0”	“0”	“0”	“0”
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \ConsentPromptBehaviorAdmin	5(**)	5	2(**)	2
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \ConsentPromptBehaviorUser	3(**)	3	1(**)	1

Local Policy Settings	Windows 7 for Experion	Windows 7 defaults	Windows server 2008/2008 R2 for Experion	Windows server 2008/2008 R2 defaults
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \DisableCAD	0	0	0	0
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \DontDisplayLastUser Name	1	(*)	1	0(*)
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \EnableInstallerDetecti on	1	1	1	1
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \EnableLUA	1	1	1	1
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \EnableSecureUIAPat hs	1	1	1	1
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \EnableUIADesktopTo ggle	0	0	0	0
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \EnableVirtualization	0	1(*)	0	1(*)
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \FilterAdministratorTo ken	1	0(*)	1	0(*)
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \LegalNoticeCaption	"Important Notice:"	0(*)	"Important Notice:"	0(*)

Local Policy Settings	Windows 7 for Experion	Windows 7 defaults	Windows server 2008/2008 R2 for Experion	Windows server 2008/2008 R2 defaults
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \LegalNoticeText	“Do not attempt to log on unless you are an authorized user”	0(*)	“ Do not attempt to log on unless you are an authorized user”	0(*)
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \PromptOnSecureDesktop	0	1(*)	0	1(*)
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \ScForceOption	0	0	0	0
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \ShutdownWithoutLogon	1(**)	1	0(**)	0
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \UndockWithoutLogon	1	1	1	1
HKLM\Software \Microsoft\Windows \CurrentVersion \Policies\System \ValidateAdminCodeSignatures	0	0	0	0
HKLM\Software \Policies\Microsoft \Windows\Safer \CodeIdentifiers \AuthenticodeEnabled	0	0	0	0
HKLM\System \CurrentControlSet \Control\Lsa \AuditBaseObjects	0	0	0	0
HKLM\System \CurrentControlSet \Control\Lsa \CrashOnAuditFail	0	0	0	0
HKLM\System \CurrentControlSet \Control\Lsa \DisableDomainCreds	0	0	0	0

Local Policy Settings	Windows 7 for Experion	Windows 7 defaults	Windows server 2008/2008 R2 for Experion	Windows server 2008/2008 R2 defaults
HKLM\System \CurrentControlSet \Control\Lsa \EveryoneIncludesAnonymous	0	0	0	0
HKLM\System \CurrentControlSet \Control\Lsa \FIPSAlgorithmPolicy \Enabled	0	0	0	0
HKLM\System \CurrentControlSet \Control\Lsa \ForceGuest	0	0	0	0
HKLM\System \CurrentControlSet \Control\Lsa \FullPrivilegeAuditing	0	0	0	0
HKLM\System \CurrentControlSet \Control\Lsa \LimitBlankPasswordUse	1	1	1	1
HKLM\System \CurrentControlSet \Control\Lsa \LmCompatibilityLevel	4	(*)	4	3(*)
HKLM\System \CurrentControlSet \Control\Lsa \MSV1_0\NTLMMinClientSec	536,870,912(**)	536,870,912	0(**)	0
HKLM\System \CurrentControlSet \Control\Lsa \MSV1_0\NTLMMinServerSec	536,870,912(**)	536,870,912	0(**)	0
HKLM\System \CurrentControlSet \Control\Lsa \NoLMHash	1	1	1	1
HKLM\System \CurrentControlSet \Control\Lsa \RestrictAnonymous	0	0	0	0
HKLM\System \CurrentControlSet \Control\Lsa \RestrictAnonymousSAM	1	1	1	1

Local Policy Settings	Windows 7 for Experion	Windows 7 defaults	Windows server 2008/2008 R2 for Experion	Windows server 2008/2008 R2 defaults
HKLM\System \CurrentControlSet \Control\Print \Providers\LanMan Print Services\Servers \AddPrinterDrivers	1	0(*)	1	1
HKLM\System \CurrentControlSet \Control \SecurePipeServers \Winreg \AllowedExactPaths \Machine	System \CurrentControlSet \Control \ProductOptions, System \CurrentControlSet \Control\Server Applications, Software \Microsoft\Windows NT\CurrentVersion	System \CurrentControlSet \Control \ProductOptions, System \CurrentControlSet \Control\Server Applications, Software\Microsoft \Windows NT \CurrentVersion	System \CurrentControlSet \Control \ProductOptions, System \CurrentControlSet \Control\Server Applications, Software \Microsoft\Windows NT\CurrentVersion	System \CurrentControlSet \Control \ProductOptions, System \CurrentControlSet \Control\Server Applications, Software \Microsoft\Windows NT\CurrentVersion
HKLM\System \CurrentControlSet \Control \SecurePipeServers \Winreg\AllowedPaths \Machine	System \CurrentControlSet \Control\Print\Printers, System \CurrentControlSet \Services\Eventlog, Software\Microsoft \OLAP Server, Software\Microsoft \Windows NT \CurrentVersion\Print, Software\Microsoft \Windows NT \CurrentVersion \Windows, System \CurrentControlSet \Control\ContentIndex, System \CurrentControlSet \Control\Terminal Server, System \CurrentControlSet \Control\Terminal Server\UserConfig, System \CurrentControlSet \Control\Terminal Server \DefaultUserConfiguration, Software \Microsoft\Windows NT\CurrentVersion \Perflib, System \CurrentControlSet \Services\SysmonLog	System \CurrentControlSet \Control\Print \Printers, System \CurrentControlSet \Services\Eventlog, Software\Microsoft \OLAP Server, Software\Microsoft \Windows NT \CurrentVersion\Print, Software\Microsoft \Windows NT \CurrentVersion \Windows, System \CurrentControlSet \Control \ContentIndex, System \CurrentControlSet \Control\Terminal Server, System \CurrentControlSet \Control\Terminal Server\UserConfig, System \CurrentControlSet \Control\Terminal Server \DefaultUserConfiguration, Software \Microsoft\Windows NT\CurrentVersion \Perflib, System \CurrentControlSet \Services\SysmonLog	System \CurrentControlSet \Control\Print\Printers, System \CurrentControlSet \Services\Eventlog, Software\Microsoft \OLAP Server, Software\Microsoft \Windows NT \CurrentVersion\Print, Software\Microsoft \Windows NT \CurrentVersion \Windows, System \CurrentControlSet \Control\ContentIndex, System \CurrentControlSet \Control\Terminal Server, System \CurrentControlSet \Control\Terminal Server\UserConfig, System \CurrentControlSet \Control\Terminal Server \DefaultUserConfiguration, Software\Microsoft \Windows NT \CurrentVersion\Perflib, System \CurrentControlSet \Services\SysmonLog	System \CurrentControlSet \Control\Print\Printers, System \CurrentControlSet \Services\Eventlog, Software\Microsoft \OLAP Server, Software\Microsoft \Windows NT \CurrentVersion\Print, Software\Microsoft \Windows NT \CurrentVersion \Windows, System \CurrentControlSet \Control \ContentIndex, System \CurrentControlSet \Control\Terminal Server, System \CurrentControlSet \Control\Terminal Server\UserConfig, System \CurrentControlSet \Control\Terminal Server \DefaultUserConfiguration, Software \Microsoft\Windows NT\CurrentVersion \Perflib, System \CurrentControlSet \Services\SysmonLog

Local Policy Settings	Windows 7 for Experion	Windows 7 defaults	Windows server 2008/2008 R2 for Experion	Windows server 2008/2008 R2 defaults
HKLM\System \CurrentControlSet \Control\Session Manager\Kernel \ObCaseInsensitive	1	1	1	1
HKLM\System \CurrentControlSet \Control\Session Manager\Memory Management \ClearPageFileAtShutdown	0	0	0	0
HKLM\System \CurrentControlSet \Control\Session Manager \ProtectionMode	1	1	1	1
HKLM\System \CurrentControlSet \Control\Session Manager\SubSystems \optional	Posix	Posix	Posix	Posix
HKLM\System \CurrentControlSet \Services \LanManServer \Parameters \AutoDisconnect	15	15	15	15
HKLM\System \CurrentControlSet \Services \LanManServer \Parameters \EnableForcedLogOff	1	1	1	1
HKLM\System \CurrentControlSet \Services \LanManServer \Parameters \EnableSecuritySignature	0	0	0	0
HKLM\System \CurrentControlSet \Services \LanManServer \Parameters \NullSessionPipes	(**)		“ browser”(**)	“ browser”
HKLM\System \CurrentControlSet \Services \LanManServer \Parameters \RequireSecuritySignature	0	0	0	0

Local Policy Settings	Windows 7 for Experion	Windows 7 defaults	Windows server 2008/2008 R2 for Experion	Windows server 2008/2008 R2 defaults
HKLM\System \CurrentControlSet \Services \LanManServer \Parameters \RestrictNullSessAccess	1	1	1	1
HKLM\System \CurrentControlSet \Services \LanmanWorkstation \Parameters \EnablePlainTextPassword	0	0	0	0
HKLM\System \CurrentControlSet \Services \LanmanWorkstation \Parameters \EnableSecuritySignature	1	1	1	1
HKLM\System \CurrentControlSet \Services \LanmanWorkstation \Parameters \RequireSecuritySignature	0	0	0	0
HKLM\System \CurrentControlSet \Services\LDAP \LDAPClientIntegrity	1	1	1	1
HKLM\System \CurrentControlSet \Services\Netlogon \Parameters \DisablePasswordChange	0	0	0	0
HKLM\System \CurrentControlSet \Services\Netlogon \Parameters \MaximumPasswordAge	30	30	30	30
HKLM\System \CurrentControlSet \Services\Netlogon \Parameters \RequireSignOrSeal	1	1	1	1
HKLM\System \CurrentControlSet \Services\Netlogon \Parameters \RequireStrongKey	1(**)	1	0(**)	0

Local Policy Settings	Windows 7 for Experion	Windows 7 defaults	Windows server 2008/2008 R2 for Experion	Windows server 2008/2008 R2 defaults
HKLM\System \CurrentControlSet \Services\Netlogon \Parameters \SealSecureChannel	1	1	1	1
HKLM\System \CurrentControlSet \Services\Netlogon \Parameters \SignSecureChannel	1	1	1	1
[Privilege Rights]	[Privilege Rights]	[Privilege Rights]	[Privilege Rights]	[Privilege Rights]
SeNetworkLogonRight	Everyone, Administrators, Users, Backup Operators	Everyone, Administrators, Users, Backup Operators	Everyone, Administrators, Users, Backup Operators	Everyone, Administrators, Users, Backup Operators
SeBackupPrivilege	Administrators, Backup Operators	Administrators, Backup Operators	Administrators, Backup Operators	Administrators, Backup Operators
SeChangeNotifyPrivilege	Everyone, Local Service, Network Service, Administrators, Users, Backup Operators	Everyone, Local Service, Network Service, Administrators, Users, Backup Operators	Everyone, Local Service, Network Service, Administrators, Users, Backup Operators	Everyone, Local Service, Network Service, Administrators, Users, Backup Operators
SeSystemtimePrivilege	Local Service, Administrators	Local Service, Administrators	Local Service, Administrators	Local Service, Administrators
SeCreatePagefilePrivilege	Administrators	Administrators	Administrators	Administrators
SeDebugPrivilege	Administrators	Administrators	Administrators	Administrators
SeRemoteShutdownPrivilege	Administrators	Administrators	Administrators	Administrators
SeAuditPrivilege	Local Service, Network Service	Local Service, Network Service	Local Service, Network Service	Local Service, Network Service
SeIncreaseQuotaPrivilege	Local Service, Network Service, Administrators	Local Service, Network Service, Administrators	Local Service, Network Service, Administrators	Local Service, Network Service, Administrators
SeIncreaseBasePriorityPrivilege	Administrators	Administrators	Administrators	Administrators
SeLoadDriverPrivilege	Administrators	Administrators	Administrators	Administrators
SeLockMemoryPrivilege	Local Servers	(*)	Local Servers	(*)
SeBatchLogonRight	Local Servers, Administrators, Backup Operators, Performance Log Users	Administrators, Backup Operators, Performance Log Users(*)	Local Servers, Administrators, Backup Operators, Performance Log Users	Administrators, Backup Operators, Performance Log Users(*)
SeServiceLogonRight	Local Servers,*S-1-5-80-0(**)	*S-1-5-80-0(*)	Local Servers	(*)

Local Policy Settings	Windows 7 for Experion	Windows 7 defaults	Windows server 2008/2008 R2 for Experion	Windows server 2008/2008 R2 defaults
SeInteractiveLogonRight	Guest, Administrators, Users, Backup Operators(**)	Guest, Administrators, Users, Backup Operators	Administrators, Users, Backup Operators(**)	Administrators, Users, Backup Operators
SeSecurityPrivilege	Administrators	Administrators	Administrators	Administrators
SeSystemEnvironmentPrivilege	Administrators	Administrators	Administrators	Administrators
SeProfileSingleProcessPrivilege	Administrators	Administrators	Administrators	Administrators
SeSystemProfilePrivilege	Administrators,*S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420(**)	Administrators,*S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420	Administrators(**)	Administrators
SeAssignPrimaryTokenPrivilege	Local Service, Network Service	Local Service, Network Service	Local Service, Network Service	Local Service, Network Service
SeRestorePrivilege	Administrators, Backup Operators	Administrators, Backup Operators	Administrators, Backup Operators	Administrators, Backup Operators
SeShutdownPrivilege	Local Engineers, Local Supervisors, Product Administrators, Administrators, Backup Operators	Administrators, Users, Backup Operators(*)	Local Engineers, Local Supervisors, Product Administrators, Administrators, Backup Operators	Administrators, Backup Operators(*)
SeTakeOwnershipPrivilege	Administrators	Administrators	Administrators	Administrators
SeDenyNetworkLogonRight	Guest(**)	Guest	Local Servers, Guest(**)	(*)
SeDenyInteractiveLogonRight	Local Servers, Guest(**)	Guest(*)	Administrators(**)	(*)
SeUndockPrivilege	Administrators, Users(**)	Administrators, Users	Administrators(**)	Administrators
SeManageVolumePrivilege	Administrators(**)	Administrators	Administrators, Remote Desktop Users(*)	Administrators(*)
SeRemoteInteractiveLogonRight	Administrators, Remote Desktop Users(**)	Administrators, Remote Desktop Users	Local Servers, Guest	Administrators, Remote Desktop Users(*)
SeDenyRemoteInteractiveLogonRight	Local Servers, Guest(**)	(*)	Local Service, Network Service, Administrators, Service(**)	(*)
SeImpersonatePrivilege	Local Service, Network Service, Administrators, Service	Local Service, Network Service, Administrators, Service	Local Service, Network Service, Administrators, Service	Local Service, Network Service, Administrators, Service
SeCreateGlobalPrivilege	Local Service, Network Service, Administrators, Service(**)	Local Service, Network Service, Administrators, Service	Users(**)	Local Service, Network Service, Administrators, Service(*)
SeIncreaseWorkingSetPrivilege	Users(**)	Users	Local Service, Administrators(**)	Users(*)

Local Policy Settings	Windows 7 for Experion	Windows 7 defaults	Windows server 2008/2008 R2 for Experion	Windows server 2008/2008 R2 defaults
SeTimeZonePrivilege	Local Service, Administrators, Users(**)	Local Service, Administrators, Users	Administrators(**)	Local Service, Administrators(*)
SeCreateSymbolicLinkPrivilege	Administrators(**)	Administrators	[Version](**)	Administrators(*)

14 Notices

Trademarks

Experion®, PlantScape®, SafeBrowse®, TotalPlant®, and TDC 3000® are registered trademarks of Honeywell International, Inc.

OneWireless™ is a trademark of Honeywell International, Inc.

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Third-party licenses

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third_party_licenses on the media containing the product, or at http://www.honeywell.com/ps/thirdpartylicenses.

14.1 Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at:

http://www.honeywellprocess.com/support

If you have comments about Honeywell Process Solutions documentation, send your feedback to:

hpsdocs@honeywell.com

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

14.2 How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

https://honeywell.com/pages/vulnerabilityreporting.aspx

Submit the requested information to Honeywell using one of the following methods:

- Send an email to security@honeywell.com.

  or

- Contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

14.3 Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx.

14.4 Training classes

Honeywell holds technical training classes on Experion PKS. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see http://www.automationcollege.com.