Automate Comprehensive Security Best Practice Guide

Overview

This guide was created to help partners with an on-premises instance of ConnectWise Automate properly lock down host systems in a manner to offer better protection from a security incident. The guide itself is broken into three elements:

- Operating System
- Network
- Application

Each area should be reviewed and implemented. Please note this document will be updated frequently. Ensure you have the most up-to-date copy.

This guide addresses the following:

- Microsoft Windows Server 2016 & 2019
- Microsoft IIS 10.x
- ConnectWise Automate v2020+

Operating System Hardware Guidelines (Before application install)

Review the Security Technical Implementation Guides (STIGs) as a methodology to secure Microsoft Server 2016 and 2019. Many of the High and Medium standards are addressed inside the AWS Standard Server AMI for the Cloud instances. The user account and STIGs information below are strongly recommended for the ConnectWise Control server.

For on-premises host systems, it is recommended to implement the STIGs located here:

- Server 2016: https://www.stigviewer.com/stig/windows_server_2016/
- Server 2019: https://www.stigviewer.com/stig/windows_server_2019/
- IIS 10: https://www.stigviewer.com/stig/microsoft_iis_10.0_server/

User Accounts and Permissions

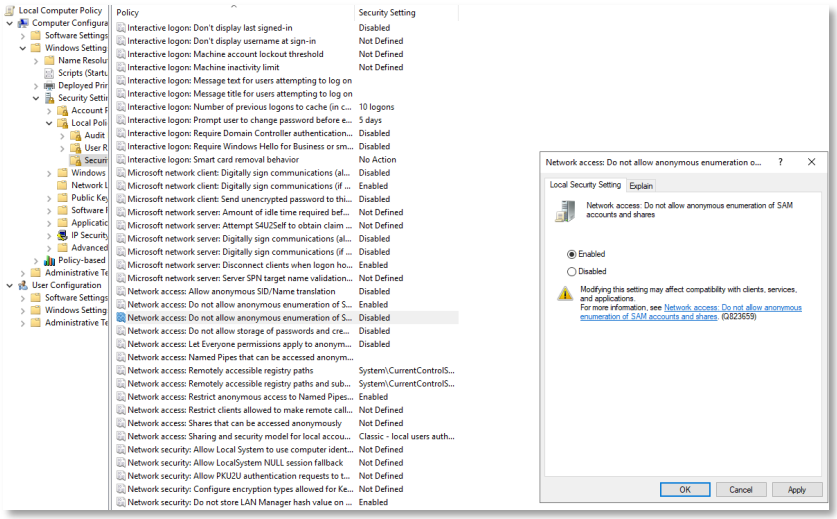
It is highly recommended that user accounts with access to the Control server and all servers, should have non-privileged (non-administrator) access for their initial login. Only users with a need for privileged access to the Control server, or any other server, should be provided a SECOND individual account with ONLY the minimum level of access needed to accomplish their specific job role and function. Limiting user access ensures compliance to the STIG and limits the overall risk exposure for the system and services provided. The assigned privileged account should NOT be used for initial login, and it is recommended that the enforcement of privileged accounts be restricted via GPO on the Control server and across all servers.

STIG Items to Modify

Run **gpedit.msc**.

1. **Network access**.

   Do not allow anonymous enumeration of SAM accounts and shares. Configure the policy value for **Computer Configuration** > **Windows Settings** > **Security Settings** > **Security Options** > Set **Network access: Do not allow anonymous enumeration of SAM accounts and shares** to **Enabled**.



2. **Disallow AutoPlay for non-volume devices**.

   Configure the policy value for **Computer Configuration** > **Administrative Templates** > **Windows Components** > **AutoPlay Policies** > Set **Disallow AutoPlay for non-volume devices** to **Enabled** (Server 2016: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options).

3. **Set the default behavior for AutoRun**.

   Configure the policy value for **Computer Configuration** > **Administrative Templates** > **Windows Components** > **AutoPlay Policies** > Set the default behavior for AutoRun to **Enabled** and select the **Do not execute any autorun commands** option.

4. **Turn off AutoPlay**.

   Configure the policy value for **Computer Configuration** > **Administrative Templates** > **Windows Components** > **AutoPlay Policies** > Set **Turn off AutoPlay** to **Enabled** and select the **All Drives** option.

   The above setting is discussed in some detail within the Certify Fundamentals course available under the ConnectWise University.

   Please ensure NO ONE is added to **Act as part of the operating system** in the GPO.

5. **Verify the effective settings within the Local Group Policy Editor**.

Navigate to **Local Computer Policy** > **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**.

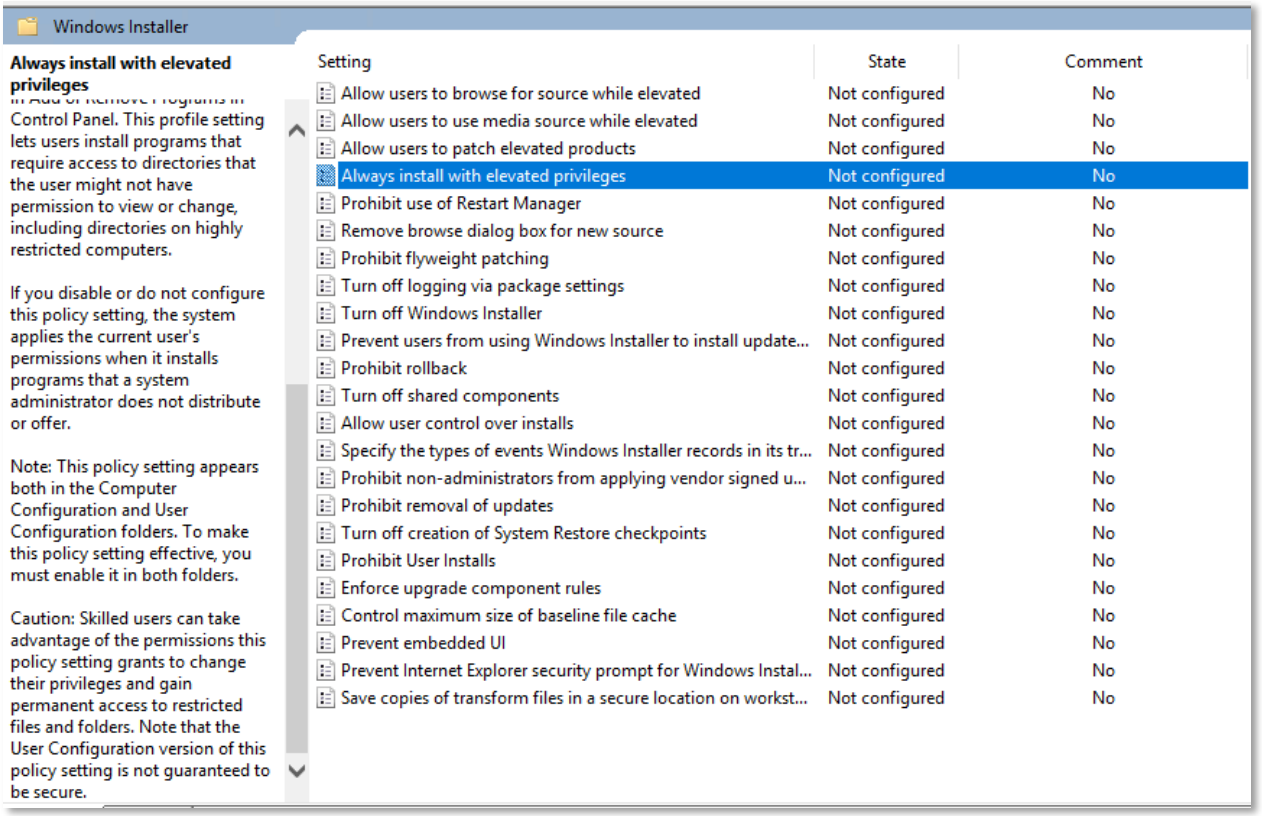
If any accounts or groups (to include administrators) are granted the **Act as part of the operating system** user right, the accounts should be removed immediately from this policy object.

Another setting to pay attention to on all Microsoft Windows Servers is the privilege escalation.

6. **Always install with elevated privileges**.

   Configure the policy value for **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Windows Installer** > Set **Always install with elevated privileges** to **Disabled**.

The **Not Configured** setting uses the user's current permission set. This is part of the reason having TWO accounts is very important. Please also note the Caution item in the following graphic.



Additionally, Microsoft Windows Server administrative accounts must not be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email.

Using applications that access the Internet or have potential Internet sources using administrative privileges exposes a system to compromise. If a flaw in an application is exploited while running as a privileged user, the entire system could be compromised. Web browsers and email are common

attack vectors for introducing malicious code and must not be run with an administrative account. Since administrative accounts may generally change or work around technical restrictions for running a web browser or other applications, it is essential that policy require administrative accounts to not access the Internet or use applications such as email. The policy should define specific exceptions for local service administration. These exceptions may include HTTP(S)-based tools that are used for the administration of the local system, services, or attached devices. Whitelisting can be used to enforce the policy to ensure compliance.

Network Hardening Guidelines

Windows Defender Firewall on Automate Server

Verify that only the following ports are open:

- Port 75 UDP: Utilized by the Enhanced Heartbeat.
- Port 443 TCP: Used for HTTPS communication.
- Port 8484 TCP: Must be open and forwarded to the Automate server in order to access the Solution Center from Control Center.
- Local machine access 127.0.0.1 on any port from 127.0.0.1 using any protocol should be opened (local machine access).

Verify the following ports and protocols are close:

- Port 70 TCP: Redirector communications without tunnels.
- Ports 70-74 UDP: Tunnels and Redirectors.
- Port 8002 TCP/UDP: For tunnels, the remote agent and the Control Center must be able to communicate to mediator.labtechsoftware.com on port 8002 TCP/UDP.
- Ports 40000-40050 TCP: Connecting via HTTP from the Web Control Center. Open ports beginning with 40000 and ending with four times the number of total technicians using Automate (e.g., If there are 25 technicians, then there are 25x4 (100) simultaneous sessions. So, ports 40000-40100 should be open).
- Ports 40000-41000 UDP: Tunnels and Redirectors, only when advanced routers are blocking and not at the Automate server, at client and agent locations or where the router in front of the Control Center is blocking.
- Port 3389: Windows RDP. This can be disabled after a ConnectWise Control client is running or there is another way to access the system. Also ensure that the perimeter firewall is blocking port 3389 for all machines.
- Port 3306: MySQL. Block this port on the perimeter router. If using a single system for Automate and database, 3306 should only be available locally. If using two separate systems, 3306 on the database machine should only be available on the private network and only accessible from the Automate machine.

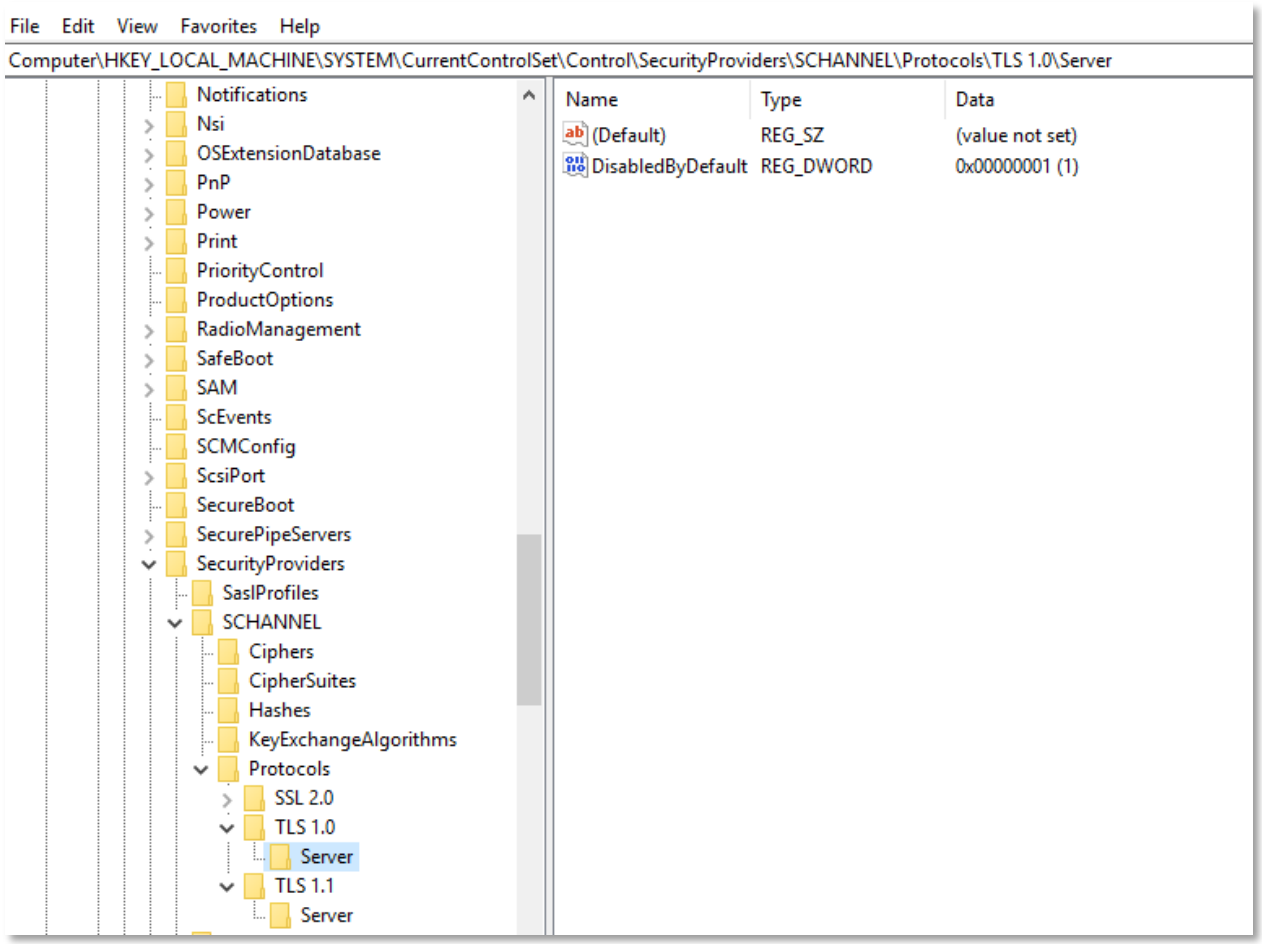
If not connected to Active Directory, these ports can be blocked.

- Port 135: MSRPC. Remove firewall rule to allow TCP-135.

- Port 139: NetBios. Remove firewall rule to allow TCP-139.
- Port 445: Microsoft-ds. Remove a firewall rule to allow TCP-445.

Disable TLS 1.0 and 1.1 in the registry:

1. Open the **Registry Editor**.
2. Navigate to *HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols*.
3. TLS 1.0 or 1.1 entry does not exist in the registry by default.
4. Create a new subkey called **TLS 1.0 or 1.1** under **Protocols**.
5. Create a new subkey called **Server** under **TLS 1.0 or 1.1**.
6. In the **Server key**, create a **DWORD DisabledByDefault** entry and set the value to **1**.
7. Reboot the server.



Application Hardening Guidelines

Additional Automate Hardening Items

- Set the Automate system password with a minimum of 12 characters and a mix of uppercase, lowercase, numbers, and symbols.
- Set the MySQL Root password with a minimum of 12 characters and a mix of uppercase, lowercase, numbers, and symbols.

Permissions

For the *C:/LTShare* directory, ensure that all permissions are removed for the EVERYONE group. Configure the minimum permissions for LTShare for the following:

- IIS AppPool\LabTech
- IIS AppPool\LabTech WebCC
- IIS AppPool\CwaRestApi
- System

The three IIS AppPool accounts should only have the following permissions applied:

- Modify
- List folder contents
- Read & Execute
- Read
- Write

IIS Hardening Items

HTTP Headers

Validate they are not disabled. Open PowerShell as Administrator, copy, and paste the following command:

```
Get-WebConfigurationProperty -pspath machine/webroot/apphost -filter
'system.webserver/security/requestfiltering' -name 'removeServerHeader'
```

Use the following command to disable server headers in IIS10:

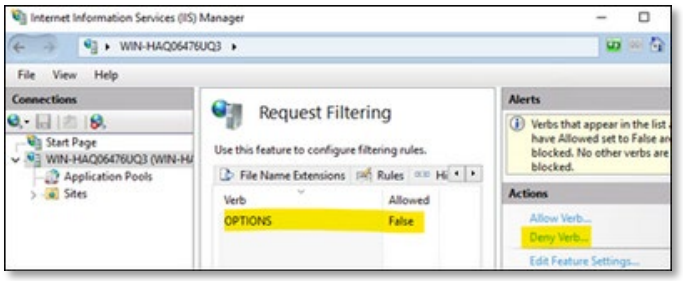
```
Set-WebConfigurationProperty -pspath MACHINE/WEBROOT/APPHOST -filter
"system.webServer/security/requestFiltering" -name "removeServerHeader"
-value "True"
```

Under HTTP Response, remove all entries:

Disable HTTP Options

To disable the Options method:

1. Open the **IIS Manager**.
2. Click on the server name.
3. Double-click on **Request Filtering**.
4. Select the **HTTP Verbs** tab.
5. On the right side, click **Deny Verb**.
6. Type **OPTIONS**.
7. Click **OK**.



API Integrations

For Control Partners:

- Server Requirements:
  - ConnectWise Automate v2019.1+
  - TCP Ports 8040 and 8041 forwarded to the ConnectWise Control server (for alternate ports, refer to Control's Changing Default Ports documentation. If using a ConnectWise Control Cloud server, port 443 is required.
- Supported Versions:
  - Control v6.4+
  - Control Remote Support and Meetings requires Control v6.4+

Permissions

Accessing features of the ConnectWise Control solution requires the user to be associated with a user class with the following permissions.

Task	Class	Level	Category
Access ConnectWise Control plugin	Plugin	User	ConnectWise Control plugin > Access
Access ConnectWise Control Remote plugin	Plugin	User	ConnectWise Control Remote plugin > Access
View Support Sessions	Plugin	User	ConnectWise Control plugin > View Support Sessions > Access

Print Over Session	Plugin	User	ConnectWise Control plugin > Print Over Session > Access
Transfer Files in Session	Plugin	User	ConnectWise Control plugin > Transfer Files in Session > Access
Use Shared Toolbox	Plugin	User	ConnectWise Control plugin > Use Shared Toolbox > Access
Manage Shared Toolbox	Plugin	User	ConnectWise Control plugin > Manage Shared Toolbox > Access
Access Backstage via the Web Control Center	Plugin	User	ConnectWise Control plugin > Manage Credentials > Access
Switch Logon Session	Plugin	User	ConnectWise Control plugin > Switch Logon Session > Access Note: This permission is required for Control Backstage.
Access Support Session Viewer	Web Extension	User	ConnectWise Control plugin > Support Session Viewer > Access
All tasks listed below require the Access ConnectWise Control plugin permission.			
View script statuses during server installation on an agent	Core	User	Scripts > Read
Configure plugin	Core	User	System Dashboard > Config > Access
Connect to computer	Core	Client and/or Group	Allows Redirector/Remote Control
Install, uninstall, enable or disable the Control Client	Core	Client and/or Group	Send Commands
Establish a remote control session from Web Control Center	Core	User	Allow Web Access