Third Wall™ V2.5 Operational Instructions

CURRENT RELEASE v2.5.0.2

Thank you for purchasing your license to Third Wall, our powerful new system for extending the functionality of your ConnectWise Automate® Software. Please read the document below thoroughly before you continue with your Third Wall™ implementation, and use this as a reference document for questions you may have. It describes in detail what you can expect from our plugin.

Third Wall works only on these machines: Windows 7 (with Service Pack 2), Windows 8/8.1, Windows 10, Windows Server 2012, Windows Server 12 and Windows Server 2019. It does not work with MacOS or Unix machines.

***Philosophy of managing user devices: principle of least privilege through system hardening*.** From a security standpoint, it's best to give users and environments the necessary software and system privileges to conduct their job *and nothing more.* When users are given more privileges than they need to do their job, the chance of a security incident occurring increases. Also, the more software applications installed on a system, the more vulnerabilities and attack vectors exist into the system. By reducing software and rights to those only necessary to conduct business, the number of vulnerabilities and attack vectors likewise decreases. As a general rule, every single software application has intrinsic vulnerabilities, some known while others unknown. Thus, removing an unused software application or unneeded system privileges can significantly reduce the likelihood of a security incident. The overall process of removing unneeded software and privileges is called 'system hardening.' *Third Wall™ greatly improves your ability to accomplish system and endpoint hardening.*

What's New in V2?

With V2, you will notice many important changes. These include:

A completely new UI, both on the Third Wall Location tab and on the Third Wall Computer tab. The new look and feel is more consistent with Windows 10®, and substantially enhances your experience.

A new Overview page on the Third Wall Location tab that shows you at a glance the status of all of your policies for that Location, on a color-coded, information-packed display.

What can you do with Third Wall™?

Once you've installed Third Wall, you can do the following activities. More details are provided later in this document.

- **Apply new policies** across an entire Location, Client or all of your computers. By doing this, you will be launching a monitor for each policy selected. That monitor will check every computer, and will, for all that do not comply with the desired policy state, change the state of those computers. Then the monitor will continue to stay active, ensuring that the state remains as set by the policy.
- **Make exceptions** on any computer for any policy, which reverses the impact of the policy, if already enabled, and prevents future impact to this computer.
- **Remove policies** across an entire Location. This will turn off a monitor, but will not change the state of any computer.
- **UNDO policies** across an entire Location This immediately removes the policy and changes the state of all impacted computers, usually to Windows

The ability to apply a Profile (a saved configuration of Third Wall policies) to a different Location, across an entire Client or even across all of your Windows® computers.

A change in how to apply the UNDO function for any Location policy. Instead of using the "filled in box," as was the technique for V1, you will get an "UNDO" link appearing if and only if you have the policy turned on. Clicking on the UNDO link is now the method for implementing an UNDO on a policy.

On the Third Wall Computer tab, you will no longer have the option to apply an exception without executing an UNDO. If you make an exception to any policy, Third Wall will execute an UNDO on that computer as part of applying that exception.

We've added the capability to make many Location UNDOs and computer exceptions temporary. Whenever you select a Location UNDO, or a computer exception (which now automatically executes an UNDO), you may get a popup asking if you want to make the UNDO permanent or temporary. If you select Temporary, then you must select a duration for that UNDO or exception to apply; at the end of that timer, the policy will retake control of that Location or computer.

We've added 27 new policies you can apply. These add tremendous new power to Third Wall. Please see the full description of these added policies in the details section later in this document. Here is a list of the added or modified policies:

NEW policies

- Set Local Administrator Password
- Disable Local Administrator Account
- Enforce Password Complexity
- Restrict WinKey +R (WinRun)
- Restrict Powershell Script
- Disallow Running 'setup.exe' and 'install.exe'
- Disable Windows 10 Keylogger
- Disable Terminal Services (RDP) – on V2.2 and later
- Enable SmartScreen
- Disable .exe Running from AppData
- Disable Write to Optical Media
- Disable Read / Write to Optical Media
- Enable USB Wall – a PREMIUM TIER feature available on v2.2 and later
- Disable Read / Write to USB Storage Devices
- Disable Common Cloud Storage (Dropbox, etc.)
- Schedule Secure Free-Space Delete
- Uninstall Blacklisted Applications
- Prevent Public Webmail Access (Yahoo, etc.)
- Prevent Social Media Access (Facebook, etc.)
- Disable Google Play
- Disable Apple App Store
- Disable Office Macros from Internet
- Disable OLE in Office Documents

- Enable Windows Firewall – Workstations (configurable)
- Enable Windows Firewall – Servers (configurable)
- Disable NetBios
- Enable User Logon Reporting
- Alert on Excessive Logon Failures
- Monitor for Ransomware

MODIFIED policies

- Select different levels of UAC enforcement
- Select “all” or “Unmanaged” for MSI restrictions on Disable Windows Installer
- Secure Free-Space Delete is now a Location policy rather than a computer action button

We’ve also added two new powerful reports:

- Client audit report showing all policies and exceptions in place, and including dates they were implemented – giving you an excellent audit compliance tool
- Logon / Logoff report by User, including Dataviews for deeper drilldown

And we’ve enhanced the Instant Action Buttons on the Computer tab:

- The Emergency Lockout button will log all Users out and disable all Local User accounts (same as V1)
- Screen Lock will simply put the computer into the locked screen state – anyone with logon credentials can sign back in. This will prevent an end user from losing unsaved documents / data that would have happened if you used the Emergency Lockout button.
- The Emergency Isolate button now will retain connection not only to the ConnectWise Automate server, but also to the ConnectWise Control server, if it is separate.
- The Annihilate Button now offers three options:
    - Same as V1 – delete My Documents and then initiate a %windir% (operating system) and a registry destruction routine.
    - Delete My Documents, then do a “secure free space delete” to fully wipe deleted data, then initiate registry destruction routine.

We’ve changed the architecture to make Third Wall execute much more quickly, switching from scripts to .net commands to create action. You will notice far less lag. This also creates a much more benign face to your antivirus, minimizing the potential for your antivirus package to mistake Third Wall as malware.

To assist in deploying a desired policy configuration across multiple Locations easily, Third Wall now has the ability to save a Profile configuration of “best practice” policy settings, and to copy policy settings from one Location to another, including the ability to copy automatically to all Locations of a given Client, or to all Locations on the ConnectWise Automate server.

What you will see when you install Third Wall™ on your ConnectWise Automate® Control Center

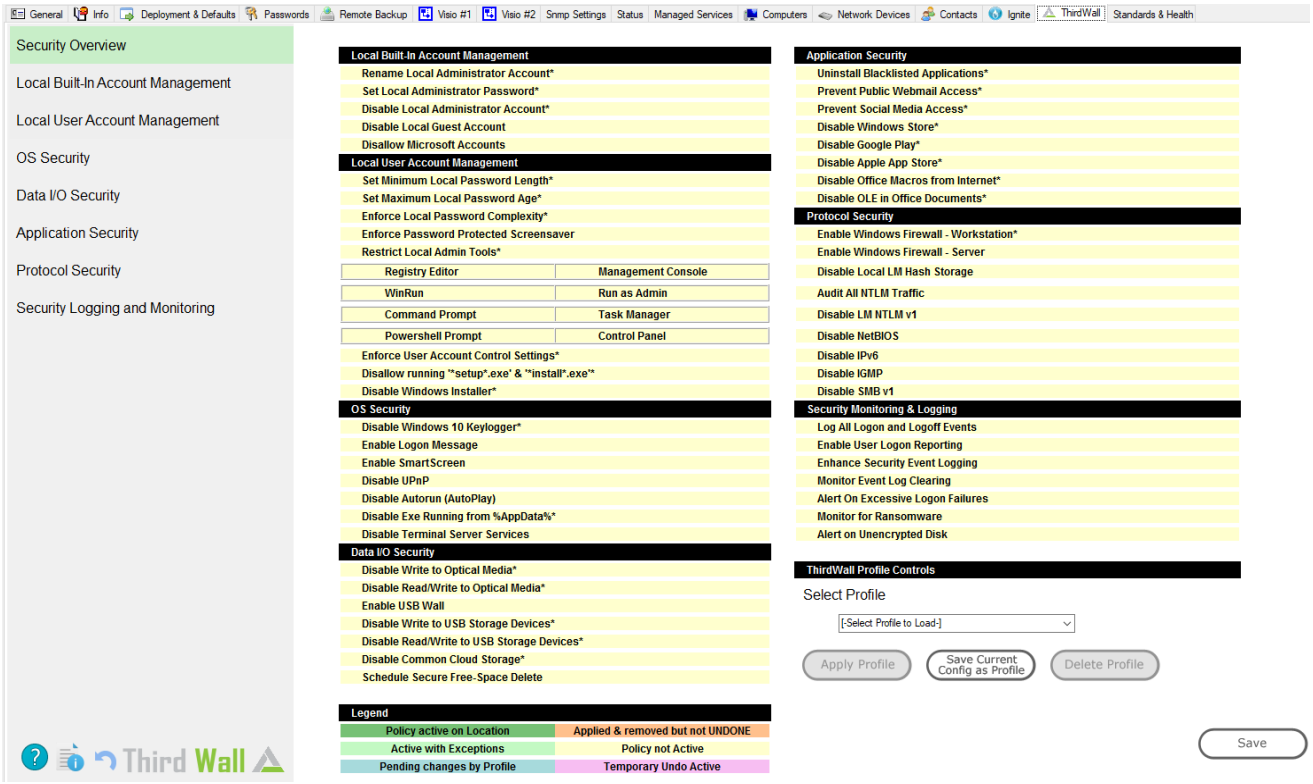
Third Wall™ adds several new screens to your ConnectWise Automate® Control Center: one for your Location Screen, one for your Computer Screen, two on the Client screen, and one on the Integration screen (see screenshots below). The new tab on your Location Screen is used to set and remove new Third Wall™

policies that are available for you – and these will then apply across that entire Location, as you would expect. The new tab on your Computer Screen is used to make exceptions for any single computer, so that the Third Wall™ policy Applied to that Location will NOT Apply to that computer; and to apply key "emergency actions" to individual computers as needed. You can exclude any computer from any policy, either permanently or temporarily. The two screens on the Client screen are used to register USB sticks for the USB Wall policy, and to set Client-level exceptions to the Disable EXE Running from %AppData% policy. The Integration screen allows you various global settings, including AppData whitelisting, setting of a default Alert Template, and setting of a default Ticket category.

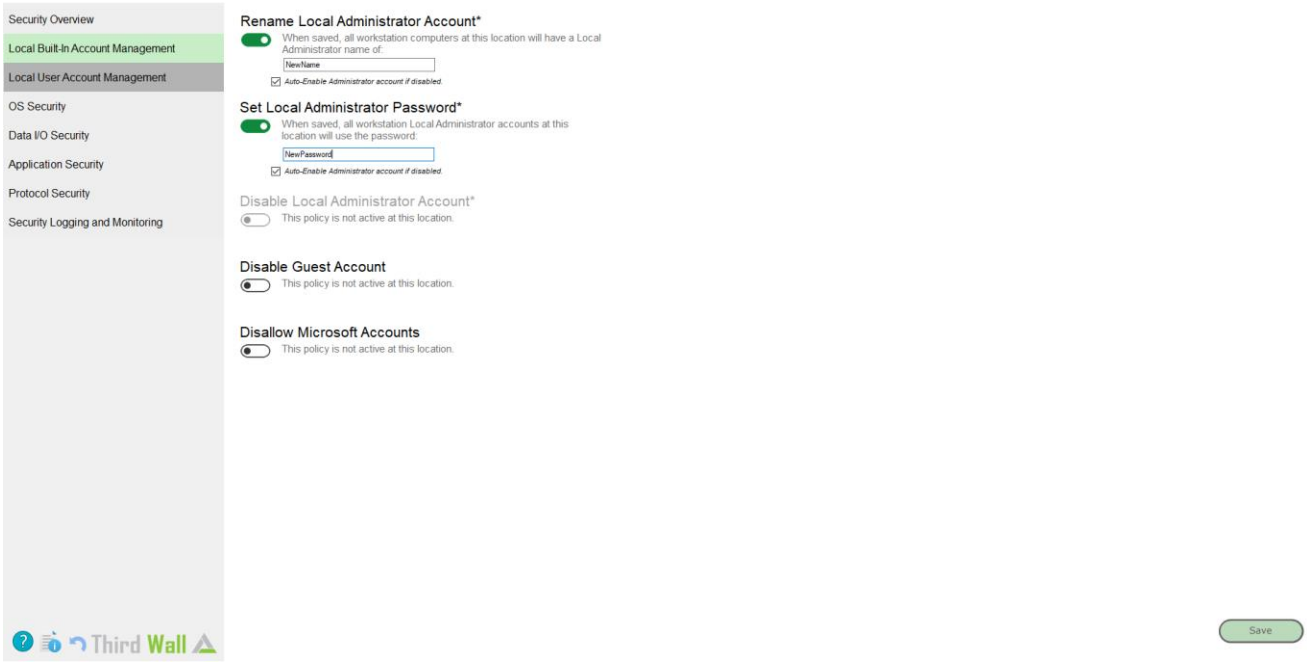
Most of the policies of Third Wall™ are applied by switches, turning on or off as appropriate. Also, once you have applied a policy you will notice that an "UNDO" link appears for that policy. At this point, should you decide to "unapply" or remove the policy across that Location, you have two options: either simply turn it off using the switch, which only removes the monitor associated with that policy (NOT recommended); or click the UNDO link to remove all restrictive settings or revert them back to default, and also remove monitor going forward (recommended).

That's it! Third Wall™ is very powerful, but very simple to use. We do strongly urge you to familiarize yourself with this document prior to jumping into Third Wall™ – as you know, applying policies without full understanding of what they do is not a recommended practice.

SCREENSHOT – Location Overview Page in Location Tab

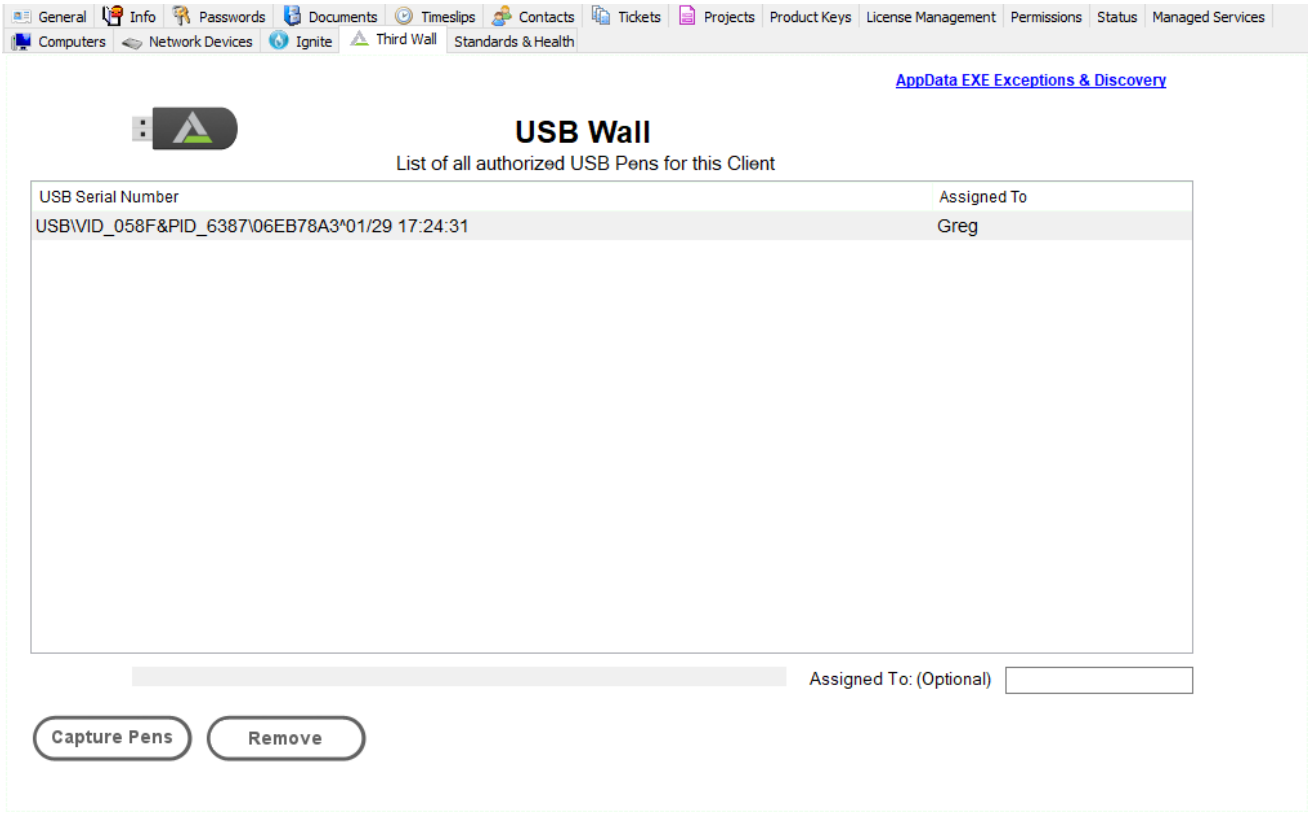


SCREENSHOT – one page of Policy Application pages in Location Tab

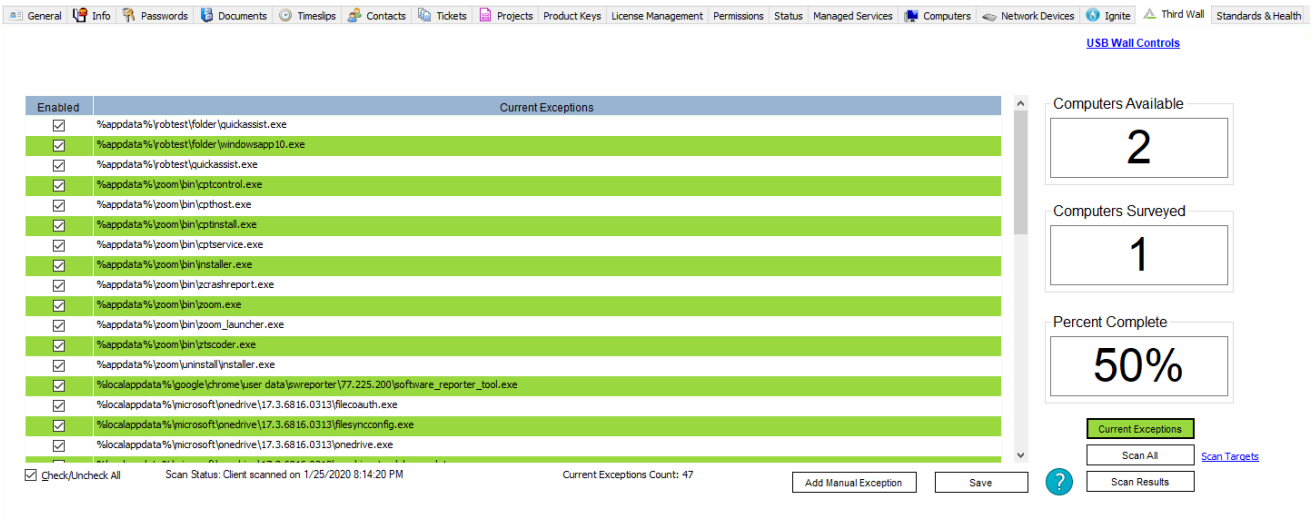


SCREENSHOT – Computer (Exceptions) Page

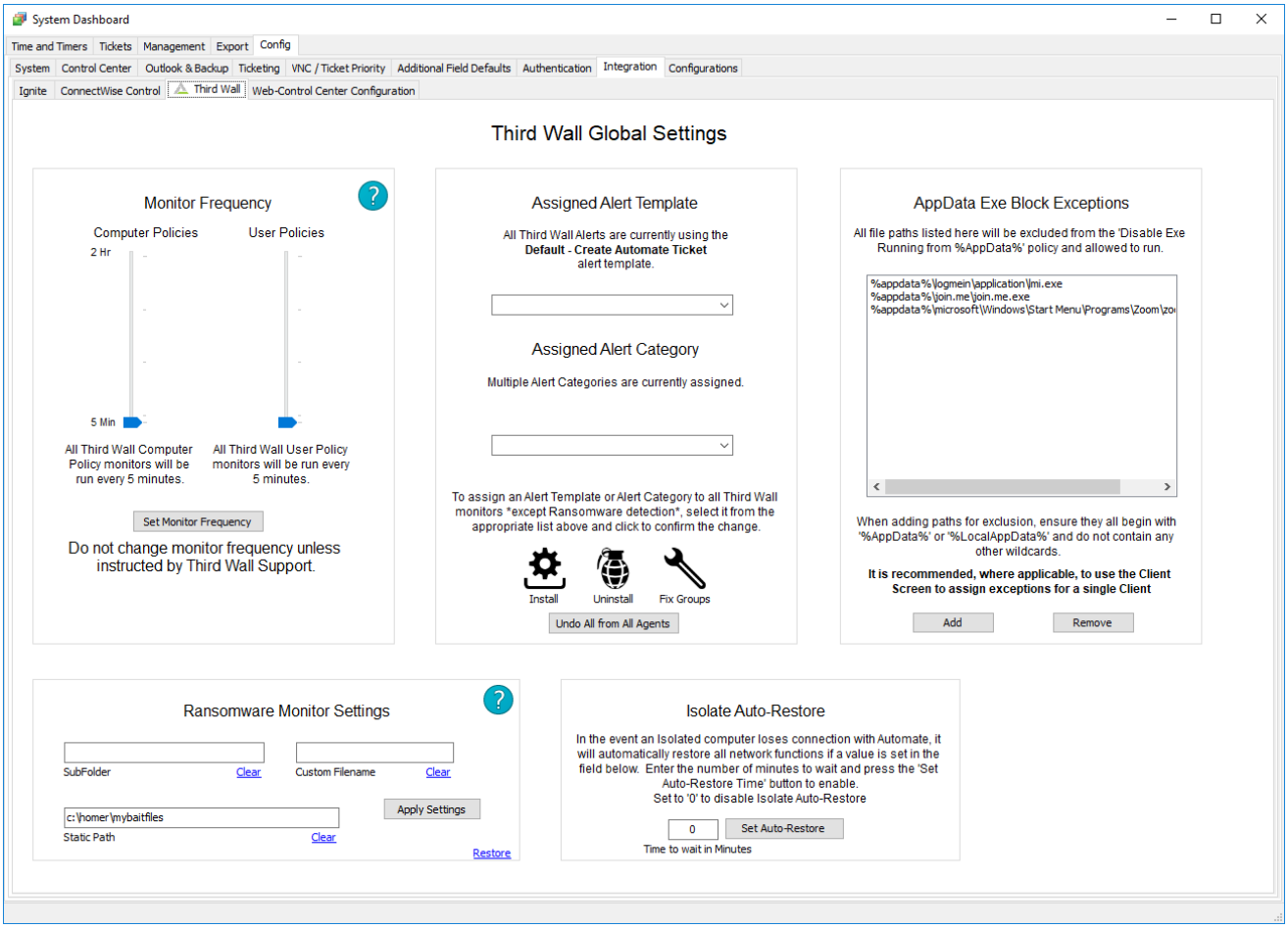
SCREENSHOT – USB Wall Registration Page



SCREENSHOT – Third Wall %AppData% Exceptions & Discovery Screen



SCREENSHOT – Third Wall Integration Page (Dashboard > Config > Integration > Third Wall)



General Behavior of Switches on Third Wall™ Location Screen:

On the **Location Screen** – impacts all computers in that ConnectWise Automate Location

- Switch On – Apply Third Wall™ policy, including monitor, for ALL computers in Location.
- Switch Off – remove Third Wall™ monitor only. NOT RECOMMENDED.
- UNDO (click on the link if present) – removes the Third Wall™ monitor for that policy, and changes the setting on all computers in that Location (other than those with Exceptions) back to either Windows® defaults or to a pre-Third Wall™ state. The UNDO action on some policies will generate a Popup, asking if you want to make the UNDO permanent or temporary, and will automatically save / execute once you confirm. A temporary UNDO selection will also generate a timer for you to specify the duration of the temporary state.
- NOTE: you must hit the "Save" button on the Location Screen to cause any changes other than UNDO to take effect.
- Some policies will not execute a true UNDO, as it makes no sense for those policies. The following policies, when UNDO is selected, will simply turn off the Third Wall monitor:
    - Set Local Administrator Password
    - Disable Local Guest Account
    - Schedule Secure Free Space Delete
    - Uninstall Blacklisted Applications
    - Monitor Event Log Clearing
    - Alert on Excessive Logon Failures
    - Alert on Unencrypted disk
- Temporary UNDO is available for all policies except:
    - Rename Local Administrator Account
    - Set Local Administrator Password
    - Disable Local Guest Account
    - Set Minimum Local Password Length
    - Set Maximum Local Password Age
    - Enforce Password Complexity
    - Enforce Password Protected Screensaver
    - Block Windows 10 Keylogger
    - Enable Logon Message
    - Enable USB Wall
    - Schedule Secure Free-Space Delete
    - Uninstall Blacklisted Applications
    - Audit All NTLM Traffic
    - Log All Logon and Logoff Events
    - Enable User Logon Reporting
    - Enhance Security Event Logging
    - Monitor Event Log Clearing
    - Alert on Excessive Logon Failures
    - Monitor for Ransomware
    - Alert on Unencrypted Disk

General Behavior of Switches on Third Wall™ Computer Screen:

On the **Computer Screen** – impacts single computer only

- Switch On – executes UNDO and excludes that computer from the Third Wall™ monitor. You may check this box before or after applying a policy on the Location Screen. If before, it will prevent application of that policy on this computer. If after, it will UNDO the policy on this computer, and will prevent further application of that policy on this computer. When you Switch On exceptions for any policy which is enabled on that Location, you will be prompted to select either Permanent or Temporary exception, and, if you choose Temporary, select a time period to remain excluded.
- Switch Off – enables Third Wall™ monitor to Apply the corresponding policy to that computer (will cause Location Policy, if active, to reapply).

Interaction Between Location and Computer Screen Settings	
Location Screen setting	**Computer Screen setting**
Switch Off: No policy is set.	**Off**: No impact.
	On: this computer's settings for this policy will reset to default setting. Should you turn on the corresponding policy later, this computer will not apply the policy.
Switch On: Policy is set across entire location, and Third Wall™ monitor is enabled to ensure that no computer reverses that policy other than through Third Wall™ Computer Screen.	**Off**: No exception is made on this computer for this policy. The policy will be applied.
	On: The Third Wall™ monitor for this computer will be disabled, and this computer's settings for this policy will reset to Windows® default setting or to a pre-Third Wall™ state for this policy only. Sys Admin, End Users and even malware can change settings on this policy and Third Wall™ monitor will not detect it.

NOTIFICATIONS

Ticket – you will receive a Ticket on your ConnectWise Automate® Control Center for any failed attempt by Third Wall™ to change a value on a computer based on application of a policy or an Undo. Also, Third Wall policies / monitors will generate a ticket if they detect states of violation of policy. For most policies, this Ticket will be automatically resolved within a few minutes by Third Wall, as it corrects the condition. If Third Wall fails to correct the condition, the ticket will remain open. Certain policies will never resolve a ticket: Monitor for Event Log Clearing; Alert on Excessive Logon Failures; Monitor for Ransomware; and Alert on Unencrypted Disk.

No Notification – you will not receive notification if no value was changed or attempted to be changed by application of a Third Wall™ policy or Undo (i.e., the value was already in the desired state).

DEPENDENCIES

Certain Third Wall policies have dependencies on other policies being active before you can apply them. If you select a dependent policy when the prerequisite is OFF, then you will be prompted to decide if you want to turn the prerequisite on. Conversely, if you try to turn a prerequisite OFF while one or more dependent policies are ON, then you will be warned that turning off (or performing an UNDO) will turn the dependent(s) OFF as well. Key dependencies are:

Prerequisite	**Dependent(s)**
Log All Logon and Logoff Events	Enable User Logon Reporting Alert on Excessive Failed Logon Events

General Information

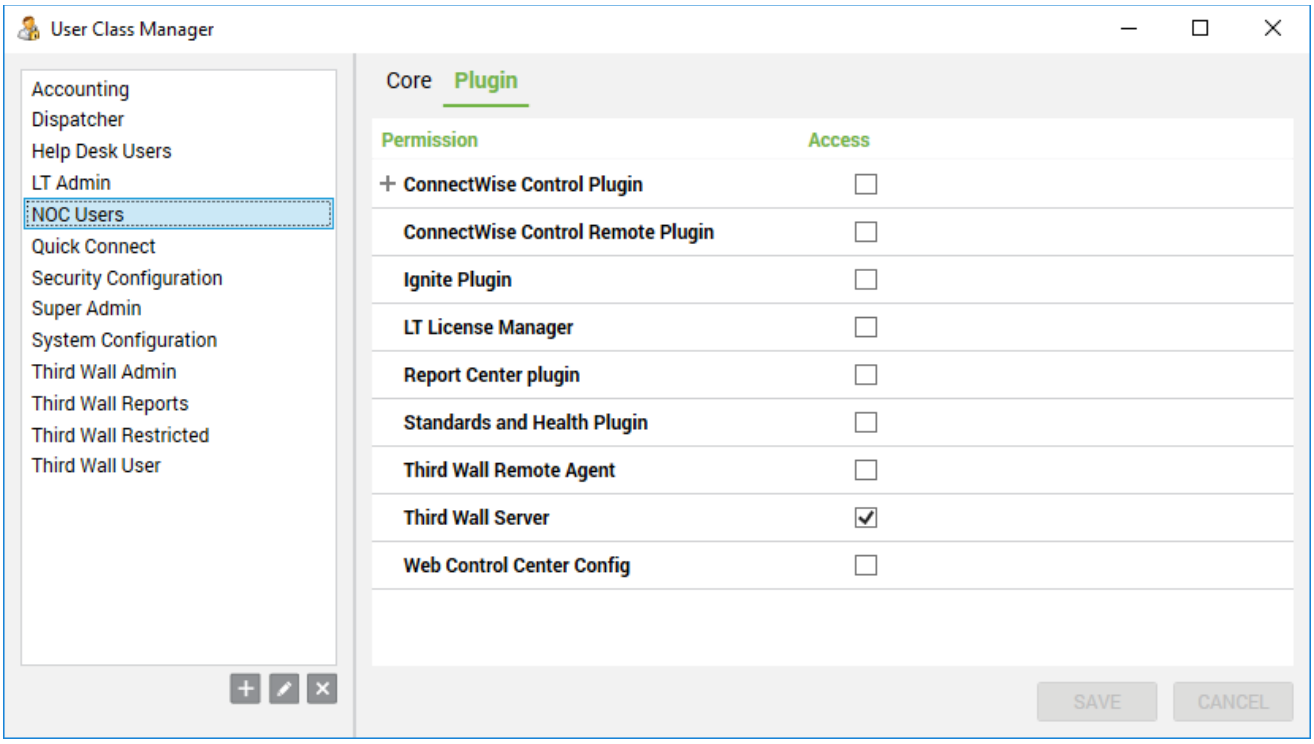
1. Third Wall™ works only on Windows® machines. It will not apply on MacOS or Unix machines. Within Windows, it will work only on Windows® 7 (with Service Pack 2) or later, and, for servers, only on Windows® Server 2008 or later. All other computers will be ignored.
2. All Third Wall™ policies will work on computers regardless of whether they are members of a Domain or not, as long as they have an Automate agent installed. However, in order to initially apply settings and a monitor, all Third Wall™ policies and functions do require that the target computer(s) be connected to ConnectWise Automate – thus, they must be connected to the network or to the internet, and must have an installed / active Automate agent. If any computer is not connected, then once it connects, the action will be accomplished.
3. Some policies will be restricted to run only on Windows® workstations and not on Windows® servers; these are annotated within the Third Wall™ Location Screen by an asterisk.
4. In order to use the following functions, as User must be designated as a Third Wall Admin: applying a Profile, executing the Annihilate emergency action button, performing a Location UNDO, and all of the functions on the Third Wall Integration page.
5. No Third Wall™ policies will interact with the end user during application (i.e., no popup boxes, requests for permission, etc.). Once a policy is applied, by switching the appropriate switch, it will be broadcast and executed on all computers within the Location (excepting those excluded by Computer Screen selections) without end user notification or prompting. Be aware that subsequent end user interactions may cause related messaging to the end user (e.g., If Disable Write to USB is selected and the end user attempts to write to a USB device, an error will be displayed.) Additionally, for each policy selected, a Third Wall monitor will be launched to ensure that no computers in that Location, other than those designated for exception on the Computer Screen, are changed from the desired settings for that specific policy; if a state change occurs, the monitor will correct it back to the desired state and will notify IT via a ticket on the ConnectWise Automate® Control Center.
6. Turning a Policy Off on the Location Screen, without performing an UNDO, will not cause any state change on any computer within that Location. However, it will disable the Third Wall monitor for that policy, allowing the state to be changed by the end user, system technician or even malware. This is not recommended – consider performing an UNDO to fully remove a policy.
7. Conflicts with Active Directory policies: It is possible to assign Domain (Group) Policies that run counter to Third Wall™ settings. In this condition, both changes will impact the target computers but at different intervals. Active Directory changes will be applied at the Domain's Group Policy refresh interval and Third Wall™ changes will be applied at the Third Wall monitor refresh interval. Each change attempt will be successful, resulting in constantly changing policies. Each time that Third Wall changes a setting in this situation, you will receive a ticket. This condition should be expressly avoided.
8. When a Third Wall™ monitor performs a change on a computer, a ticket within ConnectWise Automate® will be generated with applicable notes listed within the contents. However, upon initial activation of a policy, no ticket will be generated for changes made.
9. When a Third Wall™ change attempt fails, a Ticket within ConnectWise Automate® will be generated alerting you to the failure and where possible, the reason why.

APPLYLING PERMISSIONS

View Permissions

Users with restricted permission in Automate may not be able to see the Third Wall tabs on the various screens. To correct this condition, use the User Class Manager in Automate to assign view permissions.

Third Wall recommends assigning access rights for 'Third Wall Server' to NOC Users, as shown below. You may assign this right to more than one User Class and any member of that User Class will now be able to view Third Wall tabs.



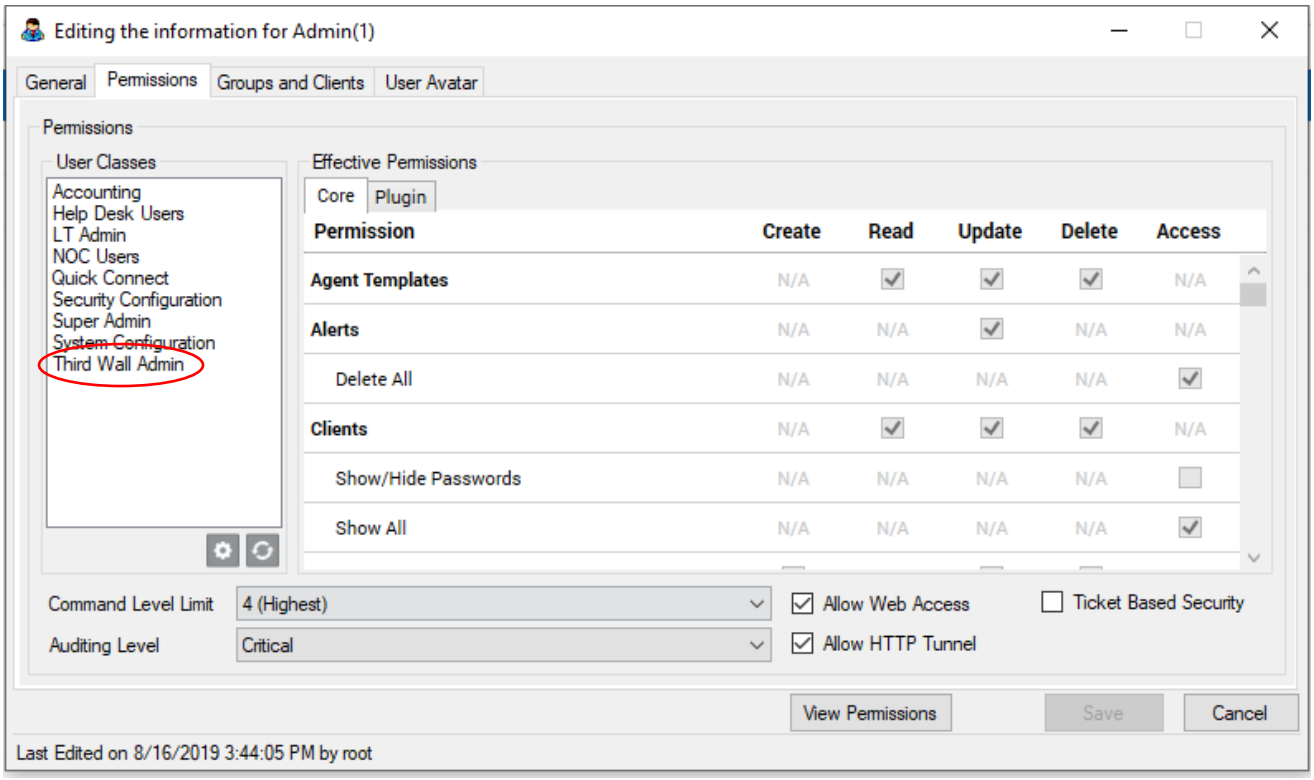
Access Permissions

Default permissions for ALL users includes access to all functions except:

- The dropdown list for Profile application
- The UNDO ALL button on the Location screen
- The ANNIHILATE button on a Computer screen
- The functions on the Integrations > Third Wall screen

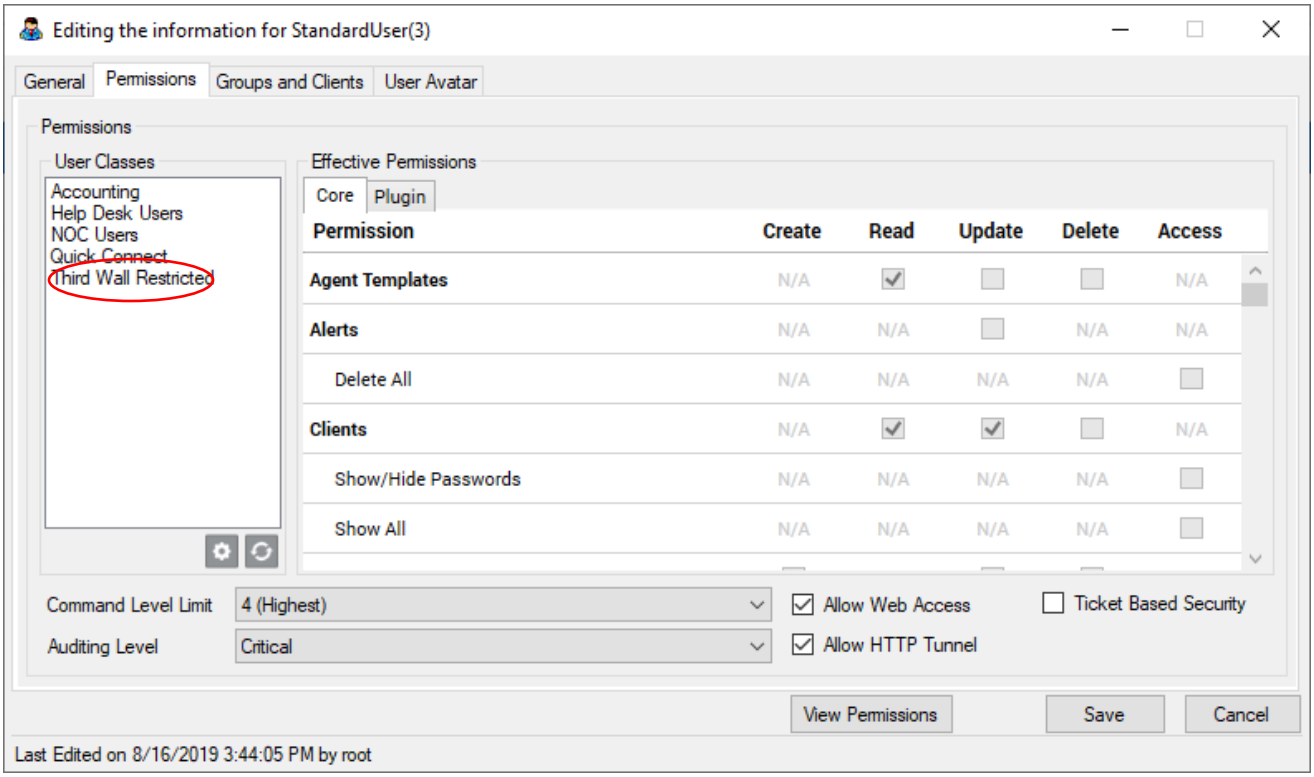
To get access to those function, you must be a Third Wall Admin; even a SuperAdmin will not be able to access these functions. Any Automate SuperAdmin can grant this permission.

1. Open the Users page in Automate, or expand your tree to see Users.
2. Expand the User category, and then double-click the user who will be receiving privileges.
3. Select the Permissions Tab, then right click in the User Classes box, and select Third Wall Admin. Click SAVE to save your changes, and then follow the prompts



Conversely, you may restrict access further to “read only” on the Location screen. This effectively limits a User to just the Exceptions on the Computer screen, plus the Isolate, Screen Lock and Lockout buttons on the Computer screen.

To apply this, assign them to the ‘Third Wall Restricted’ User Class.



Going forward, any users that are a member of the 'Third Wall Restricted' user class that open the Third Wall Location screen will find all controls disabled.

APPLYING POLICIES

Applying policies for a Location is the primary action for Third Wall, enabling protection across all computers within that Location.

To start applying policies, open a Location page and navigate to the Third Wall tab. You will see the default page – the Security Overview – which is a color-coded map of the current state of policies within that Location. The colors signify:

- Yellow – policy not active / not applied
- Green – policy active, along with the date activated
- Light green – policy active, but at least one computer has an exception applied to that policy
- Orange – policy was activated, but then turned OFF without performing an UNDO. NOT RECOMMENDED
- Pink – policy was activated, but now has a Temporary Suspension / UNDO applied
- Blue – pending changes from application of a profile (see Applying Profiles, below)

Although most colors will update right away, you may need to refresh the screen by closing and reopening the Location screen.

The Security Overview page also has the Profile application function, where you can apply a saved configuration across an entire Location, and entire Client, or all of your managed computers (see Applying Profiles, below). Otherwise, there are no available functions on the Security Overview page.

To make changes, you will need to use the navigation tabs on the left side of the Third Wall Location screen. Each of them corresponds to a major grouping of policies, as delineated with the black-bar titles on the Security Overview page. This allows you to quickly find the specific policy you want to change.

Navigate to the tab(s) where you wish to make changes. You will have a number of options:

1. Activate a policy that is currently not active: simply click the switch and turn on the policy. If there are values, checkmarks, sliders or radio buttons associated with that policy, select / enter as appropriate. You will notice that the SAVE button on the lower right turns green – click to save the policy activation. You may enable multiple policies prior to clicking SAVE.
2. If a policy is in the ORANGE state (turned ON, then turned OFF without performing an UNDO), then you may turn it on the same as described above.
3. Once the policy is on, you may wish to change values or settings within the policy. Make the changes you wish, then click the green SAVE button.
4. Once a policy is on, you may perform and UNDO, which reverts changes made by that policy and removes the monitor. To UNDO an active policy, click on the UNDO hyperlink to the right of the policy name. You will get a popup requesting confirmation.
    a. Some policies allow you to perform a suspension, or TEMPORARY UNDO on the policy. For those, the popup will ask you if you wish to perform a permanent or a temporary UNDO. Select the option you desire; if temporary, use the slider to select between 5 and 60 minutes. This feature is extremely useful for you to temporarily remove Third Wall restrictions should you need to take actions on those computers that are inhibited by Third Wall policies. IMPORTANT NOTE: performing a Temporary UNDO will NOT reset the "Enabled Since" date for that policy, and will preserve your audit trail validating uninterrupted protection over time.
    b. If you have temporarily suspended a policy, you can only take three actions for that policy:
        i. Perform an UNDO, and select the option to permanently UNDO the policy.
        ii. Perform an UNDO, and select the option to remove the suspension, which will re-enable the policy on that Location
        iii. Let the timer expire, which will then re-enable the policy on that Location.
5. You may also turn an active policy OFF by clicking the switch (rather than performing an UNDO). After you click the switch, click the green SAVE button.
    a. CAUTION: this option is NOT recommended. <u>It will turn off the monitor, but will NOT revert any values changed by the policy</u>. You should consider an UNDO instead.
    b. This will cause the policy to turn Orange on the Security Overview screen.
    c. You may turn a policy back on from the Orange state by clicking the slider switch for the policy.
    d. You may also UNDO a policy from an Orange state.

<u>Applying Profiles</u>

We have built into Third Wall a capability for you to easily apply policies across multiple Locations within your environment – Profiles. This is how they work.

First – an important note. Only users with Third Wall Admin privileges can actually apply Profiles – this is a very powerful tool, so we have protected it from casual use. To give a user Third Wall Admin privileges, have an Automate SuperAdmin take these steps:

1. Open the Users page in Automate, or expand your tree to see Users.
2. Expand the User category, and then double-click the user who will be receiving privileges.
3. Select the Permissions Tab, then right click in the User Classes box, and select Third Wall Admin. Click SAVE to save your changes, and then follow the prompts.

To begin, you create within a Location a set of active, enabled policies that you want to apply across multiple Locations. This will include values within each setting, such as the "name" field in Rename Local Administrator Account. Once you are satisfied with the settings, you will click on the "Save Current Config as Profile" button on the Security Overview tab, which will prompt you for a name. Type in a unique name, and save the profile. NOTE: the name must only contain letters and numbers, no symbols.

Then, on the Security Overview Tab on any Location screen, select any saved profile from the Select Profile dropdown list. [NOTE: you will have to have Third Wall Administrator privileges to do this.] After verifying that this matches what you wish to do – you will see Blue colors designating changes to the Location you are currently on – you will click on the "Save" button or the "Apply Profile" button. Alternatively, at this point, you may click on "Clear Profile," which will abort the process; or "Delete Profile," which will (after prompting) delete the selected profile from the database and abort the process.

If you click on Save, then you will apply that Profile to the current Location only. However, if you select "Apply Profile," you will be prompted as to whether you want to apply the selected profile to this single Location only, or to the entire Client of which this Location is a subset, or to **all** of the Windows computers you have under management (all Locations).

When you attempt to do this, Third Wall will look at the current policies enabled on each Location to which you want to apply this profile, including the currently displayed Location. If there are no enabled policies in any of those Locations, then Third Wall will apply the profile across all selected Locations. However, if there are any enabled policies in any of the selected Locations which would be changed by the selected Profile, then Third Wall will prompt you. You will have to choose whether you want to:

- Apply the profile entirely, including applying any values within the profile that differ from the values within the already-enabled policy in any given Location. For example, if you are applying a profile that Renames Local Administrator Account to the value "myMSP" while one of the Locations already has that policy active with the name "thirdwallsecurity," then the new value of "myMSP" will replace the old value of "thirdwallsecurity." CAUTION: this will reset the "Protected Since" date for any policies where the values are changed by the application of a profile.

- Apply the profile but retain all current Third Wall set values for any policies that are already active in a Location where you are applying the profile. For example, if you are applying a profile that Renames Local Administrator Account to the value "myMSP" while one of the Locations already has that policy active with the name "thirdwallsecurity," then the new value of "myMSP" will not replace the old value of "thirdwallsecurity." The "Protected Since" date will not change in this scenario.

If you attempt to apply a profile to a given Location or to multiple Locations, and that profile has fundamental conflicts with a target Location, then the profile application process will abort, and you will get an error

message. For instance, if you attempt to apply a profile that turns on the Minimum Password Length policy, but there is already a Set Local Admin Password policy active with a shorter password than the profile specifies, the profile application process will identify the error and abort.

IMPORTANT NOTE: Applying a Third Wall profile will never disable or UNDO any policy on any Location. If a policy is already enabled at a Location where you are applying a profile, it will stay active if the profile does not include that policy. Thus, profiles are additive only – they will preserve (or modify) policies that are already enabled, and will add more if there are additional policies in the profile that were not enabled for that Location, but will never turn off or UNDO a policy. If you wish to do that, you must go to the desired Location(s) and perform an UNDO at that Location. The single exception to this rule is within the Restrict Local Admin Tools policy – if your Profile does not include sub-policies already in effect, those sub-policies will be turned off upon save of a Profile.

Once you select a profile to apply, but prior to Saving or Applying the profile, then the Security Overview page will show all of the policies being changed by that profile in blue. For that Location, if the policy is already enabled, then the color will turn blue only if embedded values will be changing. However, if the profile will be applying a policy that is already active (green) on that Location, then the color will stay green unless a setting within that policy is changed by the profile. Then, after you click on Save, all applied policies will turn green to indicate they are active, and will display the appropriate date. Again, if a given policy was already enabled prior to applying the profile, and no values were changed on that policy, then the "Protected Since" date will not change.

If you choose to apply the profile to multiple Locations, then obviously those Locations will NOT be highlighted in blue colors for proposed changes. USE CAUTION when applying profiles across multiple Locations. Once applied, you will need to reload a Location page (close and reopen) to show the newly-applied Third Wall policies on Locations other than the one from where you applied the profile.

Third Wall comes pre-configured with several built-in Profiles, which are listed below:

TW – No-brainers: This Profile is loaded with Policies that end-users will not even know are there; thus, you can provide added protection without causing any end-user negative reaction or tickets, etc. We strongly recommend you deploy this Profile, or one you create with no-brainers specific to your judgment, to ALL of your managed computers asap, as a baseline for immediate enhanced security. You can then add more, either globally, by Client or by Location, to overlay on top of these anytime you wish.

- Rename Local Administrator Account
- Disable Local Guest Account
- Restrict Local Admin Tools (Registry Editor, Run as Admin, Powershell Prompt only)
- Disable Windows 10 Keylogger
- Enable Logon Message
- Disable Autorun (Autoplay)
- Uninstall Blacklisted Applications
- Disable Office Macros from Internet
- Disable OLE in Office Documents
- Log All Logon and Logoff Events
- Enable User Logon Reporting
- Enhance Security Event Logging
- Monitor Event Log Clearing

- Alert on Excessive Logon Failures (A/V and Ticket actions only)

TW - Enhanced Auditing
- Audit All NTLM Traffic
- Log All Logon and Logoff Events
- Enable User Logon Reporting
- Enhance Security Event Logging
- Monitor Event Log Clearing

TW - Data Security
- Disable Write to Optical Media
- Disable Write to USB Storage Devices
- Schedule Secure Free Space Delete (weekly, after 4:00 PM)
- Disable Office Macros from Internet
- Disable OLE in Office Documents

TW - User Restrictions
- Disallow Microsoft Accounts
- Restrict Local Admin Tools (all but Task Manager and Control Panel)
- Enforce User Account Control Settings (level 3)
- Disallow running 'setup.exe' & 'install.exe'
- Disable Windows Installer (unmanaged)
- Disable Windows Store

TW - Workstation protection
- Disable Local Guest Account
- Set Minimum Local Password Length (8 characters)
- Set Maximum Local Password Age (30 days)
- Enforce Password Protected Screensaver (30 minutes)
- Enforce User Account Control Settings (level 3)
- Disable Windows 10 Keylogger
- Enable Logon Message
- Disable UPnP
- Disable AutoRun (AutoPlay)

TW - Instant Reaction
- Log All Logon Events
- Alert on Excessive Failed Logon Events (3/hr; run AV Scan & Isolate)
- Monitor for Ransomware Attacks (Disable VSS, run AV Scan & Isolate)

APPLYING POLICY EXCEPTIONS TO INDIVIDUAL COMPUTERS

You may exclude any computer from any one or more policies, either preemptively (before the policy is enabled for the Location) or post-application of the policy. Once you activate an exception, that computer will execute an UNDO on that computer for that policy, reverting any changes made by the policy (if any), and will remove that computer from further monitoring. Removing the exception will place the computer back in the monitoring group, and which will quickly apply the policy, if active.

To apply an exception, navigate to the Third Wall tab on the target computer's Automate page. You will see a color-coded overview:

- Yellow = inactive policy at that Location, and no computer exception applied
- Green = active policy at that Location, and no computer exception applied
- Orange = computer exception applied, regardless of whether policy is active or not

On this page, choose the policy you wish to exclude on this computer, and simply click the switch to the ON position. You will get a popup box asking you to confirm the exception.

- If the policy is not currently active on that corresponding Location, simply confirm your action
- If the policy is currently active on that corresponding Location, you will be given a choice of applying the exception permanently (i.e., until you remove it) or temporarily. If you select the temporary exception option, you may select the time period for the exception, from 5 to 60 minutes. This feature is very useful for removing the policy restriction for a short period of time to accomplish key actions on that single computer that were inhibited by the policy.

To remove an exception, simply turn the switch OFF and confirm your action.

CREATING REPORTS & DATEVIEWS

Third Wall now gives you access to two very powerful reports and five Dataviews within Automate. We strongly recommend you set the reports up to automatically generate and save once per month, for each of your clients, giving you a full archive record of critical information.

To generate a Logon Dataview, right click the CLIENT, LOCATION, COMPUTER or GROUP within Automate. Then select DATAVIEWS, ThirdWallv2, and ThirdWall User Login Audit.

To generate a Third Wall Enabled Policy Dataview, right click the CLIENT, LOCATION, COMPUTER or GROUP within Automate. Then select DATAVIEWS, ThirdWallv2, and Third Wall Enabled Policy. This will show you which policies are active for that grouping, and when they were activated.

To generate a USB Wall File Transfer Audit Dataview, right click the CLIENT, LOCATION, COMPUTER or GROUP within Automate. Then select DATAVIEWS, ThirdWallv2, and USB Wall File Transfer Audit. This will show you a list of the past 60 days of all files transferred to a USB Wall-registered USB data stick.

There are also two Dataviews that give you log information about which tech has made changes to Third Wall policies, exceptions, etc. Again, right click the CLIENT, LOCATION, COMPUTER or GROUP within Automate. Then select DATAVIEWS, ThirdWallv2, and Third Wall Computer Audit Log or Third Wall Location Audit Log.

Reports can only be generated at the Client level, or for All Clients at once. To generate a report on demand

in **Automate 11**, right click on either CLIENT or a single Client , then select VIEW REPORTS, then Third Wall, then the desired report. You may also use the Report Manager to automatically generate these reports on a schedule – we strongly recommend you do that for each Client and have those reports emailed to you or directly to the Client monthly.

To generate a report in **Automate 12**, you must determine which version of Third Wall you are using. If v2.2.1.8 or earlier, you first have to set up access to legacy features. To do that, navigate to System / Configuration / Dashboard / Config / Control Center. Then, on the bottom right, check the box "Display Legacy Category." This will give you an icon called Legacy on your Automate main page. Click on that, then Report Manager, and select the Third Wall report you wish to run. Then select the Client (no other parameters will work) and Print or Print Preview the report. This screen will also allow you to set up these reports to automatically generate on a schedule – we strongly recommend you do that for each Client and have those reports emailed to you or directly to the Client monthly.

If you are running Third Wall v2.2.1.9 or later, then these reports are available in the new Automate Report Center. Simply right-click the desired Client, and navigate through the context menus to select the appropriate Third Wall report.

1. Audit Report

   The Audit report lists, by Location, the currently active Third Wall policies and when they were enabled, giving you a powerful audit trail showing continuous protection. It will also list, under the applicable policy, any computers currently excluded from the policy due to an exception set within the Third Wall computer screen.

2. Logon Report

   The Logon Report shows a full month (plus one day) history, from the date the report is generated, of all logons, logoffs, unlocks and locks (screen lock and password-protected screensaver locks) within the unit selected. It will be sorted by Domain, then by Username, then by ComputerID, then by time/date to give you an easy method of finding information. If you need dynamic or interactive data, please use the Third Wall Dataview. For viewing Logon Failures, please use the Dataview.

DESCRIPTION OF THIRD WALL™ POLICIES AND FUNCTIONS

***Implement policy changes in a business environment separately, one at a time*.** Local policy assignment changes should be done individually or in isolation to first assess impact on the business networking environment. Thus, it's advisable not to make multiple changes to devices simultaneously since, if an important service becomes unstable or stops working, it's harder to isolate and trouble shoot the reason. When changes are made, it's recommended they be done individually and then after waiting a sufficient amount of time, other changes can be made.

Remember that activating a Third Wall policy generally does two things: changes certain settings on every computer in the Location, and assigning a monitor to ensure the settings stay that way. The monitoring allows Third Wall to ensure long-term compliance with a policy, which is the foundation of our Audit compliance report.

Several policies will require a reboot of the computers prior to taking effect. Normally, we recommend you simply allow the user to perform their normal reboot cycle, unless the deployment of the policy is urgent.

IMPORTANT NOTE on GROUP POLICY: if you have Group Policy settings that are contrary to any given Third Wall policy setting, then you will have various failures and / or reversing policies. We strongly recommend **NOT** having both Group Policy and Third Wall managing the same parameters. If you do, and they have differing settings, then they will alternately change those settings; each time that Third Wall monitors change those settings, you will receive a ticket for each computer changed. Please contact Third Wall support for assistance in resolving these conflicts.

1. **Local Built-in Account Management**
    a. Rename Local Administrator Account
        i. Commandeering an Administrator account is a primary goal for hackers during an attack. To do this, a hacker needs a username and a password. By leaving the administrator account named to its default setting of 'Administrator,' half of the account security is effectively compromised as the username can be easily guessed. Use this option to rename the local Administrator account on all workstations within the Location. NOTE: this ONLY applies to the built-in Local Administrator Account. If you have created other Local Administrator Accounts, those will not be impacted by this policy.
        ii. Usage warning: If this setting is applied to a machine currently signed on with the local Administrator while locked, the user will not be able to unlock the desktop by entering their password in the provided field. In this condition, the user will likely and incorrectly assume the password is changed. To resolve, use the mouse to click 'Sign in as another user' and provide the new Administrator user name along with the existing password.
        iii. NOTE: if the Local Administrator Account is disabled via methods other than using Third Wall policy, then applying this policy will have no impact unless you select the checkbox to "Auto-enable Administrator Account if disabled." Otherwise, you will receive tickets from all computers in that Location where the Local Administrator Account is disabled.

iv. User accounts with a trailing '$' (dollar sign) are hidden from username listings. Use of this policy to increase internal security is recommended.
v. This policy will not run on Windows® servers.
vi. To change the Administrator account on the Domain, use the appropriate Domain tools.

b. Set Local Administrator Password
i. Proactively managing the Local Administrator Passwords adds another layer of protection, particularly for those computers with the default password. NOTE: this ONLY applies to the built-in Local Administrator Account. If you have created other Local Administrator Accounts, those will not be impacted by this policy.
ii. If the Enforce Password Complexity policy in Third Wall is active, then this password must meet the requirements for complexity.
iii. NOTE: if the Local Administrator Account is disabled via methods other than using Third Wall policy, then applying this policy will have no impact unless you select the checkbox to "Auto-enable Administrator Account if disabled." Otherwise you will receive tickets from all computers in that Location where the Local Administrator Account is disabled.
iv. This policy will not run on Windows® servers.

c. Disable Local Administrator Account
i. To fully remove the Local Administrator Account from the threat of attack or misuse, use this policy to disable the account. This policy is mutually exclusive of the Rename Local Administrator policy and the Set Local Administrator Password policy. NOTE: this ONLY applies to the built-in Local Administrator Account. If you have created other Local Administrator Accounts, those will not be impacted by this policy.
ii. This policy will not run on Windows® servers.

d. Disable Local Guest Account
i. While this default setting is normally disabled on all Windows® OS computers, Third Wall™ applies an ongoing monitor to assure that this does not get changed. This is particularly important should malware try to hijack a computer using this account.
ii. Third Wall™ UNDO will NOT enable the Guest Account.

e. Disallow Microsoft Accounts
i. Windows® 8 and above allow local logon using @Hotmail and other Microsoft accounts. Applying this policy means users will not be able to create new Microsoft accounts on a computer, switch a local account to a Microsoft account or connect a Domain account to a Microsoft account.
ii. NOTE: many Azure AD implementations will not work if you enable this policy; please test before you deploy.

2. Local User Account Management

a. Set Minimum Local Password Length
i. This policy is helpful to apply appropriate security policies to non-Domain users. Use it to enforce a minimum password length for all local user accounts, measured in characters, for all computers within the Location. Required by key compliance

statutes, including HIPAA, even if the computer is normally logged on as a Domain account.

ii. If you have enabled Set Local Administrator Password prior to enabling this policy, you will be required to modify the Local Administrator Password to meet password length requirements, if it does not already, before you can activate this policy.

iii. Use of this policy will not impact Domain members' Active Directory user accounts.

iv. This policy will not run on Windows® servers.

b. Set Maximum Local Password Age

i. This policy is helpful to Apply appropriate security policies to non-Domain users. Use it to enforce a maximum password age for all local user accounts, measured in days. Required by key compliance statutes, including HIPAA, even if the computer is normally logged on as a Domain account.

ii. Use of this policy will not impact Domain members' Active Directory user accounts.

iii. There is a potential Windows conflict if any computer has set the Minimum Local Password Age to greater than the new Maximum Local Password Age. To avoid this, Third Wall will automatically set Minimum Local Password Age to zero when this policy is activated.

iv. This policy will not run on Windows® servers.

c. Enforce Password Complexity

i. You should ensure that passwords meet minimum complexity standards. This policy requires passwords must contain characters from three of the following five categories:

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages. NOTE: Third Wall does not recognize this set of characters, so will not count these toward satisfying the complex password requirement.

ii. If you have enabled Set Local Administrator Password prior to enabling this policy, you will be required to modify the Local Administrator Password to meet password complexity requirements, if it does not already, before you can activate this policy.

iii. Use of this policy will not impact Domain members' Active Directory user accounts.

iv. This policy will not run on Windows® servers.

d. Enforce Password Protected Screensaver

i. This policy will perform several changes to the local policies of all the computers within a Location. It will enable the Windows® screen saver and the screen saver timeout; it will disable the user controls for the screensaver and it will enforce a password requirement on unlock. This is a critically important security tool, as you do not want unattended computers available to unauthorized users.

ii. Local Administrators will be unable to change this setting using the Control Panel.

iii. UNDO will only run on one user, whoever is signed on the computer at the time of UNDO. Other user(s) of this machine, as they sign on, will then receive the UNDO for a period of up to 3 weeks after issuance of the UNDO command.

e. Restrict Local Admin Tools
   i. Many end users and / or locally infected computers can use select local admin functions to potentially cause great damage, either on a single computer or as a conduit to entire environments. When selected, these policies cause the following applications to be inaccessible for users of Windows® desktops, regardless of their local security group membership. This means you can continue to allow users to run with local admin privileges while restricting their ability to run inappropriate system tools. Third Wall™ supports restricting the following applications:
      - Disable Registry Editor
      - Disable WinRun (Windows Key +R)
      - Disable Command Prompt
      - Disable Powershell (NOTE: for Rel 2.0, will NOT block Powershell v4.0)
      - Disable Microsoft Management Console (MMC)
      - Disable 'Run as Admin'
      - Disable Task Manager
      - Disable Control Panel Access
   ii. This policy will not run on Windows® servers.
   iii. UNDO will only run on one user, whoever is signed on the computer at the time of UNDO. Other user(s) of this machine, as they sign on, will then receive the UNDO for a period of up to 3 weeks after issuance of the UNDO command.
   iv. There is an optional checkbox allowing you to exclude anyone signed onto that computer as a Local or Domain Administrator from this policy. NOTE: this exclusion is ONLY for the built-in (native) Administrator Accounts, not any additional ones you may have created.
   v. For some Operating Systems and certain functions, you may need to reboot the end user computer(s) to cause changes to take effect.

f. Enforce User Account Control (UAC) Settings
   i. User Account Control (UAC) is a Windows® feature which notifies the user when a program or user attempts to make a change which could impact system stability. Many users consider this a needless intrusion and disable this important security feature. Use this Third Wall™ policy to ensure all computers within the Location have UAC enabled and set appropriately. If disabled again by the user, Third Wall™ will detect the change and revert the computer to its desired setting.
   ii. You will have the option to choose one of 4 levels of protection within UAC, corresponding to the 4 options normally available within the Windows interface.
   iii. This policy will not run on Windows® servers.

g. Disallow Running '*setup*.exe' and '*install*.exe'
   i. Many environments struggle with unauthorized applications being installed on internal computers. At best, these applications waste hardware resources and employee time. At worst, they compromise system security. This policy will prevent

any files with the word 'setup' or 'install' in them from running. This policy is now set up with **wildcards**, so it will restrict *setup*.exe and *install*.exe.

ii. If you need to run either of these programs legitimately for system administrator purposes, we recommend you use the Temporary Undo function for the period of time you will be running the program(s). You may also build in commands into scripts to bypass / restore this policy. Contact Third Wall for assistance with this option.

iii. ConnectWise Automate® pushed applications may not install when this policy is applied. We recommend you use the Temporary Undo function for the period of time you will be running the program(s). You may also build in commands into scripts to bypass / restore this policy. Contact Third Wall for assistance with this option.

iv. You may whitelist applications within the Client-level "Third Wall %AppData% Exceptions and Discovery" screen using the manual exception function.

v. This policy will not run on Windows® servers.

h. Disable Windows® Installer

i. The Windows® Installer is an installation and configuration service provided with Windows® which facilitates user installation of applications. Most application installations require this service. By disabling it, the user will be unable to install these applications.

ii. You may select to disable either all MSI files, or just Unmanaged MSI files.

1. Disable Unmanaged: The Windows Installer is disabled for unmanaged applications but is still enabled for managed applications. Non-elevated per-user installations are blocked. Per-user elevated and per-machine installs are allowed.
2. Disable All MSI: Windows Installer is always disabled for all applications. No installs are allowed including repairs, reinstalls, or on-demand installations.

iii. ConnectWise Automate® pushed applications may not install when this policy is applied. We recommend you use the Temporary Undo function for the period of time you will be running the program(s). You may also build in commands into scripts to bypass / restore this policy. Contact Third Wall for assistance with this option.

iv. This policy will not run on Windows® servers.

3. OS Security

a. Disable Windows 10 Keylogger

i. This policy will disable the built-in Keylogger on all Windows 10 computers, preventing the recording / transmittal of keystrokes to Microsoft.

ii. This policy will not run on Windows® servers.

b. Enable Logon Message

i. Secure environments need to be labeled accordingly. Use this policy to provide a 'no trespassing' sign to legally declare your network's boundaries. You may also use this policy to insert messages to enhance branding.

1. Further information including an example message: https://technet.microsoft.com/en-us/library/jj852199.aspx

c. Enable SmartScreen
   i. This policy only works to protect Internet Explorer or Internet Edge browsers. It will not impact other browsers.
   ii. This policy will restrict users from downloading software from external websites, and will also block access to known bad websites, either by warning them or requiring Admin privileges.
   iii. This policy will not run on Windows® servers.

d. Disable UPnP
   i. Disabling Universal Plug and Play (UPnP) will impact users attempting to install new hardware devices. This prevents undesired hardware from self-installing; malware often piggybacks on this process.

e. Disable Auto-Run (Autoplay)
   i. Auto-Run has long been a well-known security vulnerability in Windows. Although Microsoft has addressed this weakness by constraining the default objects that automatically run code on insertion, Third Wall™ recommends completely disabling all Auto-Run activities by Applying this policy. The end user will NOT get the popup box, upon insertion of a disk or USB drive, asking what the user would like to do.

f. Disable .exe Running from AppData

   Malware, particularly ransomware, often hides an .exe file in the AppData folder.

   i. This policy will prevent any .exe within that folder, up to 8 layers deep, from running.

   ii. You may select to Include %LocalAppData%, Alert on File Block and/or to Block All Executable types
      1. Include %LocalAppData%: Selection this option will apply the same constraint to the %LocalAppData% folder as is provided the %AppData% folder. If 'Block All Executable Types' is selected then the %LocalAppData% folder will also be identically constrained.
      2. Alert on File Block: Enable this option to receive a ticket anytime a remote computer is blocked from running an executable file. The ticket will include the full path to the blocked file which may be directly assigned to the whitelist.
      3. Block All Executable Types: expands the policy to block any executable file. Blocked filename extensions are:
         .ADE, .ADP, .BAS, .BAT, .CHM, .CMD, .COM, .CPL, .CRT, .HLP, .HTA, .INF, .INS, .ISP, .LNK, .MDB, .MDE, .MSC, .MSI, .MSP, .MST, .OCX, .PCD, .PIF, .REG, .SCR, .SHS, .URL, .VB, .WSC
         a. Blocking All Executable Types will also extend protection to all folders, no matter how many sub-folders deep.

   iii. **NOTE**: some legitimate programs launch .exe files from %AppData% and %LocalAppData% folders. This policy will prevent them from running. However, you can globally whitelist all of those legitimate programs in the Third Wall Integration page, or per-client on the Third Wall Client Screen.

1. Global Whitelist can be found on the Integrations page. All entries *must* begin with either '%AppData%' (e.g. '%AppData%\Zoom\Zoom.exe') or with '%LocalAppData%', otherwise the addition will be rejected.
2. Client Whitelist can be found on the Client Screen. From the Client Screen, open the 'Third Wall' tab. From there, click the 'AppData EXE Exceptions & Discovery' link.
    a. On first use, this screen will show no Current Exceptions or Scan Results. Use the 'Add Manual Exception' button to assign individual files to the Current Exceptions screen. Unlike the Global Exception List, any file path may be entered (e.g. 'C:\Program Files\Product\File.exe').
    b. Conversely, the 'Scan All' button will launch an interrogation of all .exe files found in %AppData% and %LocalAppData% folders. This scan will be run on all remote workstation within the Client. A de-duplicated list of all found files will be shown on the Scan Results screen.
        i. The environment variables %AppData% and %LocalAppData% only exist when a user is signed onto the remote computer. You will want to run this scan at a time that maximizes the chance all remotes have active users. Computers without current users will find no files.
        ii. The Scan Targets supplements the 'Scan All' button and should be used when the environment is or will be using the 'Block All Executable Types' policy. When clicked, a list showing all executable types will be shown. Any file type that is checked on this screen will also be searched for when scanning the Client.
        iii. Once the 'Scan All' button has been used on a Client, this screen will display a 'Scan Results' button. Press this button to switch the display from the list of Current Exceptions to showing your Scan Results. Press the 'Current Exceptions' button to return.
    c. Files can be moved from the Scan Results screen to the Current Exceptions screen by use of the 'Save' button. Use the checks on the Scan Results screen to choose which discovered file or files to be excepted. Any checked file, on Save will be moved to the Current Exceptions screen. Duplicate entries are discarded.
        i. Files can be individually checked. For convenience, a 'check/uncheck all' option is provided. Another method of moving Scan Results to the Current Exceptions is by text search. Use the field on the bottom of the screen to enter search criteria and press the 'Search' button. When used, any file in Scan Results which matches the search will be automatically checked. The search button will not uncheck

files that don't match. This allows multiple search conditions to be stacked and selected.

ii. If your policy assignment doesn't include the LocalAppData folder, there is no need to whitelist %LocalAppData% files. For these environments, you can select only the %AppData% files by entering '%AppData%' and pressing 'Search'.

d. Exceptions will be realized on the remote only after this sequence of events occurs.

i. Update Config' is run. This Automate command will also relay the whitelist to the remote.

ii. The monitor runs with the user signed onto the computer. Each monitor run makes sure the whitelist communicated in the 'Update Config' is applied and makes appropriate changes when not.

iii. The remote computer is rebooted.

1. The above requirement is per Microsoft. However, we've seen consistent results when the user signs out and back in.
2. Likewise, we've found restarting the 'Windows Explorer' process consistently applies the whitelist as well.

g. Disable Terminal Server Services

i. Malware can use RDP / Terminal services as an entryway. This policy will shut down the Terminal Server services on computers in the Location. It does not impact the Terminal Client services.

ii. You may select either Workstations or Servers or both with the checkboxes.

4. **Data I/O Security**

a. Disable Write to Optical Media

i. This setting will prevent users from writing data to any optical storage device. This setting requires a reboot to take effect, which Third Wall™ will not initiate.

ii. This policy will not run on Windows® servers.

b. Disable Read / Write to Optical Media

i. This setting will prevent users from reading data from and writing data to any optical storage device. This setting requires a reboot to take effect, which Third Wall™ will not initiate.

ii. This policy will not run on Windows® servers.

c. Enable USB Wall

i. Enabling this policy will cause all computers within a Location to be unable to see any USB data storage device except for those that you have registered using the Third Wall Client page. This will also completely restrict mobile phones and similar mobile devices from acting as USB data storage. Currently, registration is limited to USB

data sticks only; additional storage devices (external hard drives, etc.) may be added at a later time.

ii. For any computer in a Location with USB Wall enabled, USB wall will record the filename of all files written to a registered USB stick. This information will be available in a Dataview, listing Username, Computer ID, USB Stick ID, date/time of event and Filename of written file. NOTE: Username can only be captured on USB sticks formatted NTFS. Other formats will not capture the Username.

iii. Pens protected by BitLocker are supported. The remote must have the credentials locally cached for the pen to be accepted.

d. Disable Write to USB Storage Devices
   i. This setting will prevent users from writing data to any USB storage device. This will impact any storage device on the local computer's USB chain. This setting requires a reboot to take effect, which Third Wall™ will not initiate.
   ii. This policy will not run on Windows® servers.

e. Disable Read / Write to USB Storage Devices
   i. This setting will prevent users from reading data from and writing data to any USB storage device. This will impact any storage device on the local computer's USB chain. This setting requires a reboot to take effect, which Third Wall™ will not initiate.
   ii. This policy will not run on Windows® servers.

f. Disable Common Cloud Storage
   i. This policy will block access to any and all selected Common Cloud Storage sites, using Host File methods. While you should expect a high rate of success, there may be situations where the policy fails to block access.
   ii. This policy will not run on Windows® servers.

g. Schedule Secure Free-Space Delete
   i. You may set up a schedule to automatically run a full 3-pass Secure Free Space Delete (i.e., overwrite) of all "'deleted" files, preventing those from being retrievable by unwanted persons at a later date. This is critical to data security. CAUTION: this will also make those files unrecoverable by you or other friendly entities.
   ii. Servers will always run at the desired time, as we assume they are always running. Workstations, however, have varied work schedules, and will run either at the desired time or later in the day. The day you activate the policy will become the baseline for which day of the week (for Weekly) or which day of the month (for Monthly) that the action will run.

5. Application Security

a. Uninstall Blacklisted Applications
   i. This policy will automatically initiate an Uninstall of any MSI-based application that has been added to the ConnectWise Automate Blacklist, as soon as the application is detected. (NOTE: future releases of Third Wall will expand to other applications as well)
   ii. In most cases, a successful Uninstall will be accomplished. However, for those applications that are not able to be uninstalled, you will receive a Ticket on your

ConnectWise Automate Control Center. You should then proceed to assess the Uninstall status and attempt other methods to complete the Uninstall.

iii. This policy will not run on Windows® servers.

b. Prevent Public Webmail Access
   i. This policy will block access to any and all selected Public Webmail sites, using Host File methods. While you may expect a high rate of success, there may be situations where the policy fails to block access.
   ii. This policy will not run on Windows® servers.

c. Prevent Social Media Access
   i. This policy will block access to any and all selected Social Media sites, using Host File methods. While you may expect a high rate of success, there may be situations where the policy fails to block access.
   ii. This policy will not run on Windows® servers.

d. Disable Windows® Store
   i. Windows® 8 and above include a feature which allows users to install applications from a centralized repository, known as the Windows® Store. As a potential conduit for unauthorized change, it should be disabled.
   ii. Due to Microsoft changes, within the Windows 10 family of operating systems, this policy will only be effective on Windows 10 Enterprise and Windows 10 Academic.
   iii. This policy will not run on Windows® servers.

e. Disable Google® Play
   i. This policy will block access to Google Play, using Host File methods. While you may expect a high rate of success, there may be situations where the policy fails to block access.
   ii. This policy will not run on Windows® servers.

f. Disable Apple® App Store
   i. This policy will block access to the Apple App Store, using Host File methods. While you may expect a high rate of success, there may be situations where the policy fails to block access.
   ii. This policy will not run on Windows® servers.

g. Disable Office Macros from Internet
   i. This policy will prevent macros embedded in Microsoft Office documents retrieved from internet sources (including email) from running on impacted computers.
   ii. This policy will not run on Windows® servers.

h. Disable OLE in Office Documents
   i. This policy changes the setting for OLE packages (Packager objects are small executable program codes that can run within other programs) so that they will not run. Default Windows setting is to ask user if they wish to continue, with a yes/no response required. This policy will simply not allow OLE packages from non-trusted sources to run. USE CAUTION when applying this policy. Although this is a common vector now for malware, it may also inhibit critical functions for some of your users.
   ii. Reading for further information: https://blogs.technet.microsoft.com/mmpc/2016/06/14/wheres-the-macro-malware-author-are-now-using-ole-embedding-to-deliver-malicious-files/

iii. This policy will not run on Windows® servers.

6. **Protocol Security** – CAUTION: disabling of protocols may cause unwanted / unanticipated side effects. Prior to enabling broadly, please test on a small Location of computers in a Client environment to determine if these occur within that Client's environment.
    a. Enable Windows Firewall – Workstations
        i. This policy turns on the local Windows Firewall on workstations. You may select a configuration file to apply if desired, and will be prompted with a popup to select the correct file if you check the Assign Config File checkbox.
        ii. If you apply a 64-bit configuration file to an environment which has any 32-bit computers in it, then those computers will ignore the configuration file and an open ticket will be generated.
        iii. If you have an antivirus managing the firewall, this policy will not apply.
        iv. By assigning a custom config file titled *nofirewall.wfw* , you will cause the policy to turn off the firewall and enable a Third Wall monitor to ensure it remains off.
        v. This policy will not run on Windows® servers.
    b. Enable Windows Firewall – Servers
        i. This policy turns on the local Windows Firewall on servers. You may select a configuration file to apply if desired, and will be prompted with a popup to select the correct file if you check the Assign Config File checkbox.
        ii. If you apply a 64-bit configuration file to an environment which has any 32-bit computers in it, then those computers will ignore the configuration file and an open ticket will be generated.
        iii. If you have an antivirus managing the firewall, this policy will not apply.
        iv. By assigning a custom config file titled *nofirewall.wfw* , you will cause the policy to turn off the firewall and enable a Third Wall monitor to ensure it remains off.
        v. This policy will not run on workstations.
    c. Disable Local LM Hash Storage
        i. Windows® computers up to 2008 use an insecure method to store credentials. Newer Windows® computers still have this service, disabled by default. Apply this policy to ensure credentials are not stored locally using the LM hash.
        ii. Use of this policy does not clear existing credentials. Forcing a password change after applying this policy is recommended.
    d. Audit All NTLM Traffic
        i. A flaw within Active Directory makes possible the theft and unauthorized use of your Domain's credentials by attacking a flaw in the NTLM protocol. Applying this policy will enable event logging of all NTLM traffic generated and received by all computers within the Location, providing you with a data to inform actions to restrict NTLM manually as desired. Logs will be kept locally on each computer.
            1. This policy is a partial step to disabling NTLM authentication within an environment and should be employed before disabling NTLM outright.
            2. You may wish to learn more here: https://richardkok.wordpress.com/2011/02/03/wireshark-determining-a-smb-and-ntlm-version-in-a-windows-environment/

e. Disable LM NTLM v1
    i. This policy will disable NTLM v1 outright within a Location and force all Windows® authentication communication over to Kerberos.
        1. It is critical that appropriate testing is done before applying this policy. IIS and SQL, for example use NTLM authentication by default and authentication to these resources will fail without prior configuration modifications.
        2. The Third Wall™ policy, 'Audit All NTLM Traffic' enables NTLM security auditing.
f. Disable NetBios
    i. This policy will disable NetBios outright within a Location.
        1. It is critical that appropriate testing is done, and preparation made, prior to enabling this policy, as it likely will break certain items.
g. Disable IPv6
    i. A fundamental component of cyber-security is to run only those services and protocols you are using. All Windows® systems Vista and above come with the IPv6 protocol enabled by default. This policy disables the IPv6 protocol on all current and new NIC bindings for all computers within the Location.
        1. Microsoft does not recommend disabling this protocol, but it may be appropriate for your environment.
        2. The disable method employed by Third Wall™ does not result in a 5 second boot time increase.
        3. This may impact Exchange servers.
h. Disable IGMP
    i. Excepting very large environments which are subject to multicast traffic, IGMP provides very little value and is potentially exploitable. Use this policy to disable all IGMP multicast support within the Location.
    ii. We strongly recommend you verify that IGMP is not being used within your environment prior to Applying this policy. This can be accomplished by sample testing or by using appropriate network analysis tools.
        1. If you are running Third Wall v2.2.1.7 or older, DHCP server services will likely be disabled by this policy.
i. Disable SMB v1
    i. SMB v1 is another potentially insecure legacy protocol which is used and enabled by default in Windows. This policy will disable this file protocol on all Windows® computers within a Location.
        1. SMB Versions in current Windows® releases
            a. Windows® Server 2003 – SMB v1 Only
            b. Windows® Server 2008 or Windows® Vista – SMB 1 or SMB 2
            c. Windows® Server 2008 R2 or Windows® 7 – SMB 1 or SMB 2
            d. Windows® Server 2012 and Windows® 8 – SMB 1, SMB 2 or SMB 3
            e. Windows® Server 2012 R2 and Windows® 8.1 – SMB 1, SMB 2 or SMB 3
        2. The importance of proper testing of this policy prior to releasing in a production environment cannot be overstated. You may want to learn more

at https://richardkok.wordpress.com/2011/02/03/wireshark-determining-a-smb-and-ntlm-version-in-a-windows-environment/

7. **Security Monitoring & Logging**
    a. Log All Logon and Logoff Events
        i. You often will need to record, for audit purposes and for forensic purposes, what user has been logged on to any computers over what time. This policy captures User Logon and Logoff data, including instances of Unlock and Lock, and stores it on each computer locally.
        ii. This policy is a prerequisite for Enable User Logon Reporting and Alert on Excessive Logon Failures. If you turn this policy off or UNDO it, you will UNDO any dependent policies that are currently active.
    b. Enable User Logon Reporting
        i. This policy simply directs Third Wall to store appropriate user-only Logon and Logoff events on the ConnectWise Automate database, where it will be available for the Third Wall Logon Report and Dataviews. Data will be stored for 60 days only. To save it longer, follow these procedures:
            Open the Dashboard
            Click Config -> Configuration -> Properties
            Add a new property:
                Name = ThirdWallNoLogonPurge
                Value = True
        ii. This policy requires that the policy Log All Logon and Logoff Events be enabled.
        iii. There is an option to include Type 3 (Network) Logon Failures. If you suspect that you have excessive Network Logon Failures in your environment, select this option to track them down. All logon failures, including these, are visible only in the Third Wall User Logon Dataview.
        iv. Target machines must be rebooted after enabling this policy for data to be captured for this policy and the associated reports / dataviews.
        v. The 'Enable User Logon Reporting' has a safety feature to prevent overloading your LabTech server with excessive entries. These entries may be caused by a multitude of factors including domain misconfiguration, virus infection or a verbose, non-standard service. Should this monitor detect 15 entries within a 300 second period, two things will occur: The computer will be immediately excepted from policy and you will receive a ticket, alerting you of the automatic exception. To resolve this condition, you simply open the computer screen and remove the exception.
            1. This behavior has an override. If you anticipate more than 25 entries within a 300 second period on a given computer, use the registry editor and make the following modification. Add *'HKEY_LOCAL_MACHINE\SOFTWARE\LabTech\Plugins\ThirdWall\store\LogonWatchSafetyOverride*' as a REG_SZ with a value equal to the newly desired threshold. The Third Wall Logon Reporting Policy will now alert only if the number value assigned to that key is exceeded.
    c. Enhance Security Event Logging

i. By default, Windows® enables a limited set of security event logging. Use this policy to enable the following extra logging events:
    - Security System Extension, success:enable, failure:enable
    - System Integrity, success:enable, failure:enable
    - IPSec Driver, success:enable, failure:enable
    - Security State Change, success:enable, failure:enable
    - File System, failure:enable
    - Registry, failure:enable
    - Sensitive Privilege Use, success:enable, failure:enable
    - Process Creation, success:enable
    - Audit Policy Change, success:enable, failure:enable
    - Authentication Policy Change, success:enable
    - User Account Management, success:enable, failure:enable
    - Computer Account Management, success:enable, failure:enable
    - Security Group Management, success:enable, failure:enable
    - Other Account Management Events, success:enable, failure:enable
    - Credential Validation, success:enable, failure:enable

d. Monitor Event Log Clearing
    i. Windows® reports to the Event Log when the Event Log is cleared. Use this policy to generate a ConnectWise Automate® Ticket anytime a Windows® computer within the Location has its Event Log cleared. This may be particularly useful for identifying malware / ransomware that has buried itself for later activation, as this is a known common behavior in these circumstances
        1. This policy makes no changes to the remote computer. Only monitors are employed, and the only action they take is to generate a ticket, if appropriate.
        2. UNDO will simply turn off the monitor for this policy.
        3. There is an option to 'Only Monitor Application, System & Security Logs'. Enabling this option will suppress alerts if any other log is cleared.

e. Alert on Excessive Logon Failures
    i. Logon failures may indicate attempted access by an unauthorized user and / or malware. For this policy, you define what constitutes suspicious (excessive failures) for logon attempts by defining the number of failures over a period of time.
    ii. This policy requires that you have the policy Log All Logon and Logoff Events enabled.
    iii. If / when excessive failures are detected, you have the following options you may select. ALL options will also send you a ticket in Automate.:
        1. Isolate and then power off the computer. This option is mutually exclusive of the other options. This option will Isolate but WILL NOT execute power down on a server. This is reversible for the isolated computer on that computer's Third Wall screen in Automate.
        2. Generate a ticket, and take no other action.
        3. Run an antivirus scan. REQUIRES that user has A/V set up properly in Automate. If there is no A/V set up on a given computer, then this will do nothing on that computer.

4. Isolate the infected computer using the Third Wall Emergency Isolate function, leaving the computer connected only to the Automate server and the ConnectWise Control server. This is reversible for the isolated computer on that computer's Third Wall screen in Automate.
5. Initiate a Third Wall Lockout, logging everyone off the computer and disabling all Local accounts. This is reversible for the locked-out computer on that computer's Third Wall screen in Automate.

iv. Regardless of which option is selected, upon detection a ticket containing the names of all failed users will be issued.
v. If an ISOLATE command is issued, the end user will be notified via a popup, with directions to contact the Help Desk. You may reverse an automatically generated Isolate event by going to that end user's Third Wall Computer screen and click the "Restore Networks" button.
vi. There is an option to include Type 3 (Network) Logon Failures. Please evaluate your environment prior to activating this option (see above in "Enable User Logon Reporting" policy discussion), as many environments have thousands of benign Network Logon Failures generated by network printers, etc.

f. Monitor for Ransomware Attacks
   i. This policy will enable a monitor that ensures 'bait' files are written to all users' *Documents* path, including redirected folders. When the files do not exist, they are created. These files have an additional monitor applied to them (not visible in Automate) which causes an alert action to run and a ticket to be generated when any one of those files are changed. Both the filename and the destination (within *Documents*) may be customized from the Ransomware Monitor Settings section on the Integrations Screen. Customization has no impact on the operation of the monitor, excepting the path and name of the 'bait' files.
   ii. Paths to *Documents* only exist when a user is signed onto the computer. To prevent a lapse in coverage and/or to provide security for computers rarely used directly by users (e.g. Servers) use the Static Path field on the Ransomware Monitor Settings section. When this field is populated with a valid path, four additional 'bait' files will be assigned to that path. Where the path doesn't exist, it will be automatically created, as will the 'bait' files.
   iii. This monitor is wholly reliant on the Automate Tray to create bait files within the *Documents* folder. If the tray is not running for a user, the 'bait' files will not be monitored. This reliance does not impact files assigned to a Static Path.
   iv. When manipulation of any of the 'bait' files is detected, Third Wall interprets that as a ransomware attack, and then will take immediate action based on what you have selected. You may select from any of the following options. Regardless of selection, a ticket will always be issued.
      1. Isolate & Shutdown. This option is mutually exclusive of the other options. First, the remote will invoke the Third Wall Emergency Isolate function, leaving the computer connected only to the Automate server and the ConnectWise Control server. To reverse the Isolation, you will need to go to

the Third Wall computer screen and click on the “Restore Network” button (which will then return to an Isolate button).. Once done, shutdown. Shutdown WILL NOT be run on a server.

2. Ticket Only does just that, and will take no other action.
3. Run an antivirus scan. REQUIRES that user has A/V set up properly in Automate. If there is no A/V set up on a given computer, then this will do nothing on that computer.
4. Turn off VSS (Volume Shadow Service) on this one computer, to prevent spread to backup files. To re-enable the VSS, use the standard procedure for starting a service.
5. Isolate invokes the Third Wall Emergency Isolate function, leaving the computer connected only to the Automate server and the ConnectWise Control server. To reverse the Isolation, you will need to go to the Third Wall computer screen and click on the “Restore Network” button (which will then return to an Isolate button).

v. Alert Action assignment – you must assign an alert action template for this policy. Choose one that takes the alert actions you desire should the policy monitor detect a suspected ransomware attack.

vi. The “bait files” will be visible to end users, and we strongly recommend you inform them before you deploy this policy that they will be there. By default, each file contains the phrase “thirdwall” in the filename, but you can globally change this in the Third Wall Integration screen. Should an end user delete one of these files, it will be immediately recreated. However, should an end user try a multiple rapid delete of any one of these files, it is possible that will trigger the response(s) you have selected in this policy as if it detected a ransomware attack.

vii. IMPORTANT NOTE: while this feature is designed to assist in protecting from Ransomware, Third Wall does NOT guarantee it will detect or mitigate all ransomware. Ransomware is constantly changing to get by any type of detection and mitigation, and some may not be detected by Third Wall. We will endeavor to update this function as we find new ways to do so.

viii. Two options may be assigned to this policy, “Alert on Delete” and “Hide ‘Bait’ Files”.:

1. Alert on Delete will cause an alert if any of the bait files are deleted. This will improve security, but you may get false alarms from user manipulation.
2. Hide ‘Bait’ Files applies the hidden attribute to all bait files, reducing the likelihood of false alarms caused by end user actions. This may or may not make the files somewhat less attractive to some ransomware packages.

g. Alert on Unencrypted Disk

i. This policy is intended to be used within environments with a disk encryption policy. If any %homedrive% (e.g. ‘C:\’) within the Location is detected to be running without BitLocker® encryption on the entire disk, a ConnectWise Automate® Ticket will be generated.

1. This policy only is applicable for full-disk encryption environments using BitLocker. If you are using the "Used Drive Space" option in Bitlocker, Third Wall will treat that disk as unencrypted.
2. The policy makes no changes to the remote computer. A combination of Third Wall™ programming and ConnectWise Automate® Monitors are employed, and the only action they take is to generate a Ticket, if appropriate.
3. UNDO will simply turn off the monitor for this policy.
4. You may select to apply this policy to Laptops only by checking the box.
5. Do NOT use this policy if the computers are not encrypted or if you are using an encryption method other than BitLocker.

8. **Emergency Action / Rapid Response Buttons**

While the policies described above have a dramatic impact on improving cybersecurity across entire Locations, there are times when you need to take rapid action on a single computer to ensure higher security. Thus, on the Third Wall™ Computer Screen, there are several rapid response buttons provided to do just that. These buttons are NOT policies. When clicked, they will execute on the target machine one time, and no Third Wall monitors will be initiated.

Be aware that, with Automate defaults, Automate normally will purge any commands issued within 48 hours if that command is not delivered (for instance, should the computer be turned off when the command is issued). However, with the Annihilate button, the Automate command is sustained until that computer receives it; thus, if it is offline for some period of days or longer, it will still get the command once it connects to the internet.

When you click on any these buttons, and confirm your selection, you will see the button have a progress bar, so you can see when the command is fully executed.

a. Emergency Lockout
    i. Use this button to prevent unauthorized users (e.g., on a stolen or lost laptop, or by a terminated employee or contractor) from continued access to a computer.
    ii. This will log out ALL users logged onto that computer. Any unsaved work will be lost, so use this option with some caution.
    iii. All local accounts, excluding system accounts, will be disabled.
    iv. Should you need to lock out Domain accounts, use proper Domain tools to disable those user accounts.
    v. Once applied, the button will change to "Restore Local User Accounts." When clicked, this will re-enable the accounts disabled by the Emergency Lockout button.
b. Screen Lock
    i. Use this button to prevent unauthorized users (e.g., on a stolen or lost laptop, or by a terminated employee or contractor) from continued access to a computer.

ii. This will NOT log out any users logged onto that computer. It will simply activate the Screen Lock state, requiring knowledge of the appropriate password to regain access to the computer.
iii. NO local or domain accounts will be disabled.

c. Emergency Isolate
   i. Use this button should you have need to rapidly disconnect a computer from the network (i.e., a computer has a suspected virus or other malware), preventing spread throughout your network.
   ii. This button will disable all network communications except for Ports 70, 80, 443, 8040 and 8041 for communication to your ConnectWise Automate® server only. This facilitates all ConnectWise Automate® operations from the ConnectWise Automate® Control Center, the ConnectWise Automate® Redirector, and ConnectWise Control. Third Wall will also automatically detect the internal settings used by ConnectWise Control.
      1. If you need to manually make a modification, add two fields using Automate properties (Dashboard -> Config -> Configurations -> Properties). Add these names / values:

         Name: ThirdWallSCServerOverride (value: ConnectWise Control server address)
         Name: ThirdWallSCPortOverride (value: ConnectWise Control server port)

   iii. Once applied, the button will change to “Restore Network.” When clicked, this will restore normal network communication to/from this computer.
   iv. The end user will be notified via a popup whenever their computer is isolated or restored from isolation, with instructions to contact the Help Desk.
   v. In the event a manual removal of Isolate is required, use the following Shell commands with Administrator authority. Running through the Automate CMD prompt is an effective method:

      netsh ipsec static set policy name="Third Wall Isolation" assign=NO
      netsh ipsec static delete policy name="Third Wall Isolation"

   vi. On the Integration screen for Third Wall, you may enter an Auto Restore setting. Enter the number of minutes after an Isolation occurs where you would like for Third Wall to automatically reconnect that computer. This will happen ONLY if Third Wall detects that it cannot communicate to your Automate server. This provides a failsafe should the computer be Isolated AND disconnected from the Automate server.

d. Annihilate
   i. This is a last-resort button only, as it will render the target operating system completely unusable. The computer will be unrecoverable. Use this for known compromised computers to prevent data / program theft. This button has special User Access restriction, to ensure only authorized users may activate this button –

only Third Wall Administrators will have access. To enable a user to be a Third Wall Admin, take these steps:

- As a SuperAdmin, open up the Users section in Automate
- Expand the User category, and then double-click the user who will be receiving privileges
- Select the Permissions Tab, then right click in the User Classes box, and select Third Wall Admin. Click SAVE to save your changes, and then follow the prompts

ii. When selected, you will be prompted to choose one of two options:
    1. Quick Annihilate: Delete Documents folder and proceed with annihilation. This is the fastest option to execute, but does not protect data on the hard drive from forensic recovery.
    2. Secure Annihilate: Delete Documents folder, then execute a Secure Free Space Delete and then proceed with annihilation. This fully deletes sensitive data on the hard drive, but may take up to several hours to complete.
    3. key.

9. **Utility Buttons**

There are two Utility buttons on the Third Wall Computer screen: Except All and Reset. The Except All button will, when selected, issue an UNDO command for that computer for all **enabled** Location policies. This will make the computer "clean," with no Third Wall restrictions or policies active on that computer. For some policies, the computer may need to be rebooted to complete the UNDO

The Reset button removes all Exceptions on that computer, so that ALL Third Wall policies enabled for that Location will impact that computer.

These buttons are particularly useful for moving a computer from one Location to another. First, your remove all Third Wall policies from the computer to be moved by clicking Except All. After a couple of minutes to ensure the commands reach this computer, then move the computer to its new Location. Once there, click the Reset button to enable the Third Wall monitors in the new Location to apply all active policies to that computer.

Should you forget to do this procedure prior to moving a computer, we recommend you move that computer back to its previous Location, then execute this steps in this procedure.

10. UNINSTALL / REMOVAL Procedures

a. Complete Uninstall
   If you desire to completely uninstall Third Wall from your system, here are the steps you should take. NOTE: you must be a Third Wall Admin to execute these steps.

   i. On the System Dashboard, select Config / Integration / Third Wall tab. Click the UNDO ALL from ALL AGENTS button and answer the prompts. This will remove Third

Wall policies from all managed computers. If you have computers not reporting in for several days, these may not receive the UNINSTALL command, and you may need to manually remove Third Wall settings from those.

ii. Then click the UNINSTALL button on the Integrations page, and follow the prompts. This will remove all Third Wall settings and data on your Automate server.

iii. Then, in the Plugin Manager, right click on the Third Wall line and Disable the plugin. Finally, with the Third Wall plugin still selected, click Advanced / Manage Plugins / Remove Plugin.

b. Uninstall a Single Client
If you wish to uninstall Third Wall settings from a single client, follow these steps. NOTE: you must be a Third Wall Admin to execute these steps.

i. On **each** Automate Location for that Client, go to the Third Wall page. Click on the "UNDO ALL" icon on the bottom left:  . This will perform a full UNDO on all **enabled** policies active in that Location.

ii. Notify us via email that you wish to have that Client / Locations removed from billing. NOTE: Simply performing an UNDO for an entire Location does not remove that Location from billing. You must notify us in writing of your desire to have that Location removed from Third Wall billing.

11. **Third Wall Integration Page**

On the Third Wall Integration page, you will find a series of Global settings, which impact all computers at all Locations. Access to these settings are restricted to Third Wall Admin Users only. There are seven sections:

a. Monitor Frequency: this allows you to change the frequency that all Third Wall policy monitors will activate. The default is every 5 minutes; by increasing the number, the monitors will fire less frequently. This is designed to reduce the operational impact of Third Wall on your Automate server; at this time, we do not see any degradation of Automate performance by Third Wall and do not recommend changing monitor frequency.

b. Assign Alert Template: this allows you to change which Automate Alert Template will be used when a monitor violation is detected. This will impact ALL policies except for Monitor for Ransomware Attacks, which has its own template selection option.

c. Assign Alert Category: this allows you to select a different Alert Category for all alerts generated by Third Wall, helping you to better manage how those alerts show to your technicians.

d. Install / Uninstall / UNDO ALL tools: generally, do not use these tools without consulting Third Wall support. However, you should use the UNDO ALL tool if you are removing Third

Wall completely from your environment. See the section for UNINSTALL / REMOVAL.

e. AppData EXE Block Exceptions: this is where you enter any EXE files you wish to not be blocked by the "Disable EXE Running from AppData" policy.

f. Ransomware Monitor settings: you can enter a subfolder destination for the bait files (with \Documents), specify a root for the filename for the bait files, and specify a Static Path for placement of additional bait files.

g. Isolate Auto-Restore: this is a failsafe in case a computer is both Isolated and not communicating with the Automate server. Enter a time in minutes; should the conditions occur, then the Isolate will be automatically removed after that time period.

12. Changing specific ticket parameters for individual policies (excluding Monitor for Ransomware Attacks)

    You may customize parameters for Third Wall tickets by going to the Group section of the Automate Control Center. Find the Third Wall group, expand to see the sub-groups, and then expand the sub-groups as needed to see the appropriate Third Wall policies. Double-click the policy you wish to change. Then select Computers / Remote Monitors. Highlight the Third Wall policy, and make changes to the Category or Alert Template only. Please do not change other parameters, inconsistent events may occur.

13. **Licensing & Other Notes**
    a. What is Third Wall?
        i. Third Wall™ is a plug-in for ConnectWise Automate® which gives you the ability to easily select and deploy security-focused changes to an environment.
    b. What constitutes use of a Third Wall™ License?
        i. A Third Wall™ License is consumed anytime a Third Wall™ Policy is assigned to a ConnectWise Automate® Remote Agent computer, or a Rapid Response button is clicked. As Third Wall™ policies are assigned to entire ConnectWise Automate® Locations, license counts are calculated using all reporting Windows computers per Location. This means the total number of agents within a Location are counted when a policy is employed, regardless of the number of exceptions within the Location or the number of policies activated.
        ii. Once a policy is enabled for the Location, adding more policies to the same Location will not impact licensing. Nor will button use within the Location regardless of the number of uses. Adding computers to the Location, however, will increase the license consumption accordingly.
        iii. Monthly billing is based on the peak number of consumed licenses during the course of a month.
        iv. Once Third Wall is used within a Location, all of the computers in that Location are counted for billing until and unless you send an email to support@third-wall.com with specific instructions to remove a Location from billing. Simply turning all Third

Wall policies off within a Location will not remove that Location from being counted for billing purposes.

c. What is the minimum monthly license purchase?
    i. The minimum monthly Third Wall™ license is 100 computers. Each additional computer covered by Third Wall™ policies will be billed at the then-current rate, and is computed daily. Your actual bill will be based on the peak number of computers within all Locations covered actively by Third Wall within your bill month.
d. What's the best way to get started with Third Wall?
    i. Begin by reviewing the policies available in Third Wall™ in detail. Determine which of the policies would improve your clients' environments. We strongly recommend you create a test Location under your existing Client and populate it with examples appropriate to simulate environments you'll be deploying to. Enable the desired Third Wall™ policies to your test Location and you've taken your first step!
e. How do I see the changes Third Wall™ makes?
    i. When a Third Wall™ monitor makes a change on any computer, it creates a ConnectWise Automate® Ticket notifying you of this change. Use the ConnectWise Automate® 'Tickets' tab to see all Third Wall™ modification made by a monitor.
f. Why is Third Wall™ generating ConnectWise Automate® Tickets?
    i. While successful Third Wall™ changes made by a monitor are recorded by a ConnectWise Automate® Ticket, any failed Third Wall™ change will also result in a ConnectWise Automate® Ticket. This ticket will list the process that failed, the applied policy that caused it to run and any other Windows® error code that could be read by the remote Operating System.
    ii. Two Third Wall™ policies primarily activate monitors which generate tickets upon finding undesired conditions. The "Alert on Unencrypted Disk" and "Monitor EventLog Clearing" policies are looking for these undesired conditions, and generate a ticket which you must manually close.
g. Is USB Wall included in my Third Wall subscription?
    i. Yes. USB is now included in all Third Wall Gold subscriptions at no additional charge.