

CONNECTWISE AUTOMATE™

TECHNICAL EVALUATION GUIDE

Contents

Contents

CONTENTS 1

USING THIS GUIDE..... 4

Navigating This Document 4

OVERVIEW 5

1. Core Architecture 6

 1.1 Agent 6

 1.2 Control Center 7

 1.3 Groups 7

2. Cross-Platform Support..... 8

3. Discovery 8

 3.1 Asset Discovery 8

 3.2 Asset Inventory 8

4. Remote Control 9

 4.1 ConnectWise® Control™ (formerly ScreenConnect) 9

 4.2 Redirectors..... 9

 4.3 Lights-Out Management..... 9

5. Systems Management10

 5.1 Desktop and Server Management..... 10

 5.2 Software Distribution 11

 5.3 Self Service 12

 5.4 Infrastructure Management..... 13

6. Windows Patch Management14

 6.1 Update Policies 15

 6.2 Reboot Policies..... 15

 6.3 Approval Policies..... 15

 6.4 Agent Device Patch Management 15

7. Systems Monitoring.....	16
7.1 Desktop and Server Monitoring	16
7.2 Network Monitoring	17
7.3 Infrastructure Monitoring	18
8. Alerting	19
9. Automation	20
9.1 Scripting	20
9.2 Corrective Actions/Self Healing	21
10. Integration	22
10.1 Platform	22
10.2 3 rd Party Patch Management	22
10.3 Active Directory	23
10.4 Backup & Disaster Recovery	24
10.5 Endpoint Security.....	24
10.6 Out-of-Band & Power Management	25
10.7 Professional Services Automation (PSA)	25
10.8 Two-Factor Authentication.....	25
11. Reporting	26
11.1 Dataviews.....	26
11.2 Heads Up Displays	26
11.3 Report Center.....	27
11.4 SAP® Crystal Reports® (legacy).....	Error! Bookmark not defined.
12. Distributed Communication & File Transfer.....	28
12.1 Agent-Based Communication	28
12.2 Agent-Based File Transfer	28
12.3 Agentless Communication	28
12.4 Agentless File Transfer	28
13. Administration & Usage.....	28
14. Customization	29
15. Multilingual Capabilities	29
15.1 Language Pack Editor.....	29
15.2 Localized Agent Functionality	29

16. Scalability30

16.1 Single Server 30

16.2 Split Server..... 30

16.3 Hosted 31

17. Security31

17.1 Agent..... 31

17.2 Control Center 32

MINIMUM SYSTEM REQUIREMENTS 33

ABOUT CONNECTWISE 33

Using This Guide

This Evaluation Guide will give you the information you need to understand the true power of ConnectWise® Automate™. Our objective is to provide straight-forward information, without all the hype. You know what your business needs and why. Our job is simply to show you how ConnectWise can help.

Navigating This Document

This document is designed to help you easily locate the information you need most. You'll see words highlighted throughout the guide, which allow you to link quickly to the [Overview](#) or other relevant sections. After you've clicked a link, you can easily navigate back to your previous section by holding ALT on your keyboard and pressing the left arrow (ALT + Left Arrow).

Overview

Businesses need to move fast, with IT services that are easy to deliver and continually monitored, so end users stay productive. IT professionals want to drive efficiency and reduce costs while providing more value to end users.

Delivering value—along with proactive and reactive IT services—becomes less difficult with ConnectWise, which incorporates years of experience in meeting end-user needs—both inside and outside the firewall.

ConnectWise® Automate™ serves as the IT management piece of the ConnectWise® Suite™ to provide features and capabilities that help you:

- Learn one product to rapidly and efficiently manage the day-to-day operations of your business
- Automate repeatable processes and tasks to enable better focus on projects and strategic goals
- Do more with less while reliably and efficiently managing more systems

ConnectWise Automate is a platform that enables IT to move at the speed of business, without the hidden costs of other IT management systems. Automate is licensed as an agent-based technology. Licensing comes in two (2) flavors—perpetual and subscription. Perpetual is offered at a higher monthly cost, but results in full ownership at the end of the agreement. Subscription is offered at a lower monthly costs, but ownership remains with ConnectWise®.

With ConnectWise Automate, you get freedom of choice. While all core functionality and ConnectWise Solutions are included in your Automate license, Invent Solutions are handled separately. Click any of the links below to learn more.

Core Functionality

- [Core Architecture](#)
- [Cross-Platform Support](#)
- [Discovery](#)
- [Remote Control](#)
- [Systems Management](#)
- [Windows Patch Management](#)
- [Systems Monitoring](#)
- [Alerting](#)
- [Automation](#)
- [Integration](#)
- [Reporting](#)
- [Distributed Communication & File Transfer](#)
- [Administration & Usage](#)
- [Customization](#)
- [Multilingual Capabilities](#)
- [Scalability](#)
- [Security](#)

ConnectWise Solutions

- [3rd Party Patch Management](#)
- [Active Directory](#)
- [Infrastructure Management](#)
- [Infrastructure Monitoring](#)
- [Out-of-Band & Power Management](#)
- [PSA & Service Desk](#)
- [Two-Factor Authentication](#)

Invent Solutions

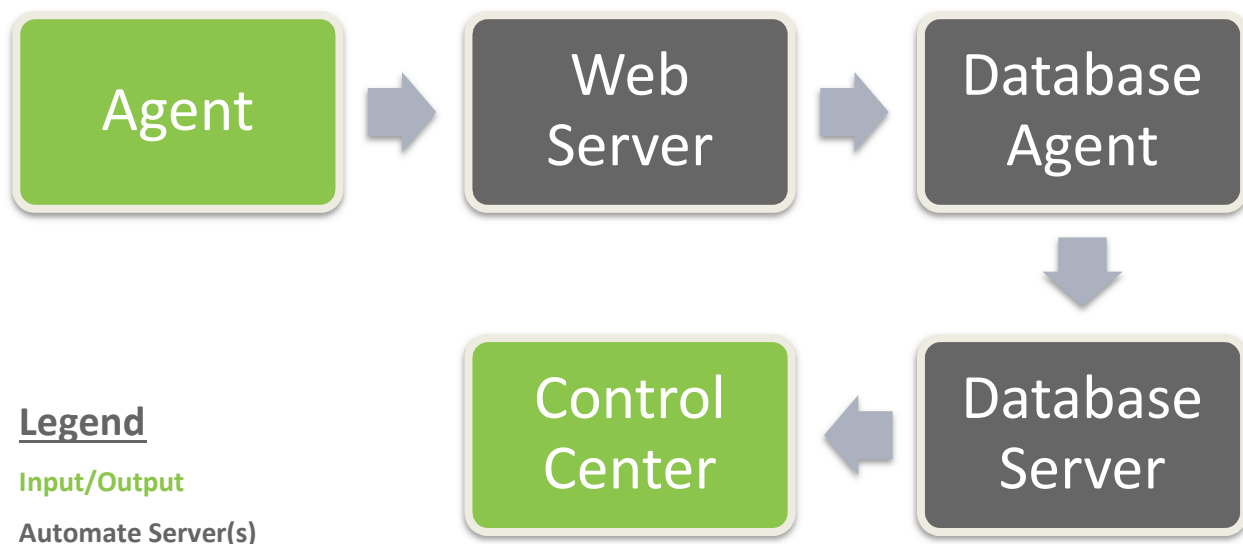
- [Backup & Disaster Recovery](#)
- [Endpoint Security](#)

1. Core Architecture

Most businesses and IT departments want to understand how ConnectWise Automate's Core Architecture is structured. Automate is an agent-based technology. The core of Automate relies on two (2) methods of input and output—the agent and Control Center. Both methods communicate with a central server (see [Scalability](#)), which hosts the Database Agent and distributes the communication back out. Beyond basic input and output, the core of Automate as an automation engine is the concept of Groups, which are also described in this section.

1.1 Agent

ConnectWise Automate's agent consists of two (2) primary components—the Automate Service and Service Watchdog. The agent can optionally consist of two (2) additional components—the Tray Icon Service and Network Probe. On average, these combined components are expected to consume less than 100MB of memory and 1% CPU. Once installed, data begins passing from the agent device to an Automate Web Server, to the Database Agent (a.k.a. Automation Server), to the Database Server, and back again.



Data In

At each check-in, the agent requests any pending commands that have been issued by a Control Center user or script.

Data Out

At each check-in, the agent sends command results, status updates ([link](#)), and any scheduled inventory (see [Asset Inventory](#)).

The agent and optional Tray Icon Service are configured using customizable Agent Templates, which allow you to define multiple settings ([link](#)). Some commonly used settings include:

- Server Address(es)
- Caching
- Branding
- Access Modes
- Tray Menus
- [Antivirus](#) Policies

Automate's Network Probe (optional) provides asset discovery and specific agentless capabilities. Any agent on a Windows device can be designated as a Network Probe. Once configured, a registry key is created and five (5) files are downloaded to the agent device—totaling 80.7MB in size. Three (3) files are for agent deployment to detected Windows devices. The other two (2) files are for core Network Probe functionality. Automate's Network Probe communicates in conjunction with the agent and Control Center.

1.2 Control Center

ConnectWise Automate's Control Center is available in two (2) flavors, each intended for specific purposes—the installable Control Center and Web Control Center. The installable Control Center provides all Automate functionality and is intended for day-to-day use by Automate users. The Web Control Center provides [Desktop and Server Management](#) functionality for individual agent devices and is intended for use by end users (see [Client Portal](#)) and Automate users unable to immediately access the installable Control Center.

Unless directly connected to the Automate Database, data passes from the Control Center to an Automate Web Server, to the Automation Server, to the Database Server, and back again.

Data In

Every action by an Automate user.

Data Out

Every management command and remote monitor.

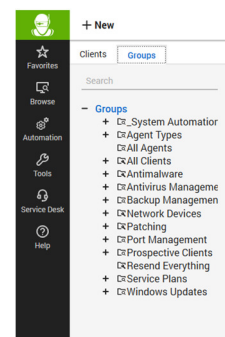
NOTE: While ConnectWise offers an iOS and Android Control Center app, due to limited adoption since 2011, the apps are no longer intended for normal use.

1.3 Groups

Groups are the heart of Automate as an automation engine. Groups come in multiple types ([link](#)) with varying levels of membership ([link](#)), yet the core concepts remain the same: find members, join them to a group, and automate some action(s). Best practice group membership involves the following:

1. **Find Members:** Define what identifies a desired group member and create a search ([link](#)). If the information isn't available, simply create an Extra Data Field ([link](#)) and make it available.
2. **Join Members to a Group:** Apply the search to your desired group.
3. **Automate Some Action(s):** Different actions are available depending on the group's membership. However, some common examples include:

- Apply an Agent Template
- Apply a Maintenance Window
- Assign [Managed Services](#)
- Schedule Scripts
- Set Group Specific [Alerting](#)
- Set Group Specific Permissions ([link](#))



[Return to Overview](#)

2. Cross-Platform Support

Another item you want to verify is whether a solution will work within your supported environment. ConnectWise supports agent functionality for multiple Windows, Mac, and Linux operating systems. Because not every OS works the same way, ConnectWise provides a list of specific supported agent functionality for each OS ([link](#)). For IT professionals that need to understand agent compatibility with specific OS versions, ConnectWise provides this information for our current and previous releases ([link](#)).

3. Discovery

Technology businesses and IT departments—regardless of size, maturity, or resources—need visibility into their supported environment(s) to start standardizing and streamlining IT services for similar devices. This section describes how ConnectWise Automate discovers and inventories both agent and agentless devices.

3.1 Asset Discovery

ConnectWise Automate provides a single method for asset discovery—the Network Probe. Simply install an agent on a Windows device with network access to all desired IP ranges at your target location, and designate it as a Network Probe. As soon as an agent is designated as a Network Probe, a wizard will walk you through configuration.

Once configured, the Network Probe will ping all IPs within the Network Probe's local address range (additional IP ranges can be added after initial configuration), and create a network device in the location for any IPs that respond. After a network device is created, the Network Probe uses Detection Templates to query the device and attempt to re-detect/classify the device.

Additionally, the Network Probe can automatically deploy agents to detected Windows devices (requires Administrator credentials). However, agents can also be installed manually or through Group Policy.

3.2 Asset Inventory

After assets are discovered, Automate provide two (2) methods of asset inventory—agent and agentless. Devices with agent-based inventory will automatically update based on agent schedules. Devices with agentless inventory require Collection Templates to define update details and schedules.

Agent Inventory (non-customizable)

- Hardware
- Software
- Patches
- Users
- Event Logs
- Services
- And More ([link](#))

Agentless Inventory (customizable)

- Storage Details
- Printer Details

NOTE: Agentless inventory requires a Network Probe in the same location as the inventoried device(s).

[Return to Overview](#)

4. Remote Control

With ConnectWise Automate, IT professionals can confidently support end users regardless of where they are. If a device is connected to the Internet, you're connected to it. For redundancy purposes, Automate provides three (3) methods for remote control—ConnectWise Control, redirectors, and lights-out management. While each method is recommended for specific purposes, all methods allow for connection logging, as well as configuration of end-user preferences, such as end-user consent.

4.1 ConnectWise® Control™

ConnectWise offers and recommends ConnectWise Control, an industry-leading remote control product, for remote control of any agent device. Control provides fast, secure, and reliable remote control functionality, such as session recording, multi-monitor support, screen blanking, and more ([link](#)). In addition to the installable Control Center, Control is also available through the Web Control Center for Automate users and end users (see [Self Service](#)). While ConnectWise Control can be purchased separately, Automate includes Control's seamless Remote Access functionality free of charge for all ConnectWise customers.

4.2 Redirectors

ConnectWise Automate provides multiple out-of-the-box redirectors/redirected applications for agent-based devices, along with the ability to add custom redirectors. ConnectWise recommends redirectors when ConnectWise Control is not possible. Some commonly used redirectors include:

1. **PuTTY:** Secure Shell (SSH) and Telnet offer direct terminal access for Linux device agents and agentless network devices.
2. **Remote Desktop:** Offers RDP access for Windows device agents and can be configured for automated authentication using the location's defined **Administrator Access** credentials.
3. **Web Browser:** Offers web browser access for agentless network device setup page(s).

4.3 Lights-Out Management

ConnectWise Automate provides three (3) out-of-the-box redirectors for a form of out-of-band management commonly called lights-out management (LOM)—PuTTY, Remote Desktop, and Web Browser. Each of these LOM redirectors function as described above, but originate from the location's Network Probe and connect to the agent device's Management IP. ConnectWise recommends LOM redirectors for Dell DRAC and HP iLO access.

NOTE: LOM redirectors require a Network Probe in the same location as the target device(s).

[Return to Overview](#)

5. Systems Management

Remote control is a great reactive service, but IT professionals need to remotely troubleshoot issues without interrupting the end user—not to mention work on multiple systems at the same time. ConnectWise Automate provides both agent and agentless systems management, so your team can do more with less. This section describes how IT professionals can leverage Automate to manage agent devices (see [Desktop and Server Management](#)), perform [Software Distribution](#) and [Self Service](#), along with integrated agentless management for virtualized hardware (see [Infrastructure Management](#)).

5.1 Desktop and Server Management

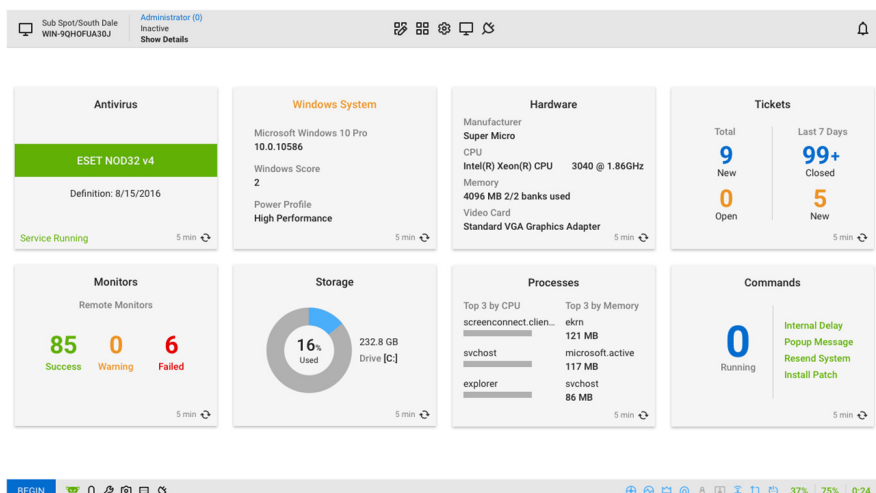
IT professionals need to work on and effectively manage multiple machines at the same time, often surpassing the limits of any remote control tool. ConnectWise Automate helps you efficiently manage more systems and solve issues with a robust Computer Management Screen that eliminates the need to interrupt your end user(s).

The Computer Management Screen provides agent details (see [Asset Inventory](#)) and over 100 out-of-the-box commands for desktop and server management ([link](#))—as well as plugin/[integration](#) specific commands. Commands are used to send specific instructions to agent devices during their next check-in. In addition to out-of-the-box commands, you are also able to add custom commands.

Some common Desktop and Server Management commands include:

- Deploy Approved Patches
- Disk Cleanup
- Disk Defrag
- Download File
- End Process
- Install Patch
- Reattempt Failed Patches
- Reboot
- Remote Control
- Remove Patch
- Request Screenshot
- Resend Inventory
- Reset Password
- Restart Service
- Set as Default Printer
- Shutdown
- Uninstall Application
- Unlock Account
- Update Virus Definitions
- Wake-on-LAN

Desktop and Server Management is also provided with [Scripting](#), which is commonly used to combine and orchestrate multiple Desktop and Server Management commands.



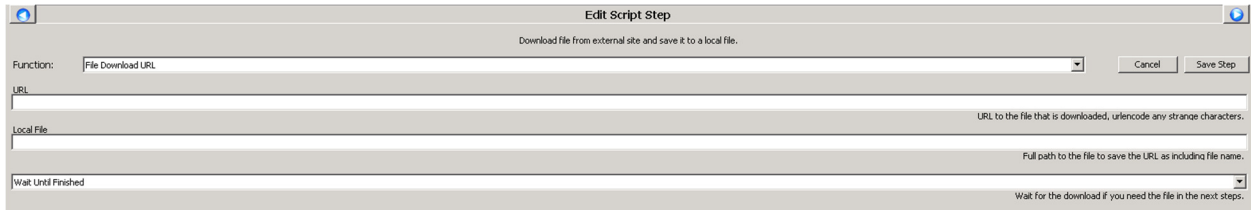
[Return to Overview](#)

5.2 Software Distribution

End users need software. You need to get it to them as easily as possible. With ConnectWise Automate, IT professionals can confidently and efficiently distribute software to multiple machines at the same time.

Automate provides a single method for software distribution—[Scripting](#). Software distribution with Automate can be super simple or highly complex, depending on your specific needs. Yet the core concepts remain the same:

1. **File Download:** Where is the software installer located and where will the agent store it?
2. **Shell Execute:** What command should the agent execute to install this software?



The screenshot shows the 'Edit Script Step' dialog box. At the top, it says 'Download file from external site and save it to a local file.' Below this, there are several fields and buttons:

- Function:** A dropdown menu currently set to 'File Download URL'. Buttons for 'Cancel' and 'Save Step' are to the right.
- URL:** A text input field.
- Local File:** A text input field.
- Wait Until Finished:** A dropdown menu set to 'Wait Until Finished'.

Small instructional text is visible next to the URL and Local File fields: 'URL to the file that is downloaded, urlencode any strange characters.' and 'Full path to the file to save the URL as including file name.'

What makes software distribution so simple is that it works the way you work. There's no need to extract MSI files. Additional logic is commonly added, such as checking if the software is installed before script execution ([link](#)), verifying the software installed ([link](#)), creating a ticket to log success or failure of the install ([link](#)), etc. Some out-of-the-box samples include:

- Adobe Flash Player 10 Active X
- Adobe Reader 10.0.1
- Google Chrome for Work
- Java Runtime Environment (JRE) v6u33
- Microsoft Fix It
- Microsoft Silverlight

NOTE: Check with the software installer's vendor for appropriate silent/quiet install command switches.

[Return to Overview](#)

5.3 Self Service

Most businesses and IT departments want to streamline, or at least reduce, end-user requests by helping users help themselves. To address this challenge, ConnectWise Automate provides two (2) methods for end-user self service—the Tray Icon ([link](#)) and Client Portal ([link](#)). Both methods enable specific functionality and can be used together for a more complete self-service experience.

5.3.1 Tray Icon

The Tray Icon (see [Core Architecture](#)) is configurable for three (3) types of end-user self service using customizable Agent Template settings:

1. **Tickets** (default): End users can create, update, and delete their own tickets in Automate.
2. **Language** (optional): End users can select a preferred Tray Icon Language (see [Multilingual Capabilities](#)).
3. **Scripts** (optional): End users can run any Computer Script (see [Software Distribution](#) and [Scripting](#)) that has been made available.

5.3.2 Client Portal

When accessed by an end user, ConnectWise Automate's Web Control Center is referred to as the Client Portal and allows three (3) types of end-user self service using contact permissions ([link](#)):

1. **Tickets**: End users can create, update, and delete their own tickets in ConnectWise Automate.
2. **Remote Control**: End users can remotely access any of their assigned agent device(s).
3. **Desktop Management**: End users can send three (3) commands to any of their assigned agent device(s)—Reboot, Shutdown, and Wake-on-LAN.

[Return to Overview](#)

5.4 Infrastructure Management

We live in an increasingly virtualized world. As your business grows and adopts more virtualization technology, ConnectWise is ready to help. Automate's integrated Virtualization Manager provides six (6) commands for agentless infrastructure management of Hyper-V® and VMware®. Hyper-V commands are used to send specific agent commands (see [Desktop and Server Management](#)). VMware commands are used to send specific vSphere PowerCLI cmdlets during the next Network Probe check-in.

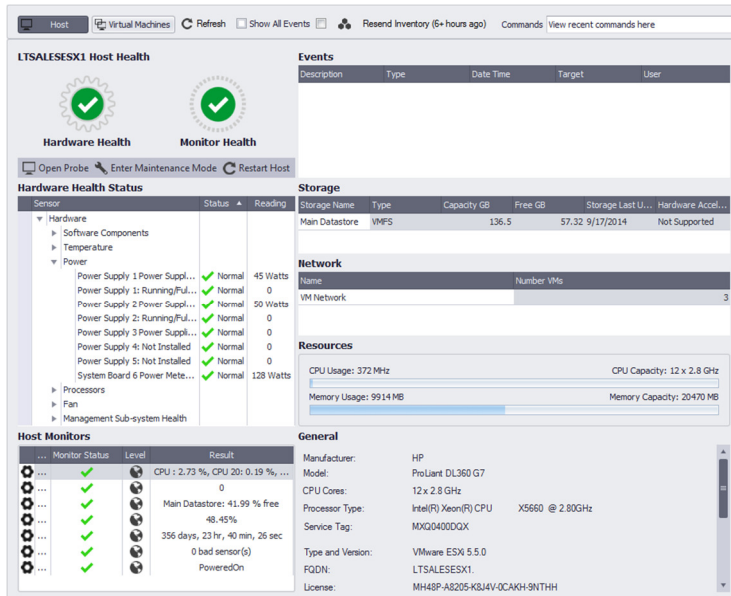
Host Management

- Enter Maintenance Mode (VMware)
- Resend Inventory
- Restart Host

Virtual Machine Management

- Restart
- Shutdown
- Suspend

NOTES: (1) Infrastructure management for VMware is agentless and requires a Network Probe in the same location as the managed infrastructure. (2) Infrastructure management for Hyper-V is agent-based and requires an agent be installed on the Hyper-V host. (3) Infrastructure management is considered a ConnectWise [Solution](#).



The screenshot displays the 'Host Management' section for a host named 'LTSALESEX1'. The interface includes several panels:

- Host Health:** Shows 'Hardware Health' and 'Monitor Health' with green checkmarks indicating good status.
- Hardware Health Status:** A table listing various sensors and their readings.

Sensor	Status	Reading
Power Supply 1: Power Supply...	Normal	45 Watts
Power Supply 2: Running/Pul...	Normal	0
Power Supply 3: Running/Pul...	Normal	50 Watts
Power Supply 4: Running/Pul...	Normal	0
Power Supply 5: Not Installed	Normal	0
Power Supply 6: Not Installed	Normal	0
System Board 6: Power Mete...	Normal	128 Watts
- Storage:** A table showing storage details.

Storage Name	Type	Capacity GB	Free GB	Storage Last U...	Hardware Accel...
Main Datastore	VMFS	136.5	57.32	9/17/2014	Not Supported
- Network:** A table showing network details.

Name	Number VMs
VM Network	3
- Resources:** Displays CPU and memory usage.

Resource	Usage	Capacity
CPU Usage	372 MHz	12 x 2.8 GHz
Memory Usage	9914 MB	20470 MB
- Host Monitors:** A table showing the status of various monitors.

Monitor	Status	Level	Result
CPU	2.73 %	Normal	CPU 20: 0.19 %
Main Datastore	41.99 % free	Normal	48.45 %
356 days, 23 hr, 40 min, 26 sec			
0 bad sensor(s)			
PoweredOn			
- General:** Provides detailed information about the host.

Property	Value
Manufacturer	HP
Model	ProLiant DL360 G7
CPU Cores	12 x 2.8 GHz
Processor Type	Intel(R) Xeon(R) CPU X5660 @ 2.80GHz
Service Tag	MXQ0400DQX
Type and Version	VMware ESX 5.5.0
FQDN	LTSALESEX1.
License	MH48P-A8205-KB4V-0CAKH-9NTHH

[Return to Overview](#)

6. Windows Patch Management

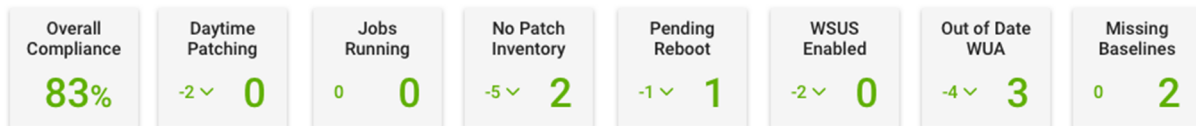
When securing your supported environment, the most basic proactive service is patch management—so systems aren’t vulnerable to known attacks. ConnectWise empowers IT professionals to patch multiple machines at the same time and manage by exception, so you can efficiently secure more endpoints without creating packages.

To accomplish this, ConnectWise provides a single method for Windows patch management—the Automate agent. Simply install an agent on a device and Update Policies will define the default behavior for Windows Update. With Managed Mode, you gain complete control over the Windows Update Agent. Once in control, you can start the process of scheduling Windows Patch updates, reboots, and approvals.

Out of the box, Automate helps you configure Windows patch management quickly with easy-to-use [Update Policy](#) options for Microsoft® updates and [3rd Party Patches](#), [Reboot Policies](#), simple setup for [Approval Policies](#), and [Agent Device Patch Management](#) for one-off or emergency situations.

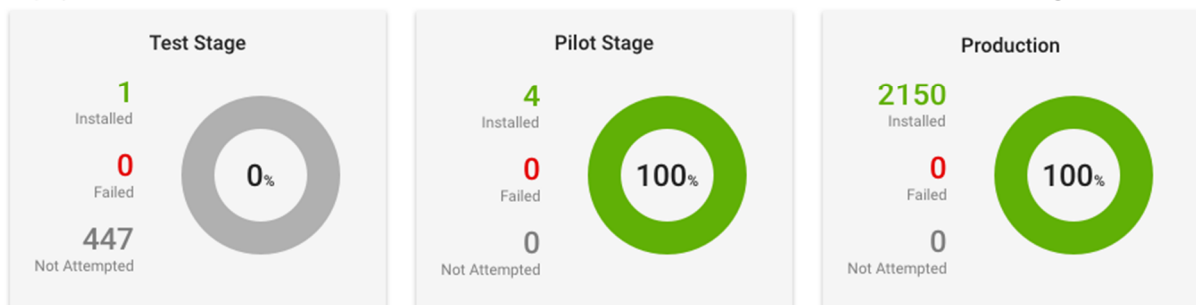
NOTES: (1) While ConnectWise Automate leverages Windows Background Intelligent Transfer Service (BITS) for patch inventory, the Automate agent downloads all patches directly from Microsoft’s Support website, unless configured for caching (see [Agent-Based File Transfer](#)). (2) ConnectWise does not provide any patch management functionality for Mac and Linux OS’s (see [Cross-Platform Support](#)).

Current Status



Deployment

Date Range: [Month to Date](#)



Compliance

Date Range: [Current](#)



[Return to Overview](#)

6.1 Update Policies

ConnectWise Automate allows patching for every location ([link](#)). Scheduling is configured in the Patch Manager using Update Policies to define when approved patches should be installed. Update Policies can be applied to workstations, servers, and specific server role groups to join all appropriate agent devices at an enabled location. Beyond scheduling, Update Policy options also allow for Wake-On-LAN or [Out-of-Band & Power Management](#) (to turn on powered off agents) and running a script before and/or after patch install. Update Policies are available for Microsoft Updates and [Third Party Updates](#) (optional). By default, approved patches are installed on the specified day between 3 a.m. and 5 a.m.

6.2 Reboot Policies

Reboot Policies are configured in the Patch Manager and compliment Update Policies. While Update Policies define when approved patches should be installed, Reboot Policies define how the Automate agent should act when an installed patch requires a reboot.

6.3 Approval Policies

ConnectWise Automate's Patch Manager allows for fully automated decisioning of patches ([link](#)). Approval Policies (a.k.a. patch decisions) define what patches should be acted on and are applied to a Patch Manager group for top-down inheritance by all sub-groups. For example, if you need to approve every Microsoft update with an Important and Critical severity, simply check the Important and Critical Severity options under Automatic Approve on the Default approval policy. If you only need to prevent installation of the 'Get Windows 10' app on workstations, simply add the title [KB3035583](#) under Automatic Deny on the Workstations Override approval policy.

Approval Policy decisions include:

1. **Approve:** Approves the patch for installation during the Automate agent's next [Update Policy](#)
2. **Ignore:** Keeps the patch in the end user's list of available updates and removes the patch from Automate's list of Discovered but Not-Set patches
3. **Deny:** Removes the patch from the end user's list of available updates

In addition, decisions defined on the Default approval policy can be staged across your supported environment by using Routine Approval. With Routine Approval enabled, newly discovered patches (see [Asset Inventory](#)) are approved first on devices marked as Test, with a delay time before approval on Pilot or Production devices—empowering your business to follow Microsoft Best Practices ([link](#)).

NOTE: Deny always overrides Approve and Ignore.

6.4 Agent Device Patch Management

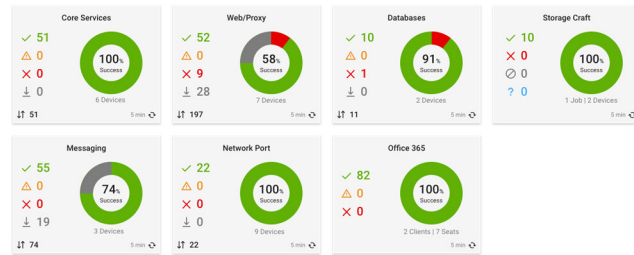
The Computer Management Screen provides [Desktop and Server Management](#) patch commands (e.g. Install Patch and Remove Patch) that take immediate effect, regardless of [Update Policies](#). Because [Approval Policies](#) will override agent device patch management, this method is not commonly recommended.

[Return to Overview](#)

7. Systems Monitoring

The first step for IT professionals seeking better reactive and proactive response times is monitoring—something ConnectWise Automate has in spades. Automate’s out-of-the-box experience (a.k.a. Ignite) helps you get started quickly, with easy-to-use Service Plan options (see [Desktop and Server Monitoring](#))

for every location ([link](#)), internal monitors for printers (see [Network Monitoring](#)), and integrated agentless monitoring for virtualized hardware (see [Infrastructure Monitoring](#)).



7.1 Desktop and Server Monitoring

At some point, every business experiences a service interruption that requires IT to perform a root cause analysis (RCA). One of the most common frustrations that come out of an RCA is the question: “Were you checking [insert tool no one else is aware of]?” With ConnectWise Automate, you get a single source of monitoring for all devices—meaning your team has only one place to check. Automate provides two (2) methods for desktop and server monitoring—internal monitors and remote monitors. Both methods allow for customizable monitoring intervals, as well as alerting and/or corrective action.

Internal Monitors

- Up/Down
- Event Logs
- Hardware
- Patches
- Services
- Software
- Users
- And More ([link](#))

Remote Monitors

- Event Logs
- Executable Results
- Files and Directories
- Network
- Performance Counters
- Registry
- Services and Processes
- System Information
- Website Latency
- WMI Results

7.1.1 Internal Monitors

Internal monitors are used to monitor device inventory changes by querying the Automate Database. Because automated inventory updates are controlled by agent schedules, internal monitors are not recommended for more real-time monitoring needs—with the exception of status updates ([link](#)), like Up/Down, which are updated at every check-in (regardless of inventory). Internal monitors can be configured globally, or for specific clients, locations, or groups of devices. While internal monitors can also be configured for an individual device, they are not recommended for this purpose.

7.1.2 Remote Monitors

Remote monitors are used to directly monitor a device, regardless of inventory updates. These monitors live on agent devices and return results to the Automate Server(s). Remote monitors can be configured for an individual device and are recommended for this purpose. Once configured, remote monitors can easily be distributed to specific groups of devices.

NOTE: Ignite Management Packs use remote monitors.

[Return to Overview](#)

7.2 Network Monitoring

As previously mentioned (see [Desktop and Server Monitoring](#)), ConnectWise Automate is a single source of monitoring for all devices—meaning your team has only one place to check and can eliminate the question: “Were you checking [insert tool no one else is aware of]?” Automate provides three (3) methods for network monitoring—internal monitors, remote monitors, and trap filters. All methods allow for customizable alerting.

Internal Monitors

- Up/Down
- Printer Errors
- Printer Supplies
- Storage Details
- Custom Collection Template Values

Remote Monitors

- Up/Down
- Bandwidth
- SNMP Object Identifier (OID)
- Web-Based Enterprise Management (WBEM)

NOTES: (1) Network monitoring is agentless and requires a Network Probe in the same location as the monitored network device(s). (2) Trap filters require each agentless device be configured to send the appropriate data to the location’s Network Probe.

7.2.1 Internal Monitors

Internal monitors are used to monitor network collected values by querying the Automate Database. Because automated updates are controlled by Collection Templates, internal monitors are not recommended for more real-time monitoring needs—with the exception of Up/Down, which is updated at every check-in (regardless of Collection Template). Internal monitors can be configured globally, or for specific clients, locations, or groups of devices. While internal monitors can also be configured for an individual device, they are not recommended for this purpose.

7.2.2 Remote Monitors

Remote monitors leverage the Network Probe to directly query/monitor a device, regardless of Collection Template. These monitors live on the location’s Network Probe and return results to the Automate Server(s). Remote monitors can be configured for an individual device and are recommended for this purpose. Once configured, remote monitors can easily be distributed to specific groups of devices.

7.2.3 Trap Filters

Trap filters are used to monitor two (2) types of data sent by configured network devices to a Network Probe—SNMP Messages and Syslog Events. Because this method requires network devices be preconfigured to send applicable data to a Network Probe, trap filters must be configured individually for each desired Network Probe.

[Return to Overview](#)

7.3 Infrastructure Monitoring

Our world is increasingly virtualized. As your business grows and adopts more virtualization technology, ConnectWise is ready to help. Automate provides two (2) types of infrastructure monitoring for Hyper-V® and VMware®—host monitors and virtual machine monitors. Both methods allow for customizable monitoring intervals, as well as alerting. All infrastructure monitors can be configured globally or per device. Some common infrastructure monitors include:

Host Monitors

- CPU Percentage Per Core
- Disk Percentage
- Memory Usage
- Power State Test
- Recently Restarted

Virtual Machine Monitors

- CPU Percentage Per Core
- Disk Percentage
- Memory Ballooned (VMware)
- Memory Pressure (Hyper-V)
- Power Status

NOTES: (1) Infrastructure monitoring for VMware is agentless and requires a Network Probe in the same location as the monitored infrastructure to leverage vSphere PowerCLI. (2) Infrastructure monitoring for Hyper-V is agent-based and requires an agent be installed on the Hyper-V host. (3) Infrastructure monitoring is considered a ConnectWise [Solution](#).

7.3.1 Host Monitors

Host monitors are used to monitor your infrastructure host by leveraging the Network Probe to directly query the host and return results to the Automate Server(s).

7.3.2 Virtual Machine Monitors

Virtual machine (VM) monitors are used to monitor the VMs running on your infrastructure host device(s). Just like host monitors, these monitors leverage the Network Probe to directly query the host and return results to the Automate Server(s).















Configure Global Monitors

Enabled Globally

Disabled Globally















Host Monitors

Remove Overrides

Name	Enabled	Operator	Value	Interval	Alert Template
 ESX-Host CPU Percentage Per Core		Less Than	80	1 Minute	Default - Do Nothing
 ESX-Host Disk Resets		Equals	0	1 Minute	Default - Do Nothing
 ESX-Host Disk Percentage		Greater Than	10	1 Minute	Default - Do Nothing
 ESX-Host Memory Usage		Less Than	80	1 Minute	Default - Do Nothing
 ESX-Host Recently Restarted		Greater Than	300	1 Minute	Default - Do Nothing
 Host Bad Sensor Count		Equals	0	1 Minute	Default - Do Nothing
 Host Power State Test		Equals	1	1 Minute	Default - Do Nothing

Virtual Machine Monitors

Remove Overrides

Name	Enabled	Operator	Value	Interval	Alert Template
 ESX-VM CPU Percentage Per Core		Less Than	80	1 Minute	Default - Do Nothing
 ESX-VM Disk Percentage		Greater Than	10	1 Minute	Default - Do Nothing
 ESX-VM Memory Usage		Less Than	80	1 Minute	Default - Do Nothing
 ESX-VM Memory Ballooned		Less Than	500	1 Minute	Default - Do Nothing
 VM Power Status		Equals	1	1 Minute	Default - Do Nothing
 VM Guest Operation Mode		Equals	running	1 Minute	Default - Do Nothing
 VM Guest Tools Running		Equals	3	1 Minute	Default - Do Nothing

[Return to Overview](#)

8. Alerting

The second step for IT professionals seeking faster reactive and proactive response times is alerting. ConnectWise Automate's out-of-the-box experience (a.k.a. Ignite) helps IT professionals get started quickly, with preconfigured Service Plan options for every location ([link](#)).

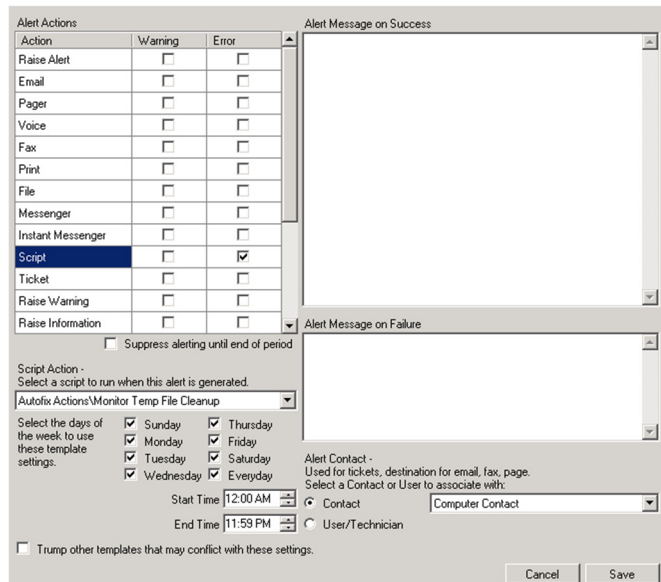
For more advanced needs, Automate provides three (3) core concepts for alerting—intervals, frequencies, and alert templates. Monitor intervals define how often Automate checks the condition(s). Monitor frequencies define how often Automate executes the alert template. Alert templates define what action a failed monitor condition triggers. Alert templates can be set globally, per group, or per device.

Some common alert template actions include:

- Create Ticket
- Raise Alert
- Run Script
- Send Email

NOTES: (1) While ConnectWise Automate can create tickets, it is not a true ticketing system. (2) Send Email requires Mail Setup to be configured ([link](#)).

[Return to Overview](#)



Action	Warning	Error
Raise Alert	<input type="checkbox"/>	<input type="checkbox"/>
Email	<input type="checkbox"/>	<input type="checkbox"/>
Pager	<input type="checkbox"/>	<input type="checkbox"/>
Voice	<input type="checkbox"/>	<input type="checkbox"/>
Fax	<input type="checkbox"/>	<input type="checkbox"/>
Print	<input type="checkbox"/>	<input type="checkbox"/>
File	<input type="checkbox"/>	<input type="checkbox"/>
Messenger	<input type="checkbox"/>	<input type="checkbox"/>
Instant Messenger	<input type="checkbox"/>	<input type="checkbox"/>
Script	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ticket	<input type="checkbox"/>	<input type="checkbox"/>
Raise Warning	<input type="checkbox"/>	<input type="checkbox"/>
Raise Information	<input type="checkbox"/>	<input type="checkbox"/>

☐ Suppress alerting until end of period

Script Action -
Select a script to run when this alert is generated.
Autofix Actions\Monitor Temp File Cleanup

Select the days of the week to use these template settings:

<input checked="" type="checkbox"/> Sunday	<input checked="" type="checkbox"/> Thursday
<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Friday
<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Saturday
<input checked="" type="checkbox"/> Wednesday	<input checked="" type="checkbox"/> Everyday

Start Time: 12:00 AM
End Time: 11:59 PM

☐ Trump other templates that may conflict with these settings.

Alert Contact -
Used for tickets, destination for email, fax, page.
Select a Contact or User to associate with:
Contact: Computer Contact
User/Technician

Cancel Save

9. Automation

Automation is the third and final step for IT professionals striving to achieve the best reactive and proactive response times possible. To assist, ConnectWise Automate provides almost 400 out-of-the-box [Scripting](#) examples for maintenance, [Software Distribution](#), system automation, and more ([link](#)). In addition, Automate's out-of-the-box experience (a.k.a. Ignite) helps your business move fast with easy-to-use Service Plan options (see [Corrective Actions/Self Healing](#)) for every location ([link](#)).

9.1 Scripting

Technology businesses and IT departments are increasingly busy and end users are more impatient than ever. As the demands on IT increase, your team needs the agility to adapt. In essence, you need to automate any process or task so your team can focus on delivering value instead of putting out fires.

To help, Automate provides three (3) methods for automation—on-demand scripts, scheduled scripts, and alert templates (see [Corrective Actions/Self Healing](#)). Scripting is function-based (e.g. [Software Distribution](#)), using natural language terms so anyone capable of writing technical documentation can use them. All Automate scripts follow the concept of IF-THEN-ELSE, and can be used to automate actions for three (3) types of objects—agent devices, agentless devices, and clients.

Script
Globals and Parameters
Permissions
Find Script
Licensing
Time Recording

Name: Chrome Uninstaller
Target: Computer
Notes: Removes Google Chrome from the computer system.

☐ Offline Computer Script
☐ Isolated Script
☐ Maintenance Script
☐ System Script
☐ Function Script
☐ Public Script

IF: Software Installed
Checks if software package is installed and sets the %softwarelocation% variable with the path.

App Name: %Chrome%
The name of the application to check for.

Then

Statement	Exit On Failure	All Operating Systems
1 IF FILE Exists %windir%\TSvc\Packages\google\chrome_installer.msi THEN Jump to :Uninstall	Exit On Failure	All Operating Systems
2 Create Folder: %windir%\TSVC\Packages\google	Exit On Failure	All Operating Systems
3 DOWNLOAD: https://dl.google.com/chrome/install/GoogleChromeStandaloneEnterprise.msi s...	Continue On Failure	All Operating Systems
4 IF FILE Exists %windir%\TSvc\Packages\google\chrome_installer.msi THEN Jump to :Uninstall	Exit On Failure	All Operating Systems
5 LOG: Google Chrome on %computername% at %clientname% failed to uninstall! Failed to...	Exit On Failure	All Operating Systems
6 Create New Ticket for %ClientID%\%ComputerID% Email:%ContactEmail% Subject:Googl...	Exit On Failure	All Operating Systems
7 Exit Script	Exit On Failure	All Operating Systems
8 :Uninstall - Label	Exit On Failure	All Operating Systems
9 SHELL: msixec /x %windir%\TSVC\Packages\google\chrome_installer.msi /qn REBOOT=Re...	Exit On Failure	All Operating Systems
10 Resend Software	Exit On Failure	All Operating Systems
11 IF NOT SOFTWARE INSTALLED %Chrome% THEN Jump to :Success	Exit On Failure	All Operating Systems
12 LOG: Google Chrome FAILED to uninstall on %computername%- %computerid%. Here are ...	Exit On Failure	All Operating Systems
13 Exit Script	Exit On Failure	All Operating Systems
14 :Success - Label	Exit On Failure	All Operating Systems
15 LOG: Removed Google Chrome on %computername%- %computerid% successfully.	Exit On Failure	All Operating Systems

Else

Statement	Exit On Failure	All Operating Systems
1 Exit Script	Exit On Failure	All Operating Systems
2 Note: Lines Below are added to aid the export of these scripts	Exit On Failure	All Operating Systems
3 RUN SCRIPT: Software\Google\Chrome Installer	Exit On Failure	Function Disabled

[Return to Overview](#)

9.1.1 Agent Devices

ConnectWise Automate provides multiple out-of-the-box script functions for [Desktop and Server Management](#) (a.k.a. computer scripts). These functions are intended to mirror and expand existing management capabilities for individual agent devices, so Automate users can manage multiple devices at once. Agent device scripts can be run on groups, clients, locations, or individual devices.

In addition to computer scripts, Automate provides contact scripts to automate tasks across all of a contact's/end user's assigned agent devices.

9.1.2 Agentless Devices

While Automate does not provide native Network Management functionality, it does provide out-of-the-box script functions for specific network device automation. These functions are intended for individual agentless devices and are not commonly recommended for use on multiple devices at once. Some common network device functions include:

1. **Set SNMP OID:** Sets the value of an Object Identifier (OID)
2. **Establish Connection:** Secure Shell (SSH) Open and Telnet Open establish terminal connections for additional automation.
3. **Send Data:** Send Raw and Send Secure pass commands and results to established connections.
4. **Terminate Connection:** Secure Shell (SSH) Close and Telnet Close terminate terminal connections.

NOTE: ConnectWise recommends the Establish Connection and Terminate Connection functions always be used together.

9.1.3 Clients

Client scripts are recommended for automating tasks within the ConnectWise Automate product itself, such as updating multiple extra data field (EDF) values at once. These scripts cannot be run on devices and are intended for use on clients only. Client scripts are considered advanced and require a more in-depth and holistic understanding of ConnectWise Automate.

9.2 Corrective Actions/Self Healing

Scripting is great, but IT professionals need help automating some of their most common requests and fixes. Automate's out-of-the-box experience provides 37 out-of-the-box corrective/auto-fix actions for self-healing ([link](#)). Corrective actions are simply preconfigured alert templates (see [Alerting](#)) that run a script (see [Scripting](#)) when a monitored condition fails. Beyond out-of-the-box corrective actions, administrators are encouraged to add custom corrective actions based on their specific environments.

Some common corrective actions include:

- Defragment Drive
- Domain Controller Diagnostics (DCDiag)
- Fix Windows Update
- Kill Bad Process
- Reboot Computer
- Resend Antivirus (AV) Definitions
- Restart Service
- Temp File Cleanup

[Return to Overview](#)

10.Integration

What about applications, tasks, and processes outside of ConnectWise Automate's core functionality? Integration delivers transformative next-level automation for businesses seeking to reduce IT complexity and siloed processes, and increase IT agility and technician dexterity. While additional integrations exist, this section describes how your business can leverage ConnectWise as a [platform](#) for seven (7) key areas:

- [3rd Party Patch Management](#)
- [Active Directory](#)
- [Backup & Disaster Recovery](#)
- [Endpoint Security](#)
- [Out-of-Band & Power Management](#)
- [PSA & Service Desk](#)
- [Two-Factor Authentication](#)

NOTE: [Infrastructure Management](#) and [Infrastructure Monitoring](#) are considered core ConnectWise Solutions and are described as a part of [Systems Management](#) and [Systems Monitoring](#).

10.1 Platform

ConnectWise provides a single method for platform integration—the Developer Network ([link](#)). Access to the Developer Network is offered to all ConnectWise customers, along with approved 3rd party vendors. The Developer Network provides tools and documentation to help participants quickly create meaningful integrations.

All approved and supported integrations (a.k.a. solutions) are available for download by administrators in the Solution Center ([link](#)) and are enabled/disabled through the Plugin Manager ([link](#)).

Some common integrations include:

- 3rd Party Patch Management
- Active Directory
- Backup & Disaster Recovery
- Endpoint Security
- Out-of-Band & Power Management
- Password Management
- PSA & Service Desk
- Remote Control
- Reporting
- Two-Factor Authentication

10.2 3rd Party Patch Management

ConnectWise Automate's core functionality includes [Windows Patch Management](#) with optional [Update Policies](#) for third party applications ([link](#)). However, other 3rd party patch management options do exist—such as Chocolatey ([link](#)) and Ninite ([link](#)).

[Return to Overview](#)

10.3 Active Directory

IT professionals frequently prefer a single username/password, and businesses demand streamlined and standardized IT services for all of an end user's associated devices. To address these challenges, Automate provides two (2) methods for Active Directory integration—LDAP and the Active Directory Solution. Both methods are intended for specific purposes and can be used together for a more complete experience.

10.3.1 LDAP

ConnectWise Automate's core LDAP, or Lightweight Directory Access Protocol, integration is for IT professionals seeking password standardization. With Automate's core LDAP integration, users can leverage their Active Directory password to access the ConnectWise Automate product. Once configured, Automate user credentials will be checked against the Automate Database. If the Automate user's password does not match what is stored, the credentials will be verified with LDAP. If successful, the Automate user's password will be updated in the Automate Database and access will be granted.

NOTES: LDAP integration is part of the core ConnectWise Automate product and does not require Solution Center download.

10.3.2 Active Directory Solution

The Active Directory Solution is for businesses seeking centralized inventory and management of Active Directory Users. With ConnectWise Automate's integrated Active Directory Solution, you can automatically create contacts based on configurable Active Directory filters.

User Inventory

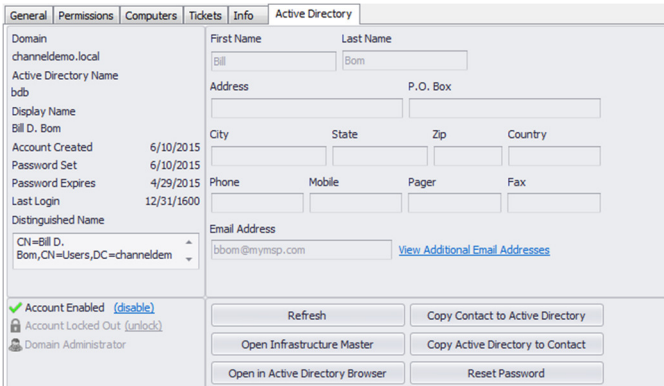
- Account Created Date
- Last Login Date
- Password Set Date
- Password Expires Date
- And More ([link](#))

User Management

- Change Active Directory Group Membership
- Enable/Disable Account
- Reset Password
- Set Password to Never Expire
- Unlock Account

In addition to centralized inventory and management, the Active Directory Solution provides automation for Managed Services ([link](#)) to help IT track applied end-user services, such as Microsoft® Office 365™.

NOTES: (1) The Active Directory Solution requires an agent on the Infrastructure Master. (2) The Active Directory Solution inventories and manages Domain Users. The Computer Management Screen inventories and manages local Users ([link](#)). (3) Contacts created from other sources, such as [PSAs & Service Desks](#), can also be linked to Users in Active Directory.



[Return to Overview](#)

10.4 Backup & Disaster Recovery

Many businesses and IT departments require regular backup of servers and desktops for effective disaster recovery planning. To ease the day-to-day management and monitoring of these applications, ConnectWise Automate offers backup and disaster recovery integration with six (6) industry-leading products:

- Acronis Backup Cloud ([link](#))
- Gladinet CentreStack ([link](#))
- Storage Guardian ([link](#))
- StorageCraft ShadowProtect ([link](#))
- Veeam Backup & Replication ([link](#))
- Veeam Endpoint Backup ([link](#))

Because no two (2) backup and disaster recovery products are exactly alike, each integrated solution offers different integration points and capabilities that your ConnectWise Account Manager can discuss. ConnectWise encourages you to leverage whichever product(s) best meet your business needs.

10.5 Endpoint Security

Your business demands endpoint security that reduces the risk of external attack. To ease the day-to-day management and monitoring of these applications, ConnectWise Automate offers two (2) types of endpoint security integration—antivirus/anti-malware and email security.

10.5.1 Antivirus/Anti-malware

ConnectWise Automate offers antivirus/anti-malware integration with six (6) industry-leading products:

- Bitdefender® Cloud Security ([link](#))
- ESET Endpoint Security ([link](#))
- Malwarebytes Endpoint Security ([link](#))
- HitmanPro by SurfRight ([link](#))
- VIPRE by ThreatTrack Security ([link](#))
- Webroot SecureAnywhere® ([link](#))

Because no two (2) antivirus/anti-malware products are exactly alike, each integrated solution offers different integration points and capabilities that your ConnectWise Account Manager can discuss. ConnectWise encourages you to leverage whichever product(s) best meet your business needs.

NOTE: Not all malware is a virus, but all viruses are malware.

10.5.2 Email Security

ConnectWise Automate offers email security integration with one (1) industry-leading product—Sophos' Reflexion ([link](#)). This integrated solution enables four (4) remote monitors for agent devices that use Reflexion ([link](#)).

[Return to Overview](#)

10.6 Out-of-Band & Power Management

Wake-on-LAN is a great technology for businesses with time to configure it, and that aren't overly concerned with security. For everyone else though, out-of-band management is commonly needed. Beyond Lights-Out Management (see [Remote Control](#)) ConnectWise Automate offers out-of-band and power management integration with one (1) industry-leading product—Intel® vPro™ ([link](#)). This integrated solution enables specific [Desktop Management](#) and [Scripting](#) functionality for vPro-enabled agent devices, along with automated configuration.

Some commonly used functions include:

- KVM (Keyboard-Video-Mouse) Redirector
- Power On vPro Device
- Power Off vPro Device
- Provision vPro
- Unprovision vPro

NOTES: (1) The KVM redirector requires another agent device in the same location as the target device(s). (2) ConnectWise recommends the KVM redirector for non-server agent devices experiencing a blue screen. (3) [LOM Redirectors](#) are recommended for Dell DRAC and HP iLO access.

10.7 Professional Services Automation (PSA)

We believe in choice. And while ConnectWise Automate can create tickets, it is not a true ticketing system. So if you're using a Professional Services Automation (a.k.a. PSA) solution to manage your IT operations, we're here to help. ConnectWise Automate offers two (2) options for PSA integration—ConnectWise® Manage™ ([link](#)) and Autotask® ([link](#)). Each integrated solution offers different integration points and capabilities, but the core concepts remain the same:

1. **Discovery:** Automate your service desk's [Discovery](#) of devices/configurations.
2. **Actions:** Take action on service desk tickets with the Computer Management Screen (see [Remote Control](#) and [Desktop and Server Management](#)).
3. **Ticketing:** Achieve operational consistency while efficiently throttling the auto-generation, categorization, and routing of any monitored failure (see [Alerting](#)).
4. **Automation:** Automate redundant tasks with a service catalog that delivers based on your approval process (see [Automation](#)).

NOTES: (1) ConnectWise does not recommend or support any many-to-one configuration for PSA integration. (2) The **Automation** concept is only available with ConnectWise Manage integration.

10.8 Two-Factor Authentication

Many businesses and IT departments require two-factor authentication (2FA) for regulatory and compliance reasons (e.g. PCI DSS Requirement 8.3). To help businesses meet these requirements, ConnectWise Automate offers integration with three (3) industry-leading products—AuthAnvil ([link](#)), Duo ([link](#)), and Google Authenticator ([link](#)).

[Return to Overview](#)

11.Reporting

Reporting is more than a requirement, it's a responsibility. Out of the box, ConnectWise Automate provides three (3) types of reporting—Dataviews, Heads Up Displays, and Report Center—all allowing for customization and quick access to your data.

11.1 Dataviews

ConnectWise Automate provides over 100 out-of-the-box dataviews. Dataviews are used to immediately view and interact with a wealth of system information and can be run on clients, locations, groups, or individual devices. Beyond out-of-the-box dataviews, you are also able to add custom dataviews.

Client	Location	Computer Name	Agent OS	User	Agent Type	Status	Agent Asset Tag
Headquarters	Administration	WIN7X64-0	Microsoft Windows 7 Enterprise x64	Not Logged In	WorkStation	Online	FHWQQ21243
Headquarters	Administration	WIN8X32-0	Microsoft Windows 8 Pro	Not Logged In	WorkStation	Online	No Asset Tag
Headquarters	ITS DataCenter App SVRS	WINSERVER08-0	Microsoft Windows Server 2008 R2 Standard x64	WINSERVER08-0\tmarengi	Server	Online	No Asset Tag
Headquarters	ITS DataCenter DC	WINSRV2012R-0	Microsoft Windows Server 2012 R2 Standard x64	CHANNELDEMO\Administrator	Server	Online	No Asset Tag
Remote Site 1	Administration	WIN7X32-0	Microsoft Windows 7 Professional	Not Logged In	WorkStation	Online	No Asset Tag
Remote Site 1	Administration	WIN8X32-2	Microsoft Windows 8 Pro	Not Logged In	WorkStation	Online	No Asset Tag
Remote Site 1	Sales	WIN8X32-1	Microsoft Windows 8 Pro	Not Logged In	WorkStation	Online	No Asset Tag

Some commonly used dataviews include:

- Assets > Network Devices
- Assets > Servers
- Assets > Workstations
- Commands > All Commands
- Contacts > Computer Contacts
- Patching > Patch History
- Reports > Scheduled Reports
- Scripts > Queued Scripts
- Software > Full Software Listing
- Startup Items > Boot Execute

11.2 Heads Up Displays

ConnectWise Automate provides eight (8) out-of-the-box Heads Up Displays (HUDs). HUDs are used to create persistent data visualizations within Automate which often include dataviews. Beyond out-of-the-box HUDs, administrators are also able to add custom HUDs.

The most commonly used HUD is Patch Status ([link](#)).



[Return to Overview](#)

11.3 Report Center

ConnectWise Automate's Report Center provides 15 out-of-the-box DevExpress® reports. Report Center is used to generate printable information for non-ConnectWise users to view and has two (2) methods for generation—on-demand and scheduled email. On-demand reports are generated in Report Center by selecting the report and clicking View Report. Scheduled email reports are generated in Report Center by using the New Schedule Wizard.

Asset Summary



ConnectWise Automate

Address 4110 George Rd, Suite 200
Tampa, FL 33634

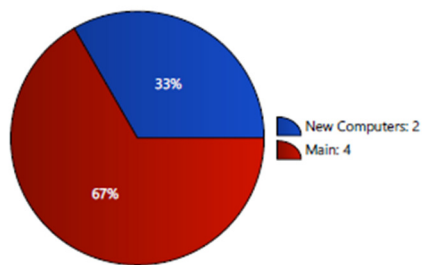
Country
Phone
Fax
Locations 2

Asset Analysis

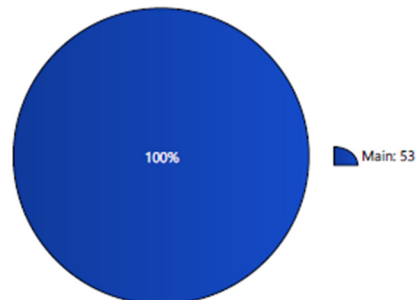
Servers	Workstations	Network Devices
4	2	53
	Windows	Other
Servers	4	0
Workstations	2	0

Assets by Location

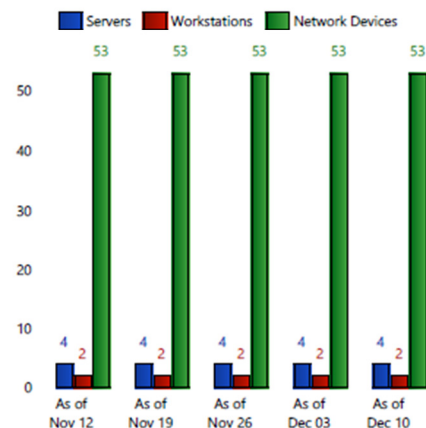
Computers



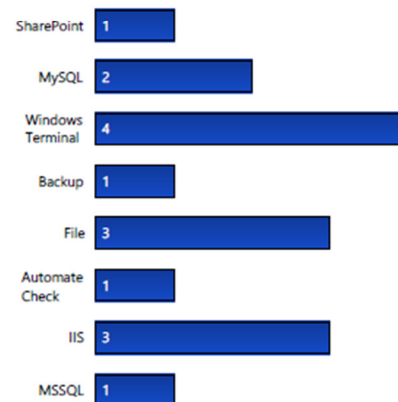
Network Devices



Deployment History



Server Roles



NOTES: (1) Report Center is a Solution (see [Platform](#)). (2) Health Reports require use of the Standards and Health Solution ([link](#)). (3) Scheduled email reports require Mail Setup to be configured ([link](#)).

[Return to Overview](#)

12. Distributed Communication & File Transfer

As your business grows, the likelihood of end users staying in the same building or even on the same network starts to disappear. To keep end users happy and productive, IT professionals need tools that help reduce overall bandwidth utilization to provide the highest network availability possible. This section details how ConnectWise optimizes communication and file transfers for both agent and agentless devices.

12.1 Agent-Based Communication

ConnectWise Automate does not provide any distributed communication with agent devices. All communication to and from agent devices is direct and cannot be routed through a different agent or device. For businesses with strict distributed communication needs, ConnectWise recommends installing a separate Automate server at each site.

12.2 Agent-Based File Transfer

ConnectWise Automate provides a single method for distributed file transfer to agent devices—caching ([link](#)). With caching, agent devices download all patches and scripted file downloads to a caching directory for other agent devices at the location to reference.

12.3 Agentless Communication

ConnectWise Automate provides a single method for distributed communication with agentless devices—the Network Probe. All communication to and from agentless devices are routed through the location's Network Probe.

12.4 Agentless File Transfer

ConnectWise Automate provides a single method for distributed file transfer to agentless devices—the Network Probe's TFTP Server. All file transfers to and from agentless devices are routed through the TFTP Server on the location's Network Probe.

13. Administration & Usage

ConnectWise Automate provides a single method for administration—the installable Control Center (see [Core Architecture](#)). The installable Control Center provides all Automate functionality and is intended for day-to-day use by Automate users—especially administrators. ConnectWise provides multiple resources to educate and assist administrators in achieving their specific goals—such as online documentation, training videos, boot camps, etc. Administrators are encouraged to leverage these resources as much as possible and provide feedback regarding their helpfulness.

ConnectWise often hears that using Automate can feel complex at first—and nostalgic of the 1990s. ConnectWise takes this feedback seriously and is making strides to improve ([link](#)).

[Return to Overview](#)

14. Customization

Every business and IT department runs differently, meaning IT professionals need solutions they can easily customize. ConnectWise Automate provides functionality to customize nearly all areas of the product. ConnectWise recommends you customize Automate to fit your specific business needs and offers multiple professional service options to help businesses seeking customization based on best practices.

However, there are certain areas that cannot be customized outside the Developer Network (see [Platform](#)). Some examples include:

- Agent Inventory ([link](#))
- Agentless Management ([link](#))
- Core Architecture ([link](#))
- Control Center Interface
- Integrations/Plugins ([link](#))
- Ignite Service Plans
- Web Control Center Interface

NOTE: Customization of a Ignite Service Plan is defined as renaming or duplicating. Configuration of existing Ignite Service Plans is fully supported.

15. Multilingual Capabilities

For businesses that support multilingual users, ConnectWise Automate provides two (2) methods for localization—the Language Pack Editor and localized agent functionality. ConnectWise recommends multilingual businesses evaluate and utilize whichever method(s) best meet their specific needs.

15.1 Language Pack Editor

The Language Pack Editor is intended for businesses who need to localize verbiage used by the ConnectWise Automate Agent and/or Control Center (see [Core Architecture](#)). Businesses that utilize this method are typically more interested in reselling the ConnectWise product or IT services Automate helps them provide.

15.2 Localized Agent Functionality

Automate's agent interacts directly with the system—a.k.a. Operating System (OS) kernel—which uses English for most major OS distributors (see [Cross-Platform Support](#)). Because of this, all supported [Desktop and Server Management](#) commands offer localized functionality, including [Windows Patch Management](#).

Additionally, [Desktop and Server Monitors](#) can leverage OS user accounts, which may utilize non-English languages. To address this challenge, [Remote Monitors](#) can be localized to support multilingual end users.

[Return to Overview](#)

16. Scalability

As your business scales, you rightfully expect solutions to scale with you. Given the appropriate resources and configuration, ConnectWise Automate can be extremely scalable. Automate provides three (3) methods for scalability—single server, split server, and hosted. Each method offers specific advantages and disadvantages, which ConnectWise encourages you to consider before purchase. Additionally, ConnectWise provides a Scalability Guide ([link](#)) for businesses needing to handle all hardware ownership that will be used to run ConnectWise Automate (i.e. Single Server and Split Server).

16.1 Single Server

Most administrators configure all of Automate's [Core Architecture](#) (Web Server, Automation Server, and Database Server) to run on a single machine. With this method, administrators must also decide if they'll use physical or virtualized infrastructure. Administrators that decide to run Automate on physical infrastructure are typically more interested in high performance. Administrators that decide to run Automate on virtualized infrastructure are typically more interested in backup and disaster recovery.

Advantage(s)

- Low infrastructure cost

Disadvantage(s)

- Single point of failure (SPOF)

NOTE: ConnectWise Control (see [Remote Control](#)) is a separate product provided free of charge for all Automate customers. While the Control Server can be installed on the same machine as Automate's [Core Architecture](#), it is not recommended for businesses with more than 1200 agent devices.

16.2 Split Server

Businesses with high scalability needs often seek a Split Server configuration, where Automate's [Core Architecture](#) (Web Server, Automation Server, and Database Server) is configured to run on two (2) or three (3) separate machines—a Front End Web Server, Automation Server, and Backend Database Server. With this method, administrators must still decide if they'll use physical or virtualized infrastructure. Administrators that decide to run Automate on physical infrastructure are typically more interested in high performance. Administrators that decide to run Automate on virtualized infrastructure are typically more interested in backup and disaster recovery.

Advantage(s)

- Distributed points of failure
- Potential for clustering & load balancing

Disadvantage(s)

- Moderate infrastructure cost
- Requires professional services

NOTE: Because Split Server is considered advanced and requires an in-depth and holistic understanding of ConnectWise Automate, this method is not supported unless installed and configured using our Professional Service Associates.

[Return to Overview](#)

16.3 Hosted

ConnectWise recommends this method for businesses not interested in handling the hardware ownership needed to run Automate. With this method, administrators are provided an Amazon AWS instance using the Single Server configuration. While the Split Server configuration is also available, businesses often prefer a separate hosted instance over a separate hosted Web Server and/or Database Server.

Advantage(s)

- No infrastructure cost
- No infrastructure maintenance
- Fully automated upgrades

Disadvantage(s)

- Higher subscription cost per agent
- Not available as a perpetual license

17.Security

Last, but not least, for businesses and IT departments concerned about unauthorized system access, ConnectWise Automate provides two (2) methods of security for input and output—the agent and Control Center (see [Core Architecture](#)).

17.1 Agent

Agent communication (a.k.a. data in transit) is secured using three (3) specific methods—agent passwords, agent SSL policy, and encrypted [Remote Control](#). ConnectWise recommends administrators leverage all three methods for a more complete security experience.

1. **Agent Passwords:** On first check-in, every newly installed agent device receives a randomly generated password from the Automate Server(s) that will be used to encrypt and decrypt data in and data out.
2. **Agent SSL Policy:** Agent Template setting for ConnectWise customers with an SSL certificate on the Automate Web Server. By default, agent SSL policy is set to accept any SSL errors. For ConnectWise customers with expired, untrusted, mismatched, or revoked SSL certificates on the Automate Web Server, this policy will allow continued agent device communication.
3. **Encrypted Remote Control:** All ConnectWise Control functionality use AES-256 encryption and, by default, all Automate redirectors use AES-128 encrypted tunnels. For businesses with higher encryption needs, tunnels can be set to AES-192 or AES-256. For businesses with no encryption needs, tunnels can be disabled while still allowing redirector functionality.

Agent device data (a.k.a. data at rest) is secured outside of the product, often involving Active Directory, network firewalls, antivirus/anti-malware, etc.

[Return to Overview](#)

17.2 Control Center

Control Center communication and data is secured using a single method—user permissions. User permissions are defined in five specific areas of the product—User Classes, Group Permissions, Client Permissions, Command Level Limits, and Script Permissions. ConnectWise recommends administrators leverage all five areas for a more complete Control Center security experience.

1. **User Classes** (foundational): Define overall product permissions for Automate users. Automate users with multiple assigned User Classes will possess the combined permissions of all assigned User Classes.
2. **Group Permissions**: Define User Class permissions for agent devices joined to the group (see [Core Architecture](#)). Agent devices joined to multiple groups with defined permissions will use the combined User Class permissions from all groups.
3. **Client Permissions**: Define User Class permissions for clients, locations, and agent devices. Agent device permissions defined here will be combined with agent device group permissions.
4. **Command Level Limits**: Define which commands (see [Desktop and Server Management](#)) an Automate user can utilize. Automate users can have a Command Level Limit of 0–4. Commands can be set to 0–5. Any commands set to 5 are only available for use by Super Admins.
5. **Script Permissions**: Define User Class permissions for individual scripts.

NOTE: The Exclusion Group type ([link](#)) with defined User Classes will prevent each defined User Class from accessing agent devices joined to the group.

[Return to Overview](#)

Minimum System Requirements

See [Core Architecture](#), [Cross-Platform Support](#), and [Scalability](#) for more information.

Web Server

- .NET Framework 3.5
- IIS 7

Automation Server

- .NET Framework 3.5 SP1
- Windows Server 2008 R2

Database Server

- MySQL 5.6 (x86, 64-bit)
- or MariaDB 10 (winx64)

Installable Control Center

- .NET Framework 3.5 SP1
- Windows 7 SP1
- Windows 8
- Windows 10

Windows Agent

- Windows Server 2008 SP2, Server 2008 R2 SP1, Server 2012, Server 2012 R2, Server 2016
- Windows Vista SP2, Windows 7 SP1, Windows 8, Windows 10

NOTE: Windows Embedded is not supported.

Mac Agent

- OSX 10.9, 10.10.5, 10.11, macOS Sierra

Linux Agent

- CentOS, Debian, Fedora, OpenSUSE, Red Hat Enterprise Linux (RHEL), SUSE Enterprise, Ubuntu

About ConnectWise

ConnectWise Automate is a powerful IT management platform that helps deliver IT services at the speed of business. Designed with cutting-edge, agent technology; ConnectWise Automate offers both proactive and reactive IT solutions from a single console to significantly improve productivity, drive efficiency, and reduce costs. See why over 5,000 partners worldwide chose ConnectWise by visiting www.connectwise.com or calling 877-522-8323.

[Return to Overview](#)

Copyright ©2018 ConnectWise. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. ConnectWise assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, ConnectWise provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will ConnectWise be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill, or lost data, even if ConnectWise is expressly advised in advance of the possibility of such damages.