ConnectWise

Automate™

GLOBAL SECURITY & COMPLIANCE

ConnectWise Automate™

Contents

Overview

ConnectWise Automate™ is an IT management platform used to improve efficiency and productivity by providing monitoring and management of endpoint machines, built-in scripts to accomplish routine tasks, and extensive automation capabilities for maintenance and issue resolution.

This document addresses the following topics:

- How ConnectWise Automate works
- Data in motion and at rest in ConnectWise Automate
- What security features are natively implemented
- Recommendations and best practices
- Security in the ConnectWise Automate cloud offering
- Privacy and data protection

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 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 (ATL + Left Arrow).

1 Inside ConnectWise Automate™

Security in ConnectWise Automate is handled by the agent-based remote system monitor, as well as by the server's database.

1.1 Agent Communications

The agent is designed in push mode, meaning the remote endpoint communicates by pushing data from itself to the server. This method is designed to ensure that the agent is the one to initiate a connection with the server, as opposed to listening for incoming connections.

1.1.1 Agent Check-In

By default, installed agents check in with the Automation Server over the standard Hypertext Transfer Protocol (HTTPS) via TCP. Once the agent connects to the Automation Server and sends its current status, it retrieves its pending commands.

1.1.2 ConnectWise® Control™ Plugin (v1.2.14+)

ConnectWise Control is a remote support, access, and meeting solution that integrates with ConnectWise Automate and can be installed on the same server.

The ConnectWise Control Plugin and the ConnectWise Control Remote Plugin, once installed, provide remote access to any agent machine managed through the Control Center; the former allows for a connection to the target machine directly from the Computer Management screen, and the Remote Plugin works in conjunction with the ScreenConnect Plugin to enable a connection between the Control Center and the remote agent.

Communication between the Control Center and the ConnectWise Control agent takes place over TCP and is brokered by the ConnectWise Control server application.

All session data from the Control Center to the agent is automatically encrypted in AES-256 block encryption combined with RSA-256 (Microsoft RSA/Schannel Cryptographic Provider).

1.1.3 Tunnels & Redirectors

Connections like Remote Desktop Protocol (RDP) or other remote-control programs originate on the agent machine. A tunneled connection is then created to carry traffic from the Control Center to the agent.

ConnectWise Automate leverages several Mediation Servers for connection "handshakes" and negotiations between the Control Center and the agent machine. Both endpoints submit outbound requests to the Mediation Server and once a connection is negotiated, communication takes place between the two endpoints (Point-to-Point) over UDP.

As a failover tunnel method, both the Control Center and the agent machine submit outbound requests for the Automation Server to initiate a connection. Once a connection is established, communication relays through the Automation Server over TCP.

1.2 Native Security

1.2.1 Encryption

Passwords stored in the database are AES-encrypted and the database implements table-level security, which gives a second layer of access control that allows or prevents read/write operations based on the user's permissions.

1.2.2 Automate Server Security

Recommended login and use of the ConnectWise Automate product should be encapsulated through an HTTPS connection versus direct connect through port 3306. The HTTPS communication protocol uses industry-standard TLS encryption and the internal agent communication leverages additional Triple DES (3-DES) encryption.

All passwords used for remote agents (data sent/received) are 16-character, randomly generated strings, and data payloads are compressed before being transmitted; these measures enhance the level of security under SSL/TLS conditions.

Software communication channels can be broken into three (3) categories:

1. **Control Center:** HTTPS is the default preferred method of connection as it utilizes industry standards of TLS 1.0, 1.1, and 1.2, which can be modified based on preference of supported environments. See required Best Practices below.
2. **Web Control Center/Client Portal:** By default, all Automate portals through a web browser are forced HTTPS.
3. **Agent:** Endpoint communication data between the Automate server and its agents is natively encrypted with Triple DES (3DES) before it is transmitted from the agent machine to the Automation Server.

1.3 Best Practices

- **REQUIRED:** Installing a SSL/TLS certificate secures the agent-server communications channel and encrypts sessions (HTTPS) with the level configured in the Web server (IIS).
- By default, ConnectWise Control communicates through an unencrypted channel; configuring ConnectWise Control with SSL/TLS to secure its traffic is highly recommended.
- The ConnectWise Automate and ConnectWise Control applications can be installed on the same server as well as share the same SSL/TLS certificate.

2 Data & Compliance

Regulatory requirements need to be addressed by implementing a foundation of business best practices to protect the integrity and privacy of client data. These practices focus on creating standardized processes for handling protected data, training staff accordingly, and building layered security practices that provide physical, network, and system-based security of the client's regulated data.

2.1 Compliance Requirements

ConnectWise Automate is designed with capabilities intended to assist partners in meeting some compliance requirements. Two states of data that raise security concerns are:

- Data in Motion
  - Encryption
  - Transmission
- Data at Rest
  - Database
  - Auditing

2.1.1 Data in Motion

Encryption & Transmission

When a SSL/TLS certificate is installed and configured at the IIS level, the initial "handshake" exchange is encrypted as well as any subsequent communications, in addition to the data being hashed. Beyond the encapsulated HTTPS protocol, communication data between the Automate server and its agents is additionally encrypted natively with Triple DES (3DES) before it is transmitted from the agent machine to the Automation Server.

All passwords used for remote agents (data sent/received) are randomly generated and data payloads are compressed before being transmitted; these measures enhance the level of security under SSL/TLS conditions.

2.1.2 Data at Rest

Database

Passwords stored in the database are AES-encrypted and the server implements table-level security, which gives a second layer of access control that allows or prevents read/write operations based on the user's permissions.

Auditing

Auditing can be used to track changes in ConnectWise Automate and notify technicians of significant events, such as the creation or modification of client scripts, groups, schedules, alert templates, maintenance windows, blacklisted items, etc. Most of the actions that can be performed in the Control Center can be audited. Each action that can be audited is assigned an audit level from 0-5:

0 = Nothing	3 = Informational
1 = Critical	4 = Normal
2 = Significant	5 = Everything

When an action occurs, the audit action level is compared to the auditing level of the user. If the level set for the user is greater than or equal to the audit action level, it will be added to the audit trail.

Audit information in ConnectWise Automate is stored by default for 120 days. In order to meet certain compliance requirements, you may need to prolong the retention period for the audit data, which could

be extended indefinitely. However, due of potential bottlenecks that can affect performance, it is recommended to export the data periodically if the table size becomes excessively large.

2.2 Recommended Best Practices for Regulated Client Data

As an IT management platform, ConnectWise Automate can be configured to operate in such a way as to enhance security and client confidentiality. Below are several configuration guidelines that can be implemented when providing services to clients with regulatory concerns.

2.2.1 Best Practice I: Regulated Client Data

Regulated client data should not be stored on your Automation Server or on any of your other systems.

Limiting the number of places that data is stored can limit your clients' potential risk for unauthorized access as well as your own. If your policy states that you do not store your clients' data on your Automation Server and you can demonstrate the processes and controls enforcing this policy in your business, you can reduce the risks associated with maintaining sensitive data on your systems.

2.2.2 Best Practice II: Access to Client Systems

Audit and log all access to client systems.

All sessions of access into client systems should be audited and logged. These records should be retained to document instances where your business and/or staff have accessed a client's regulated data.

2.2.3 Best Practice III: Remote Access to Client Systems

Remote access to client systems should be authorized and documented.

Remote access tools – RDP, ConnectWise Control, or other redirectors – enable you to directly interact with client systems and potentially access regulated data in them. ConnectWise Automate is designed to log each redirector that is launched, compiling a history of who has accessed individual systems as well as which redirected applications were used to access each system.

2.2.4 Best Practice IV: User Security Roles

User roles should be used to implement the principle of least privilege.

The principle of least privilege states that "every program and every user of the system should operate using the least set of privileges necessary to complete the job." ConnectWise Automate has a multi-tier permissions system in place, and its class-based access controls should be used to limit users' access to client data by assigning only the permissions necessary for job performance.

2.2.5 Best Practice V: Client Systems Credentials

Access credentials belonging to client systems should be audited and protected.

Data stored on the Automation Server for access to client systems should be logged and protected based on user security roles. The most specific type of data concern for user access control is regarding authentication credentials, which are documented in order to allow access to client systems. The ability to read, edit, or delete client passwords is defined in the Client Details screen within the Control Center.

3 ConnectWise Automate Cloud Offering

ConnectWise Automate's cloud offering is hosted remotely, which reduces or eliminates overhead costs associated with on-premise servers. Cloud offerings, also known as Software as a Service (SaaS), remove the need for organizations to handle the installation, setup, and often daily upkeep necessary for server maintenance.

3.1 Amazon Web Services (AWS)

All of ConnectWise Automate's cloud server instances, storage volumes, and databases are hosted by Amazon Web Services (AWS). Amazon's sophisticated implementation of large-scale datacenters, from their design and construction to their operation, also extends to its cloud hosting platform infrastructure.

ConnectWise® heavily utilizes AWS for the administration of all of its ConnectWise Automate cloud environments because it offers several resources that facilitate and streamline the management of a large number of virtual machines.

3.1.1 Platforms

ConnectWise Automate's cloud operates on multiple, resilient, high-availability, scaling platforms hosted within AWS. These platforms exist and span a number of different AWS Regions to provide increased performance for customers around the globe. At present, ConnectWise utilizes the core platforms hosted in the following regions:

REGION
US East
US West
Canada
EU
Asia Pacific
South America

Automate server instances are launched in datacenters located around the world. The region that is closest to the partner geographically is selected to help ensure that partners experience the best performance.

3.1.2 Availability Zones

There are multiple availability zones located in each region. A cloud instance is placed within the specific availability zone within the region. Distributing the instances to a specific zone helps ensure if a zone experiences issues, it would not impact all cloud instances within the region.

3.1.3 Instance Hosting

ConnectWise Automate utilizes Amazon EC2 (Elastic Compute Cloud) for its cloud hosting and management. This is a service that gives us the ability to quickly launch new virtual machines (instances) using premade images known as Amazon Machine Images and have these instances hosted in the cloud.

With datacenters strategically located to support domestic and international IT service

3.2 Monitoring & Management

ConnectWise provides monitoring and management services of ConnectWise Automate cloud servers when partners opt for the cloud offering, which is necessary for proper instance maintenance and support.

3.2.1 CloudWatch

Amazon CloudWatch is used to measure resource utilization, application performance, and operational health. When ConnectWise Cloud Administrators review metrics for cloud instances, they typically look at performance metrics such as CPU, Disk Usage, and RAM.

In addition to the instance monitoring services provided by AWS CloudWatch, core platform services are monitored for health and throughput via custom metrics pushed to CloudWatch.

3.2.2 ConnectWise Automate & Instance Updates

The ConnectWise Cloud Administration team performs updates to ConnectWise Automate cloud server instances on a regular basis to ensure that all environments have the latest Windows and ConnectWise Automate updates. These updates are automated to maintain consistency across all environments. Each cloud hosting region has a designated maintenance timeframe for Windows updates, run weekly during off-peak hours, if pertinent updates are available for a given server. As network and system vulnerabilities are discovered and made known to the ConnectWise Infrastructure team, appropriate fixes are devised, tested, and then installed on all affected systems to mitigate any future vulnerabilities.

3.2.3 Platform Status

Current platform health, status, and issues are proactively reported to end users on a comprehensive System Status page. In addition to alerting users to potential issues and notifying them of upcoming planned maintenance windows, it includes a Status History page *[see Show History link]* listing previous maintenance instances and issues in order to provide insights into platform stability and response times.

3.3 Hosting Security

ConnectWise is committed to maintaining the privacy and security of the ConnectWise Automate SaaS offering and partner's confidential information. For this SaaS offering, we have transitioned from on-premise servers to AWS for our data hosting needs due to Amazon's robust security standards.

Details: AWS Compliance Whitepapers

3.3.1 Security Groups

Amazon's Security Groups are used to restrict what ports to have open on the server, such as whether or not it is accessible via Remote Desktop Protocol (RDP) and under what circumstances.

The ConnectWise Cloud Administration team utilizes these security groups to block external inbound traffic to the Control Center so as to only permit access from within the ConnectWise internal network, as well as for allowing agent connections into the Automation Server.

Although the Cloud Administration team is responsible for maintaining the ConnectWise Automate cloud server instances, partners can still connect to and utilize their Control Center over HTTP (port 80) or HTTPS (port 443), but they cannot remotely connect to the cloud instance itself.

3.3.2 Agent Communication

Agent to Server Encryption	TLS 1.0, 1.1, 1.2
Protocol	HTTPS / TCP 443; 8040 [ConnectWise Control]

3.3.3 Remote Access

ConnectWise Automate cloud partners can access servers in a limited capacity remotely via a limited-permissions account supplied by ConnectWise Infrastructure. Access is granted to each company's designated Automate Administrator and gated behind a login, with email verification required for authentication.

Remote access allows partners to perform basic server-side tasks that are otherwise unavailable in the Control Center, such as retrieving file uploads from the LTShare directory. These remote access sessions are not recorded in order to help maintain privacy and compliance for partners.

3.3.4 Physical Security

AWS datacenters are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other means of security. Authorized staff must pass two-factor authentication at minimum twice in order to be granted access to datacenter floors. All visitors and contractors are required to present identification, are signed in, and continually escorted by authorized staff through the facility.

Details: AWS Cloud Security

3.4 Cloud Storage

AWS has multiple locations where data can potentially be stored and the following sections will outline the different areas.

3.4.1 Elastic Block Store (EBS)

The primary data storage volume for ConnectWise Automate cloud instances is Elastic Block Store (EBS). EBS is very flexible and can be attached to any instance running in the same availability zone.

EBS also allows us to gather performance metrics for the instances, such as bandwidth, throughput, latency, and average queue length using Amazon CloudWatch. This lets us monitor to ensure that cloud instances are performing effectively and can alert in advance if a particular instance requires attention.

3.4.2 Simple Storage Service (S3)

Amazon Simple Storage Service (S3) is a repository for internet data used for quick data retrieval whether inside of Amazon EC2, or outside on the Web. The ConnectWise Automate cloud offering uses S3 to accomplish the following:

- **AMI Storage**: Newly created AMIs are stored within Amazon S3. These images are easily accessible and continually used to launch new instances.
- **Backup Storage**: Backup of cloud partners' instances are performed on a regular basis and can be used to restore an instance in the event of a major issue, such as database corruption.

3.4.3 EC2 Types

If a partner's instance must not share resources with other instances in a public cloud environment due to regulatory data restrictions, a Cloud Dedicated Instance can be enabled for the instance to run on its own dedicated hardware.

4 Privacy & Data Protection

At ConnectWise®, we understand that partner information is sensitive and private, we recognize the importance of data protection and security, and we support current industry initiatives to preserve individual privacy rights. ConnectWise is committed to upholding ethical standards in its business practices and only collect the minimum necessary information required to troubleshoot and support the target Automation Server.

ConnectWise does not view, access, disclose, or use non-public personal information about partners or their customers other than to carry out the purpose for which the information was disclosed and as permitted by applicable laws.

Where personally identifiable information (PII) may reside, we take appropriate steps to protect it from unauthorized access or disclosure. We do not share personal or company information with third parties without consent (unless legally required to), nor is this information processed for reasons outside of what is necessary to meet contractual obligations and deliver the support and service expected based on the agreed upon business relationship.

Cloud Hosting

Amazon Web Services has gained approval from the EU Data Protection Authorities with regard to its cross-border data transfer arrangement.

Details: EU Data Protection