WatchGuard

Endpoint Security Plug-in for ConnectWise Automate

About This Guide

The *Endpoint Security Plug-in for ConnectWise Automate Guide* helps you set up and use the WatchGuard Endpoint Security Plug-in with ConnectWise Automate.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 5/11/2021

Copyright, Trademark, and Patent Information

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online at https://www.watchguard.com/wgrd-help/documentation/overview.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter, @WatchGuard on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

Contents

About the WatchGuard Endpoint Security Plug-in for ConnectWise Automate

WatchGuard endpoint security products enable you to:

- Protect computers and devices on your network.
- Review detected security incidents that occur on your devices.
- Develop prevention and response plans against unknown and advanced persistent threats.

WatchGuard endpoint security products manage communication with deployed endpoint security agents, provide a management console for administration and configuration, and process the data collected by the endpoint security agents for analysis.

Supported Products

The WatchGuard Endpoint Security plug-in supports these products:

- WatchGuard Endpoint Security
  - Endpoint Protection, Detection and Response (EPDR)
  - Endpoint Detection and Response (EDR)
  - Endpoint Protection Platform (EPP)
- Panda Aether platform:
  - Adaptive Defense and Adaptive Defense 360
  - Endpoint Protection and Endpoint Protection Plus

ConnectWise Automate Integration

You can use the WatchGuard Endpoint Security plug-in to integrate WatchGuard endpoint security products with ConnectWise Automate to monitor and manage security on the devices in your client accounts.

Manage Accounts and Devices

To manage device security in your client accounts, you can use the WatchGuard Endpoint Security plug-in to:

- Synchronize account and device data between ConnectWise Automate and WatchGuard.
- View WatchGuard endpoint security product license information for each device.
- Show devices that do not have endpoint protection installed.
- Install WatchGuard endpoint security products on a device.

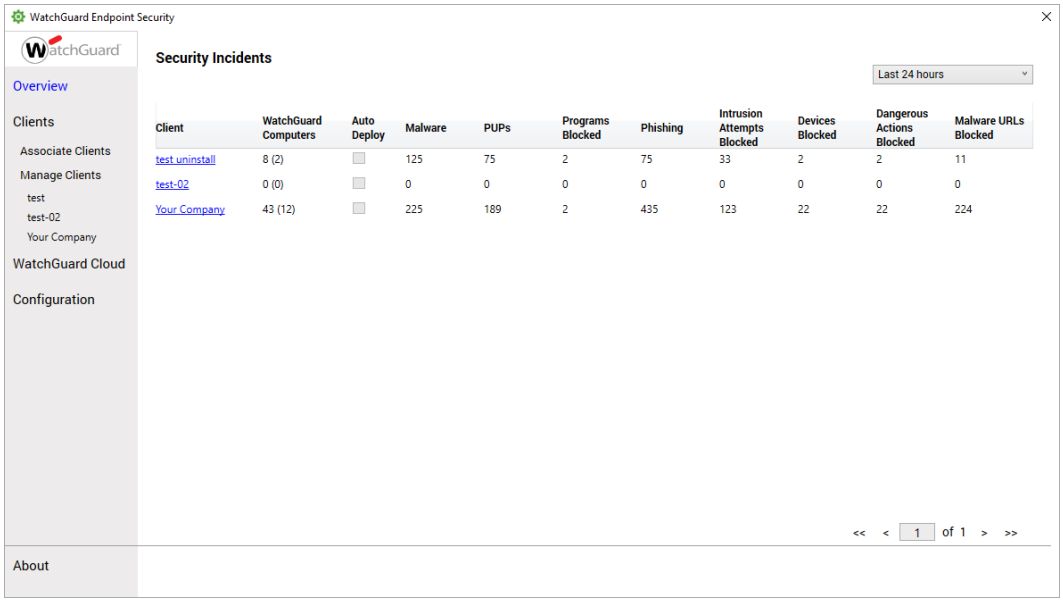
View Security Status

You can view the security status of managed devices and perform these immediate actions, if required:

- List the threats detected on your devices over a specified time period
- View the WatchGuard endpoint security status of each device
- View all security configurations available for the device
- Assign a security configuration to a device
- Perform immediate security scans of devices
- Isolate devices or stop device isolation

Plug-in Interface Overview

The WatchGuard Endpoint Security plug-in contains these sections:



Overview

The *Overview* page provides a dashboard that shows the number of computers and devices in a client account that have WatchGuard endpoint security products installed, the number (in brackets) of devices registered in ConnectWise, and any detected security incidents on these devices.
For more information, see *Security Incidents Overview*.

Clients

The *Clients* section enables you to manage the computers and devices for the selected client account, and includes these pages:

- Associate Clients – A list of clients where you can associate ConnectWise Automate and WatchGuard Cloud accounts.
  For more information, see *Associate ConnectWise Automate and WatchGuard Cloud Accounts*.
- Manage Clients – A dashboard that shows statistics for all the devices in the account. You can also perform actions on client computers and devices, such as start a file scan, isolate a computer, or apply a security configuration.
  For more information, see *Manage Clients*.

WatchGuard Cloud

The *WatchGuard Cloud* page opens the WatchGuard Cloud login page at cloud.watchguard.com so you can manage your WatchGuard Cloud account while you use the plug-in. You must log in with your credentials if you are not already authenticated to WatchGuard Cloud.

Configuration

The *Configuration* page enables you to configure the plug-in with your API access information for WatchGuard Cloud. You must have the authentication and API URLs, access ID and password, and API key provided to you when you enabled API access in WatchGuard Cloud. For more information, see *Configure the WatchGuard Endpoint Security Plug-in*.

When you open the plug-in, if the configuration is not set, the Configuration page opens. If the configuration is set, the Overview page opens.

About

The *About* page shows information about the plug-in version, build date and time, links to the WatchGuard Endpoint Security documentation page, and a link to the WatchGuard web site.

Install the WatchGuard Endpoint Security Plug-in

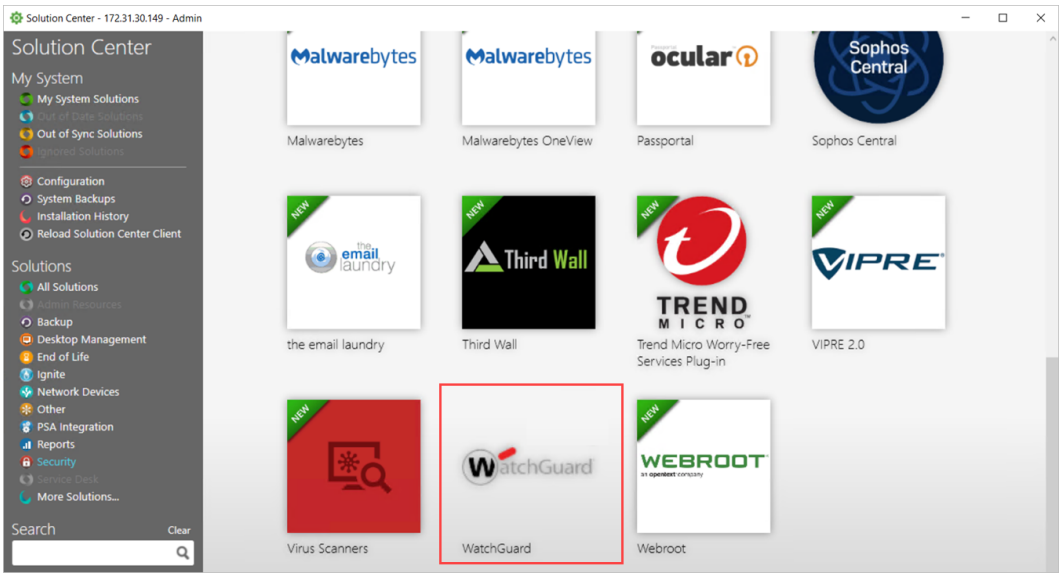
You can install the WatchGuard Endpoint Security plug-in from the ConnectWise Automate Solution Center.

> The WatchGuard Endpoint Security plug-in is supported on ConnectWise Automate server version 2020 and higher.

Get the Plug-in

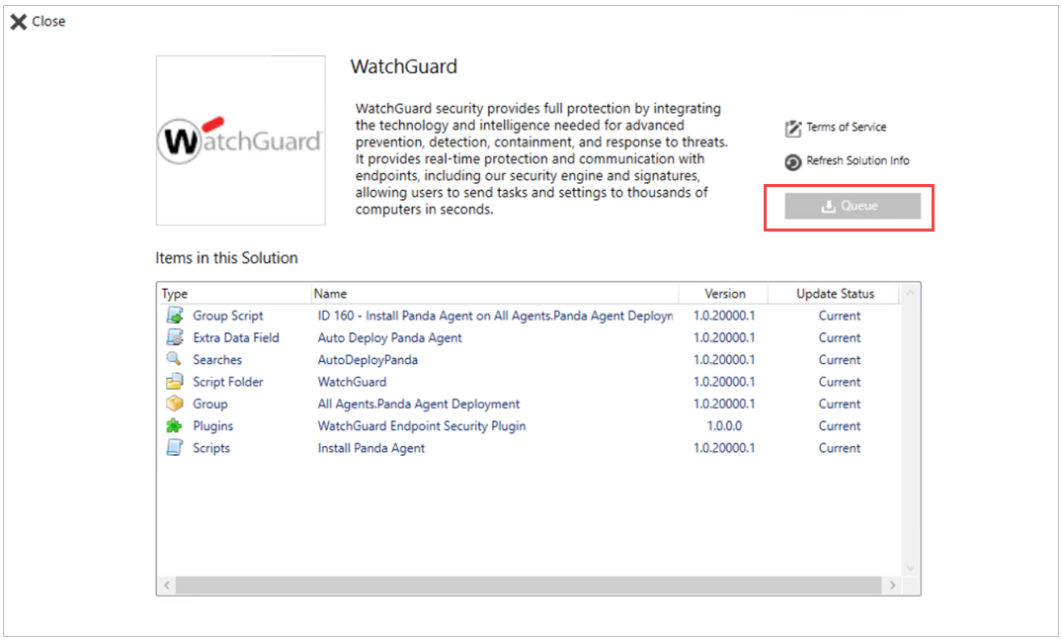
To get the plug-in from the ConnectWise Automate Solution Center:

1. Open ConnectWise Automate Control Center.
2. Select **System**.
3. Select **Automate Solutions Center**.
4. Select **Security**.
5. Select **WatchGuard Endpoint Security**.



6. Click **Queue** to queue the installation of the WatchGuard plug-in in the ConnectWise Automate Control Center.

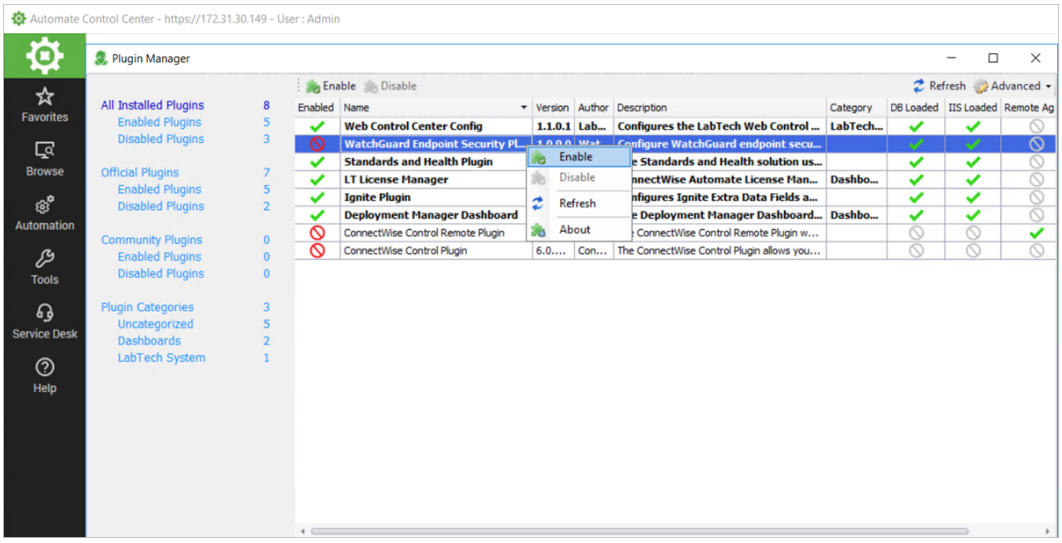
   The plug-in installation process also includes the necessary scripts and software that enable you to install WatchGuard endpoint security products on your devices.



Enable the Plug-in

To enable the plug-in in ConnectWise Automate Control Center:

1. Open ConnectWise Automate Control Center.
2. Select **System > Solutions > Plugin Manager**.
3. Select or right-click the **WatchGuard Endpoint Security** plug-in, then click **Enable**.

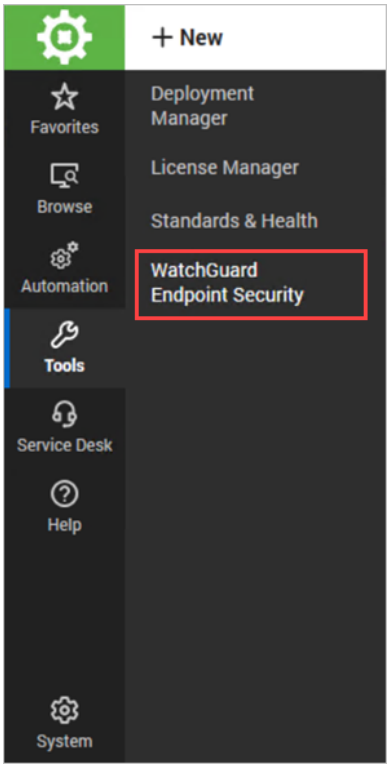


Open the Plug-in

After you install and enable the plug-in, you can open it.

To open the WatchGuard Endpoint Security plug-in:

1. Open ConnectWise Automate Control Center.
2. Select **Tools**.
3. Select **WatchGuard Endpoint Security**.



If this is the first time you open the plug-in, the Plug-in Configuration page opens. Use the Plug-in Configuration page to configure the plug-in with your WatchGuard Cloud API account details. For more information, see *Configure the WatchGuard Endpoint Security Plug-in*.

If you previously configured the plug-in, the plug-in synchronizes its database with WatchGuard Cloud to make sure the database has the most recent list of WatchGuard Cloud managed accounts and devices and their WatchGuard endpoint security product license status. When the synchronization process completes, the Security Overview page opens. For more information, see *Security Incidents Overview*.

This client synchronization process might take some time to compete, based on how many accounts you added or removed since the last synchronization with WatchGuard Cloud.

Configure the WatchGuard Endpoint Security Plug-in

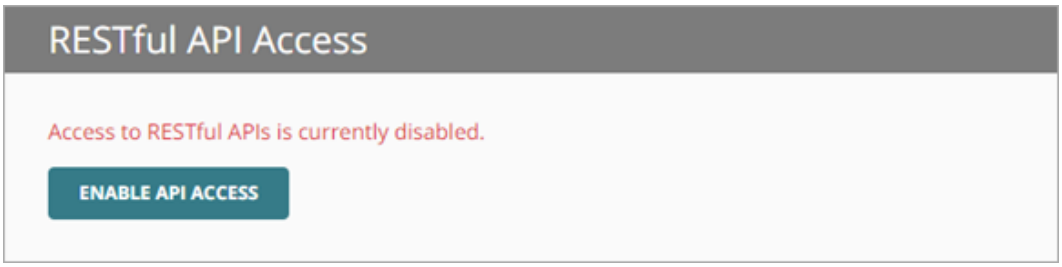
You must configure the plug-in to access the Endpoint Security Management API in WatchGuard Cloud. This enables you to connect with WatchGuard Cloud and download your managed account data. You can then associate your WatchGuard Cloud managed accounts with your existing ConnectWise Automate client accounts.

Enable API Access in WatchGuard Cloud

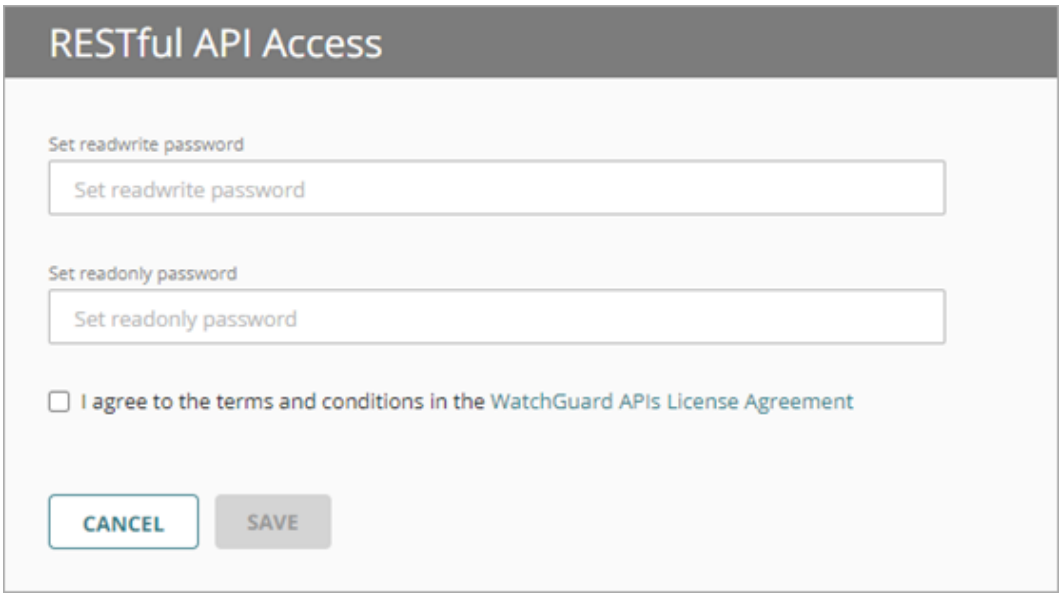
WatchGuard public APIs use the Open Authorization (OAuth) 2.0 authorization framework for token-based authentication. To use the Endpoint Security Management API, you must first enable API access in your WatchGuard Cloud account to retrieve the required parameters for your plug-in configuration. For more information, see Enable API Access in WatchGuard Cloud.

To enable API access in Watchguard Cloud:

1. Log in to WatchGuard Cloud.
   *If you are a Service Provider, from **Account Manager**, select **My Account** or a managed account.*
2. Select **Administration > Managed Access**.
3. Click **Enable API Access**.



4. Specify the **readwrite** and **readonly** passwords to use as your API access credentials.

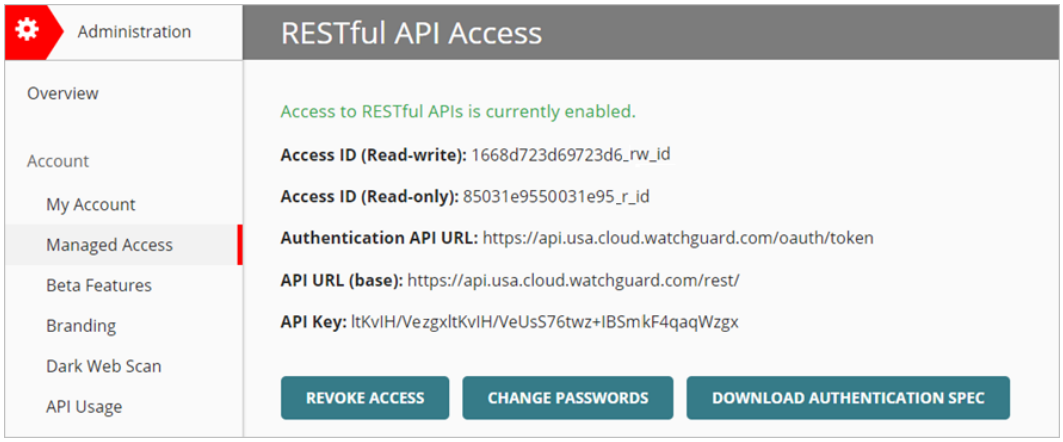


Passwords must include an uppercase letter, a lowercase letter, a number, and a special character. The **Read-write** password and the **Read-only** password must be different.

You must use the **Read-write** Access ID and password for the plug-in configuration.

5. Select the **I agree to the terms and conditions in the WatchGuard APIs License Agreement** check box.
6. Click **Save**.

After you enable API access, these parameters appear that you must specify in your plug-in configuration. You can see these parameters on the **Administration > Managed Access** page in WatchGuard Cloud.

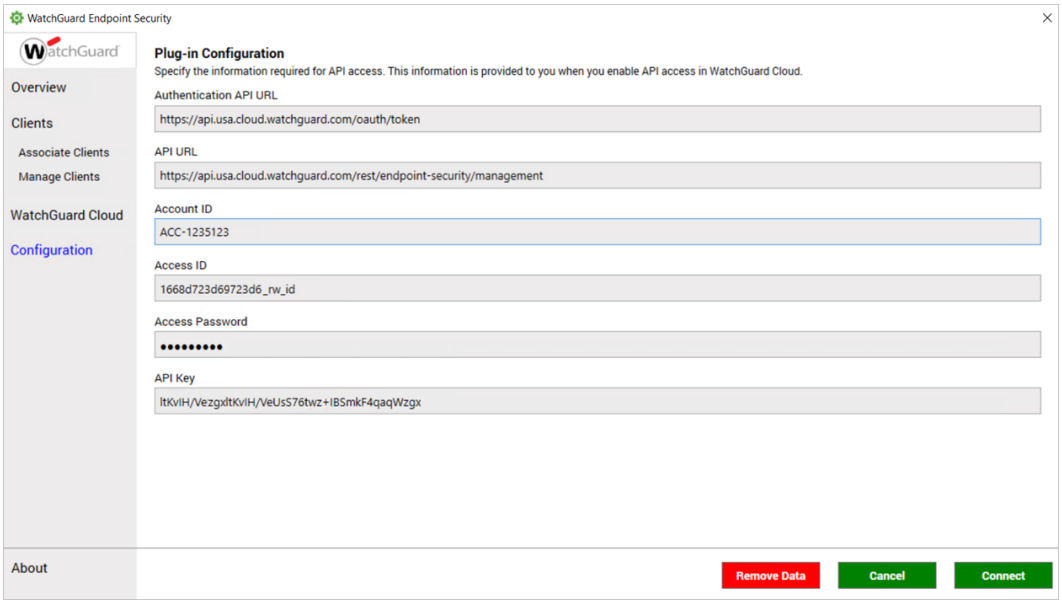


The base URL varies by region. This example shows a US-based server.

Configure the Plug-in

To configure the WatchGuard Endpoint Security plug-in:

1. Select **Configuration**.



2. Configure these parameters:
   - **Authentication API URL** –Type the URL to authenticate API access to WatchGuard Cloud. The base URL varies by region. For example, the US region uses this server:
     `https://api.usa.cloud.watchguard.com/oath/token`
   - **API URL** – Type the URL for API access to WatchGuard Cloud.
     The base URL varies by region. This example uses US-based servers.

     For WatchGuard Endpoint Security product customers, use this URL:
     `https://api.usa.cloud.watchguard.com/rest/endpoint-security/management`
     For Panda Aether platform customers, use this URL:
     `https://api.usa.cloud.watchguard.com/rest/aether-endpoint-security/aether-mgmt`
   - **Account ID** – Type the WatchGuard Cloud Account ID of the managed account for which you want to make API requests. This must be the Account ID of a service provider or subscriber account that you manage in WatchGuard Cloud. To view your account ID, select **Administration > My Account** in WatchGuard Cloud.
   - **Access ID** – Type the Access ID for **Read-write** API access to WatchGuard Cloud.
   - **Access Password** – Type the password for the **Read-write** Access ID you specified for API access to

WatchGuard Cloud.

Make sure you specify the **Read-write** Access ID and password for API access. The **Read-only** Access ID might cause errors when you use the plug-in.

- **API Key** – Type the API key associated with your WatchGuard Cloud account.

Test the Connection

To test the connection for WatchGuard Cloud API access, click **Connect**.

If the connection is successful, the plug-in saves the configuration and enables you to continue to the client association process. For more information, see *Associate ConnectWise Automate and WatchGuard Cloud Accounts*.

If you configure the plug-in with a WatchGuard Cloud service provider account, the plug-in also retrieves all managed accounts of the partner account. This process might take several seconds to retrieve data about the accounts from WatchGuard Cloud.

If the connection is not successful:

- Make sure the Access ID for API access is enabled in WatchGuard Cloud.
- Make sure the Access ID and password are for the correct WatchGuard Cloud Account ID.
- Verify the API Key.
- Make sure the Account ID is correct.
- Check if the WatchGuard Cloud Account ID was removed or merged with another account.

Remove Plug-in Data

You can remove all data from the plug-in, including all client account data and your WatchGuard Cloud API access information. We recommend you remove all data before you remove the plug-in. For more information, see *Remove the WatchGuard Endpoint Security Plug-in*.

To remove all data from the plug-in:

1. Click **Remove Data**.
   A confirmation message appears
2. To confirm that you want to remove all plug-in data, click **Yes**.
3. Close and restart the ConnectWise Automate Control Center if you want to restart and reconfigure the plug-in.

Associate ConnectWise Automate and WatchGuard Cloud Accounts

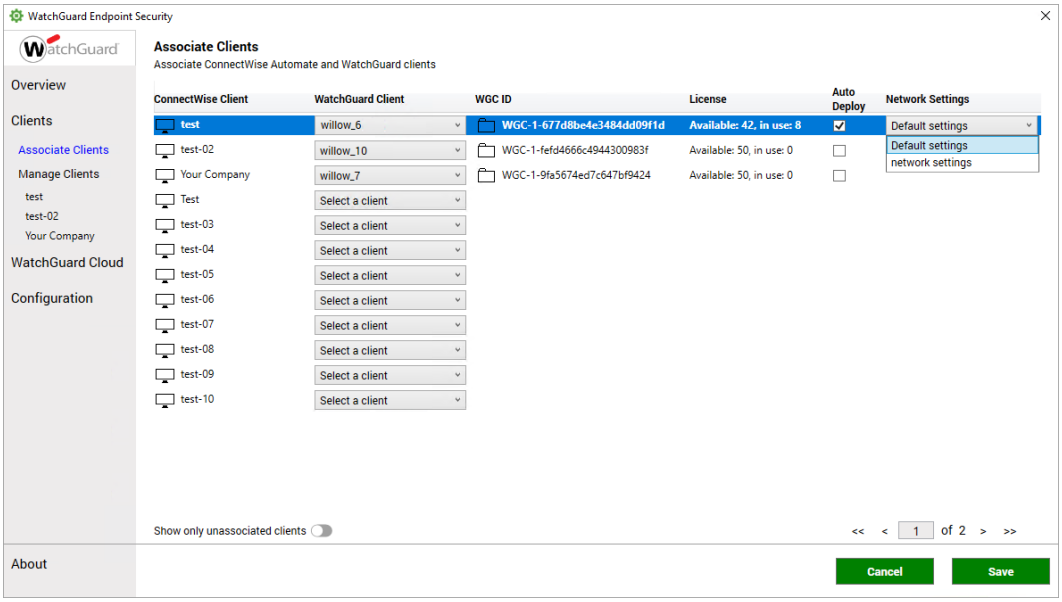
After you configure the WatchGuard Endpoint Security plug-in and test the connection for WatchGuard Cloud API access to your WatchGuard Cloud account, you must associate your accounts between ConnectWise Automate and WatchGuard Cloud. If you have not yet configured the plug-in, see *Configure the WatchGuard Endpoint Security Plug-in*.

The first time you open the Associate Clients page, the client list shows the clients that you manage in ConnectWise Automate, and a list of all WatchGuard Cloud accounts you manage that have an endpoint protection product license.

This enables you to map a WatchGuard Cloud managed account to the corresponding client account in ConnectWise Automate.

To associate ConnectWise Automate and WatchGuard Cloud accounts:

1. Select **Clients > Associate Clients**.
   The Associate Clients page opens.



2. Select a ConnectWise Automate client account that you want to associate with a WatchGuard Cloud account.

   To filter the list to only show clients that are not currently associated, enable **Show only unassociated clients**.

3. From the **WatchGuard Client** drop-down list, select the WatchGuard Cloud managed account to associate with the selected ConnectWise Automate client account.
   - The **WGC ID** column shows the WatchGuard Cloud account ID of the selected account.
   - The **License** column shows the endpoint security product license information for the selected WatchGuard account.

To remove an association, from the drop-down list, choose **Select a client**.

4. To automatically install WatchGuard endpoint security products on all computers in the client account after you associate the accounts, select the **Auto Deploy** check box.

The device must already have the ConnectWise Automate agent installed to process and schedule the installation of the WatchGuard agent. The ConnectWise Automate process that schedules installation tasks runs every 12 hours. It might take up to 12 hours to install the WatchGuard agent on client computers.

5. From the **Network Settings** drop-down list, select a network configuration to apply to a device when you install WatchGuard endpoint security products.

   These network settings contain the necessary network information such as proxies, cache, and discovery services required to install WatchGuard endpoint security products, and are managed in your WatchGuard endpoint security product configuration.

6. When you complete your client associations, click **Save**.

When the association process is complete, you can monitor and manage your clients. For more information, see *Manage Clients*.

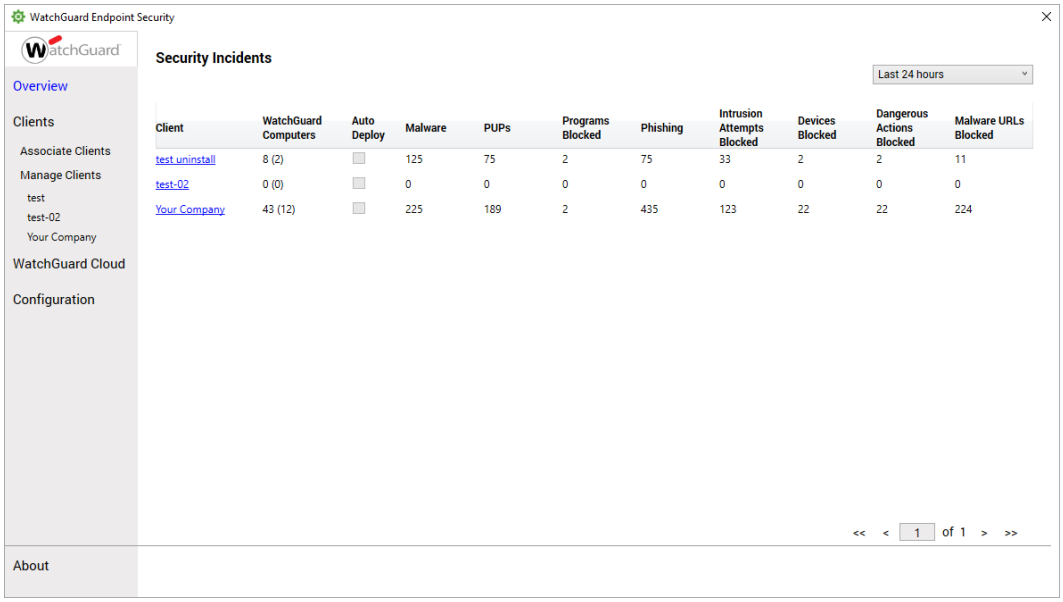
Security Incidents Overview

The Security Incidents Overview page provides a dashboard of all your client accounts. The dashboard indicates the number of computers and devices (including Windows, Mac, Android, and Linux devices) in the client account, and indicates any specific security incidents on devices that have WatchGuard endpoint security products installed.

Select a specific client account to view statistics and manage the devices in the account.

You can filter the data based on these time periods:

- Last 24 hours
- Last 7 days
- Last month



The Security Incidents overview page shows these columns:

- Client – Shows the name of the client account. You can click the client name to see more detailed information about the client and the devices in the account. For more information, see *Manage Clients*.
- WatchGuard Computers – Indicates the number of computers and devices in the client account.
  - The first number indicates the number of computers and devices in the client account that have WatchGuard endpoint security products installed.
  - The second number in brackets indicates the total number of computers and devices that are registered in ConnectWise. This includes both devices with WatchGuard endpoint security products installed and devices that do not have endpoint security installed.

The number of devices reported by ConnectWise and WatchGuard might differ because of their different discovery processes.

- Auto Deploy – Indicates if the client account is configured to automatically deploy WatchGuard endpoint security products on computers in the account. You can configure this option on the **Associate Clients** page. For more information see *Associate ConnectWise Automate and WatchGuard Cloud Accounts*.
- Malware – Indicates the number of incidents of malware on devices in the client account. Malware is software intended to damage the contents of a computer or allow unauthorized access.
- PUPs – Indicates the number of incidents of potentially unwanted programs (PUPs) on devices in the client account. PUPs can include unwanted programs installed by the end user or tools used by hackers to gain access to target computers.
- Programs Blocked – Indicates the number of incidents of blocked programs on devices in the client account.
- Phishing – Indicates the number of phishing incidents on devices in the client account. Phishing is a technique to obtain confidential information, such as user names and passwords or financial information from end users.
- Intrusion attempts blocked – Indicates the number of intrusion attempts that were blocked on devices in the client account.
- Devices blocked – Indicates the number of devices that were blocked in the client account. A device is blocked after an end user tries to use a restricted device.
- Dangerous actions blocked – Indicates the number of dangerous actions that were blocked on devices in the client account. Dangerous actions are end user actions identified as dangerous based on local behavioral analysis.
- Malware URLs blocked – Indicates the number of malware URLs that were blocked on devices in the client account. Malware URLs are web addresses of pages that contain malware.

Manage Clients

On the Manage Clients page, you can manage device security for all your client accounts.

You can perform these actions:

- View a list of security incidents for each client account
- View WatchGuard endpoint security product license information
- Show devices that do not have WatchGuard endpoint security products installed
- Install WatchGuard endpoint security products on a device
- Perform actions such as assign security configurations, perform file scans, and isolate devices

Before you Begin

Before you can manage your clients, you must configure the WatchGuard Endpoint Security plug-in and associate your ConnectWise Automate client accounts and WatchGuard Cloud managed accounts.

- If you have not yet configured the plug-in, see *Configure the WatchGuard Endpoint Security Plug-in*.
- To associate your ConnectWise Automate and WatchGuard Cloud accounts, see *Associate ConnectWise Automate and WatchGuard Cloud Accounts*.

Manage Clients

To manage your clients, select **Clients > Manage Clients**.

The Manage Clients page initially shows the data and statistics for the first client account in your client list. Click on a specific client to see data for that account.

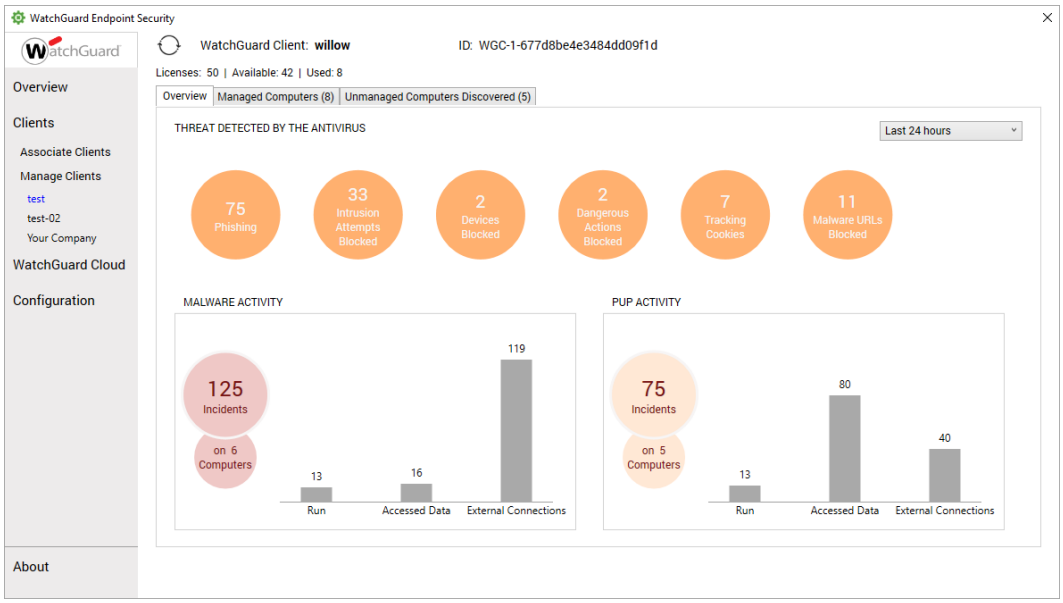
The current WatchGuard Cloud account name and account ID appear at the top of the page.

The licenses section shows the total number of WatchGuard endpoint security product licenses, the number of licenses available, and the number of licenses in use.

Click ↻ to refresh the data shown on the page.

You can filter the data based on these time periods:

- Last 24 hours
- Last 7 days
- Last month



Overview

The **Overview** tab shows statistics for all computers and devices in the selected client account.

Threats Detected By The Antivirus

This section shows the number of security incidents detected for each threat category:

- Phishing – A technique to obtain confidential information, such as user names and passwords or financial information from end users.
- Intrusion attempts blocked – Malformed network traffic designed to cause unwanted system behavior on the targeted computer.
- Devices blocked – An attempt by a user to use a restricted device.
- Dangerous actions blocked – End user actions identified as dangerous based on local behavioral analysis.
- Tracking cookies – Cookies used to track web activity by a user.
- Malware URLs blocked – Web addresses of pages that contain malware.

Malware Activity

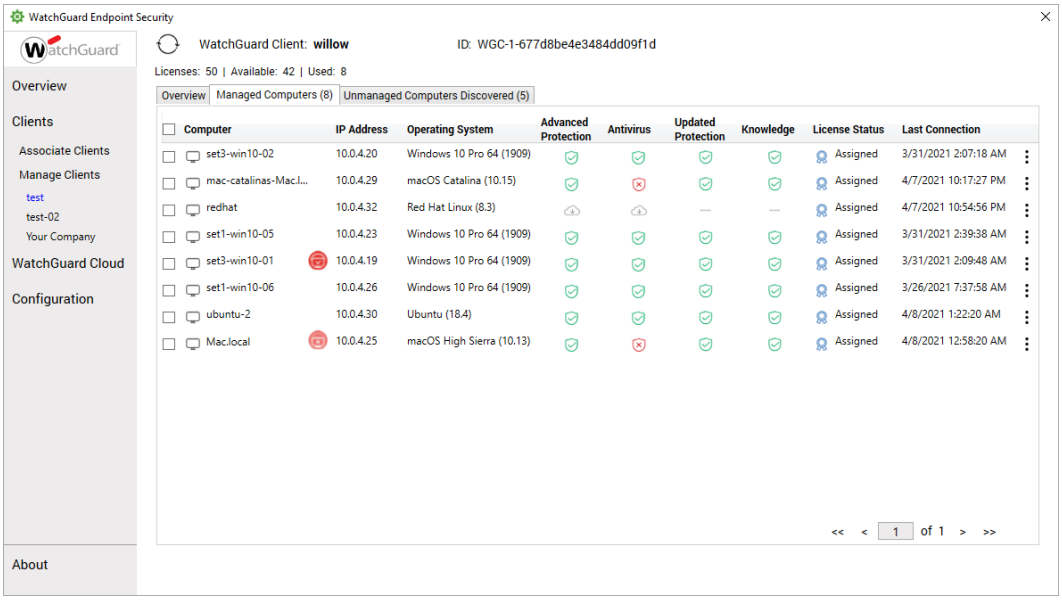
Indicates the number of malware incidents, the number of computers on which they occurred, the number of malware programs run, the number of incidents where data was accessed, and the number of incidents that involved external communications.

PUP Activity

Indicates the number of PUP (Potentially Unwanted Program) incidents, the number of computers on which they occurred, the number of programs run, the number of incidents where data was accessed, and the number of incidents that involved external communications.

Managed Computers

The **Managed Computers** tab shows all devices in the selected client account that have WatchGuard endpoint security products installed.



The **Manage Computers** tab shows this data:

- Computer – The name of the device.
- IP Address – The IP address of the device.
- Operating System – The detected operating system of the device.
- Advanced Protection – The status of Advanced Protection on the device.
  - Enabled
  - Disabled
- Antivirus – The status of Antivirus protection on the device.
  - Installing
  - Error
  - Enabled
  - Disabled
  - No License
- Updated Protection – Indicates the status of the Protection Module and if the device requires an updated release.
  - Updated
  - Not updated (7 days since the last update)
  - Pending restart

- Knowledge –The status of Knowledge signature files on the device.
  - Updated
  - Not Updated (3 days since the last update).
- License Status – Indicates the status of the WatchGuard endpoint security product license.
  - Assigned
  - No License
  - Excluded
- Last Connection – Indicates the date and time the device was last connected to the network.

You can select one or more devices and perform these actions.

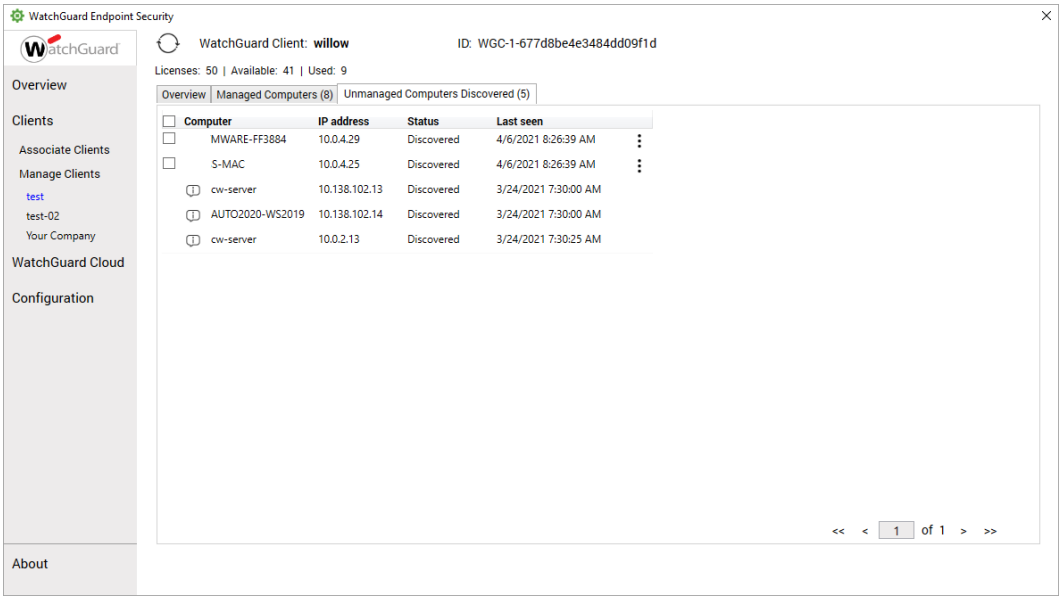
Click ⋮ for the computer on which you want to perform the action, then select the required action. If you select more than one device, the action applies to all selected devices.

- **Assign Security Configurations** – A security configuration is a set of WatchGuard endpoint security settings that you define and assign to your managed devices. Select a security configuration from the list, then click **Apply**.
- **Uninstall WatchGuard Endpoint Protection** – Uninstall WatchGuard endpoint security products from the computer.
- **Scan Computer** – Perform a file scan on the selected managed devices. To perform a file scan, the device must be connected to the network. If the device is not connected to the network, the request remains active for 7 days (by default). The scan runs when the device connects to the network.
- **Isolate Computer** – Isolate a device (Windows computers only). To isolate a device, the device must be connected to the network to receive the request. The request remains active indefinitely for unconnected devices. The isolate request is performed when the device connects to the network. A icon appears when the device is isolated. The isolation icon flashes while the request to isolate the device is active.
- **Stop Isolating Computer** – Stop isolation for a device (Windows computers only). To stop device isolation, the device must be connected to the network to receive the request. The request remains active indefinitely for unconnected devices. The request to stop isolation is performed when the device connects to the network. The isolation icon flashes while the request to stop isolation is active.

Unmanaged Discovered Computers

The **Unmanaged Computers Discovered** tab shows all detected devices in the client account that do not have WatchGuard endpoint security products installed. To manage and perform actions on unmanaged devices, you must install WatchGuard endpoint security products on the device.

To install WatchGuard endpoint security products from the plug-in, the device must already have the ConnectWise Automate agent installed to process and schedule the WatchGuard agent installation.

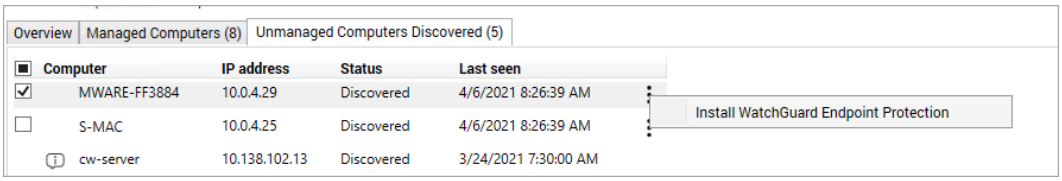


The **Unmanaged Computers Discovered** tab shows this information:

- Computer – The name of the device.
- IP Address – The IP address of the device.
- Status – The current installation status of WatchGuard endpoint security products on the device.
  - Unmanaged
  - Installing
  - Installation Error
- Last Seen – Indicates the date and time the device was last connected to the network.

The only action you can take for unmanaged computers is to install WatchGuard endpoint security products on the device.

Click ⋮ for the device on which you want to install WatchGuard endpoint security products, then select **Install WatchGuard Endpoint Protection**. If you select multiple devices, the WatchGuard agent installs on all selected devices.

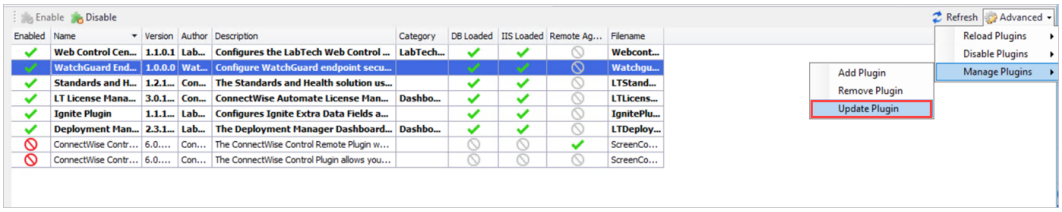


The installation process for the device is scheduled after approximately two minutes.

Update the WatchGuard Endpoint Security Plug-in

To update the WatchGuard Endpoint Security plug-in and install the latest version from ConnectWise Automate:

1. Open the ConnectWise Automate Control Center.
2. Select **System > Solutions > Plugin Manager**.
3. Select the WatchGuard Endpoint Security plug-in.
4. From the **Advanced** drop-down list, select **Manage Plugins > Update Plugin**.



5. From the list of files, select the `WatchguardPlugin.dll` file for the update version you want to install.
6. Click **Open** to update the plug-in.
   A message appears when the update completes.
7. Click **OK**.
8. Close and restart the ConnectWise Automate Control Center to update the plug-in.

Remove the WatchGuard Endpoint Security Plug-in

You can remove the WatchGuard Endpoint Security plug-in from ConnectWise Automate.

To remove the plug-in, you must perform these steps:

- Remove plug-in data
- Disable the plug-in in ConnectWise Automate
- Remove the plug-in from ConnectWise Automate

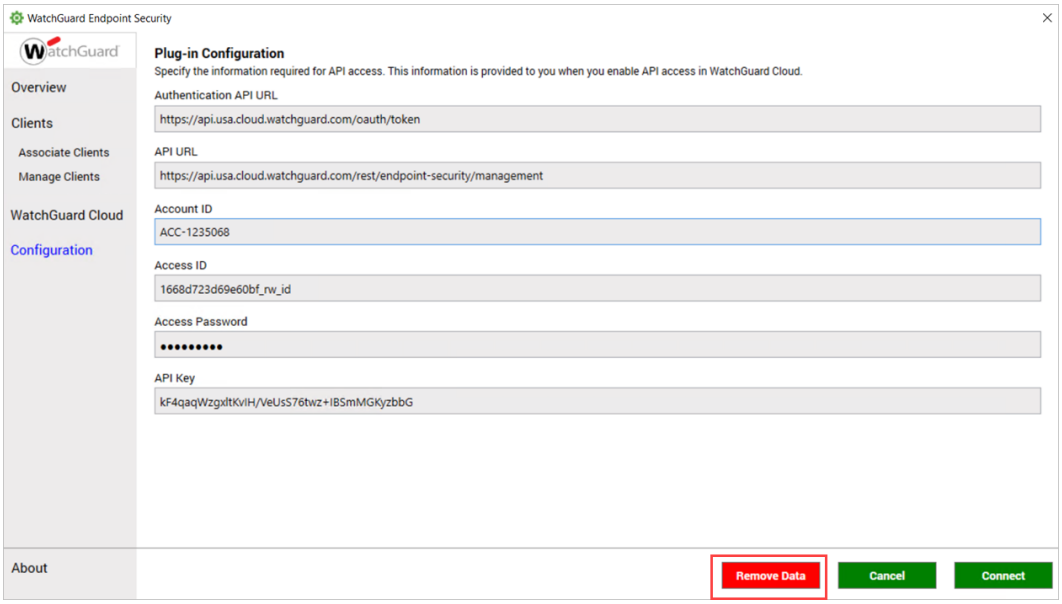
Remove Plug-in Data

We recommend you first remove all data from the plug-in before you uninstall the plug-in from ConnectWise Automate. This removes all client account and configuration information, such as:

- Connection information for WatchGuard Cloud API access on the Configuration page
- WatchGuard account list
- WatchGuard account mappings with ConnectWise Automate clients
- WatchGuard endpoint security product license and security configuration information

To remote all data from the plug-in:

1. Open the WatchGuard Endpoint Security plug-in.
2. Select **Configuration**.
   The Plug-in Configuration page appears.

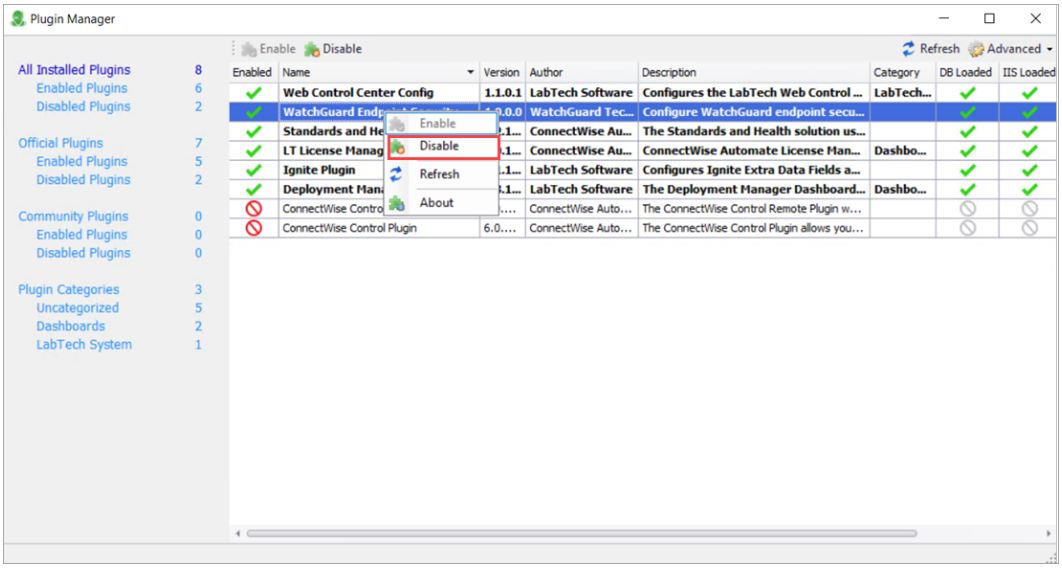


3. Click **Remove Data**.
   A message appears to confirm if you want to remove all stored plug-in data. This action cannot be undone.
4. Click **Yes**.

Disable the Plug-in

To disable the WatchGuard Endpoint Security plug-in in ConnectWise Automate:

1. Open the ConnectWise Automate Control Center.
2. Select **System > Solutions > Plugin Manager**.
3. Select or right-click the WatchGuard Endpoint Security plug-in, then click **Disable**.



Remove the Plug-in from ConnectWise Automate

If you want to remove the WatchGuard Endpoint Security plug-in from ConnectWise Automate:

1. Open the ConnectWise Automate Control Center.
2. Select **System > Solutions > Plugin Manager**.
3. Select the WatchGuard Endpoint Security plug-in.
4. From the **Advanced** drop-down list, select **Manage Plugins > Remove Plugin**.