



# Integration for ConnectWise Automate User Guide

**For ConnectWise Automate Version 2019 & above**

**Plugin Version 3.2.1.244 and above**

Doc Version 3.2.5



## Table of Contents

What's new with version 3.2.1.244 .....	4
Previous Versions .....	4
What's new with version 3.2.1.242 .....	4
What's new with version 3.2.0.236 .....	4
How to use this manual .....	5
Help & ? .....	5
SECTION 1 - Installation instructions for new users .....	6
Step 1 – Obtaining the plugin .....	6
Step 2 – Plugin settings .....	7
Step 3 – Assigning Clients to existing Webroot Sites .....	11
Step 4 – Creating new Webroot sites .....	13
Step 5 – Activating Auto Deploy .....	14
Step 6 – Plugin reference & walkthrough .....	14
SECTION 2 - Upgrade instructions from legacy plugins .....	15
Step 1 – Upgrading from plugin version 2.5 or older .....	15
Step 2 – Obtaining the plugin .....	15
Step 3 – What happens after an upgrade from plugin version 2.5 .....	16
Step 4 – Plugin settings .....	17
Step 5 – Assigning Clients to existing Webroot Sites .....	21
Step 6 – Creating new Webroot sites .....	22
Step 7 – Activating auto deploy .....	23
Step 8 – Plugin walkthrough .....	23
SECTION 3 - Plugin Reference & Walkthrough .....	24
Dashboard .....	24
Overview tab .....	24
Clients .....	25
Computers in Webroot Clients .....	25
Threats Detected (last 7 days) .....	25
Webroot Agent Distribution .....	25
Clients tab .....	26
Webroot Site .....	26
Webroot site > Assign an Existing Webroot Site to a Client .....	27
Webroot Site > Creating a New Webroot Site and assigning it to a Client .....	28
Webroot Site > Use a non-GSM manually entered site key .....	29
Webroot group – Auto Deploy to Group Policy .....	31

---

Auto Deploy .....	33
Automate scans .....	34
Computers tab .....	35
Send Agent Command .....	35
Webroot Policy .....	36
Auto Deploy .....	37
Automate scans .....	38
Locations .....	39
Auto Deploy .....	39
GSM Portal .....	40
Settings .....	41
API Authentication .....	41
Webroot Agent .....	41
Alerts and Pop-ups .....	41
Help .....	43
Computer Plugin Page .....	44
System .....	45
Threat History .....	46
Monitors .....	47
CW Automate Group .....	48
Scripts .....	48
Database Tables .....	49
Adding/Updating Plugin via Plugin Manager .....	50
Known issues .....	53

## What's new with version 3.2.1.244

This maintenance release resolves an issue with MySQL 8.0

## Previous Versions

### What's new with version 3.2.1.242

This interim maintenance release is designed to improve the underlying MySQL DB access speed and addresses some bugs where Computers Page may not load correctly. For a summary of features and enhancements see list below.

#### Enhancements

- Computers page: Change related SQL view to work more efficiently with MySQL 5.7
- Computer plugin tile: Change so the Automate Computer management screen loads quicker

#### Bug fixes

- Computers page: Not displaying any computers data in the grid
- When the data reconciliation is happening, it is causing SQL Deadlock errors

### What's new with version 3.2.0.236

This important feature release allows our largest customers to use the plugin in a much more efficient manner and adds other important security and usability enhancements. For a summary of features and enhancements see list below. For more details, see [SECTION 3 - Plugin Reference & Walkthrough](#).

#### New Features

- Global Client filter to enable vastly faster access to plugin pages by larger customers
- Added Location as a new column within the Computers page to help usability
- Added Active Threats value to Computers page
- Added the ability to turn on ARPNOREMOVE via plugin global settings for additional security

#### Enhancements

- Removed Client & Location tabs and -Clone Unique Identifier option to reduce legacy technical debt
- Fixed SQL injection vulnerability as well small bugs
- Changed the API endpoints used with the computer data synch process to be more efficient
- Restricted Threat History to 3 months to reduce strain on DBs with large numbers of detections

## How to use this manual


This manual is in three main sections.

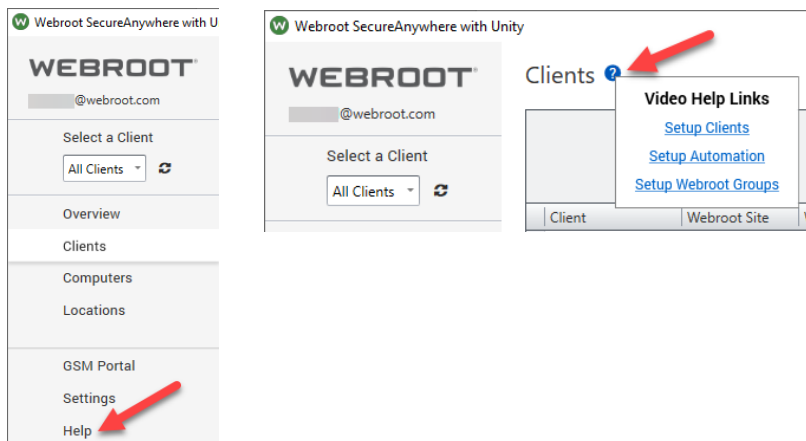
**Section 1 - New Webroot users** start here. If you are new to Webroot or have not used a Webroot plugin before please follow the step by step [Installation instructions for new Webroot users](#) below. This manual assumes you have already purchased Webroot and have signed into the Webroot console. If you have not purchased Webroot, please contact your ConnectWise representative.

**Section 2** - users **upgrading from legacy Webroot plugins, prior to version 3.x** start here. Please allow yourself enough time for the upgrade and actions afterwards. Read and follow the step by step [Upgrade instructions](#) before commencing. If you are upgrading from Version 3.x go to Section 3.

**Section 3 - Plugin Reference & Walkthrough.** We recommend you start in the most appropriate section first and then read through Section 3 – [Plugin Reference & Walkthrough](#)

## Help & ?

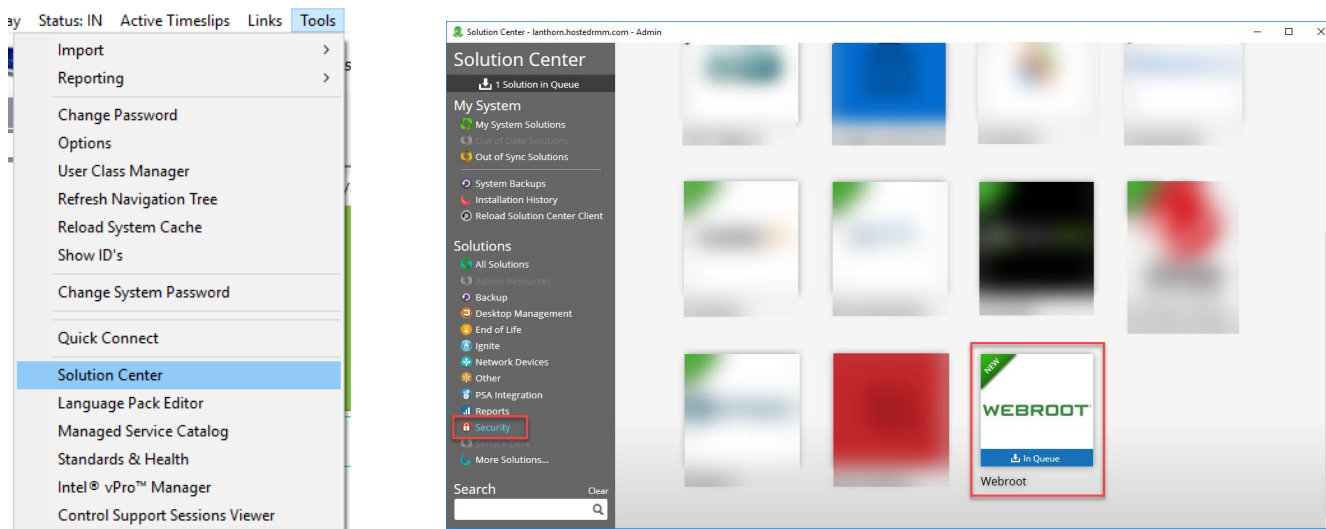
Please make use of the **Help** tab located on the bottom left of the plugin and the video tutorials  found within the **Client**, **Computers** and **Locations** tabs throughout the plugin.



## SECTION 1 - Installation instructions for new users

### Step 1 – Obtaining the plugin

If you are new to Webroot the latest Webroot plugin can be installed from CW Solution Center. Please select Security and Webroot and follow the standard Solution Center installation instructions.



**Note:** Please navigate to the **Plugin Manager** within the Control Center and **Enable** “Webroot SecureAnywhere with Unity” and “Webroot SecureAnywhere with Unity RA” and restart your Control Center, before proceeding to next step.

✓	Webroot SecureAnywhere with Unity	3.0.1622.8	Webroot Inc.	Webroot SecureAnywhere with Unity	✓	✓	✗	webroot.dll
✓	Webroot SecureAnywhere with Unity RA	3.0.1622.8	Webroot Inc.	Webroot SecureAnywhere with Unity RA	✓	✓	✓	WebrootRA.dll

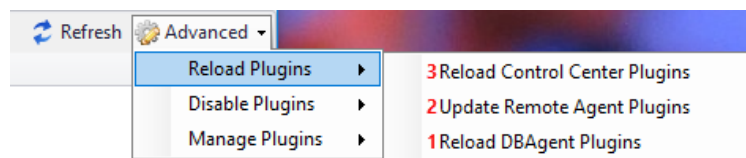
Enable

Disable

Refresh

About

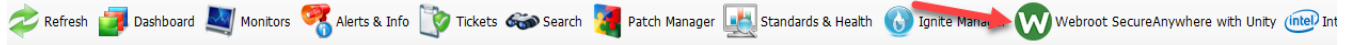
**Best Practice:** After installation, we recommend re-loading the **Reload DBAgent Plugins**, **Update Remote Agent Plugins** & **Reload Control Center Plugins** in the order shown below.



## Step 2 – Plugin settings

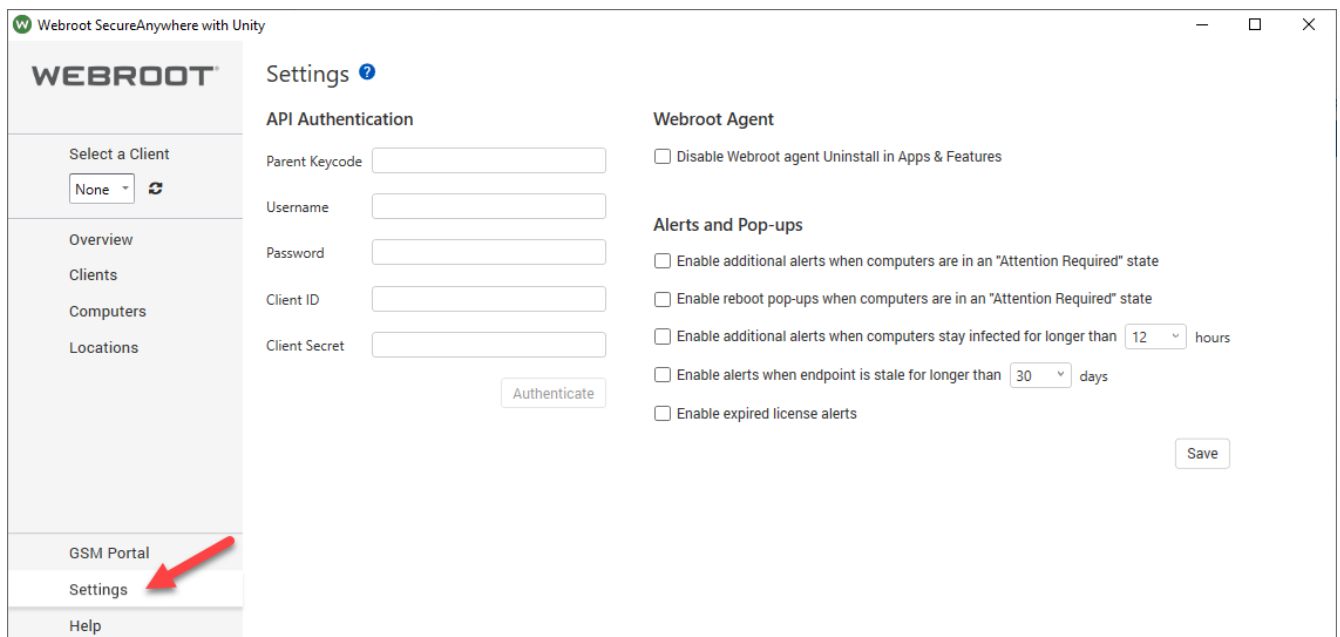
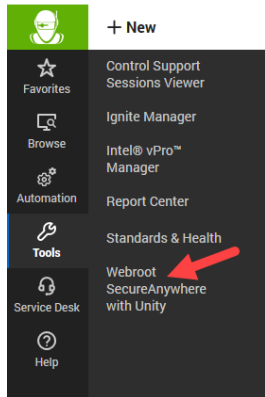
After you have restarted the Automate Control Center, click on **Webroot SecureAnywhere with Unity** to open the plugin dashboard and select **Settings**.

### ConnectWise Automate V11.x

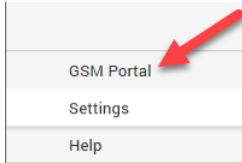


### ConnectWise Automate V12.x

Webroot - https://[redacted].hostedmm.com - U

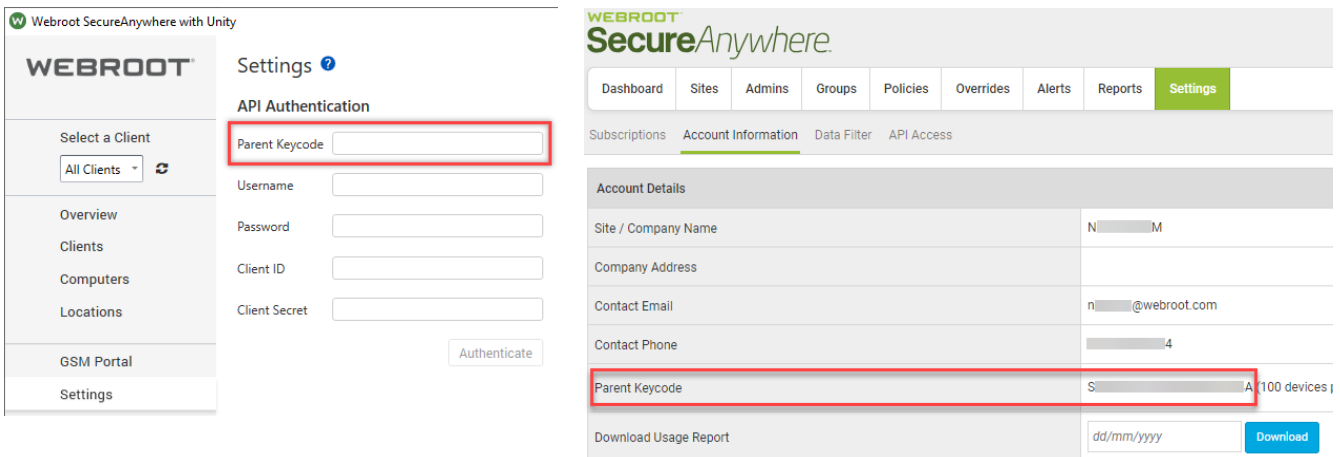


Click on **GSM Portal** to access the **Webroot Console** and enter your authentication information to access the GSM.



**BEST PRACTICE:** We strongly recommend you create a **NEW USER** with ADMIN rights across **ALL** existing Webroot Sites in the GSM and use the NEW USER Account for Webroot Unity Access for CW Automate. This will then avoid data discrepancies if Unity users do not have Admin rights across some Webroot Sites. Once complete follow instructions below.

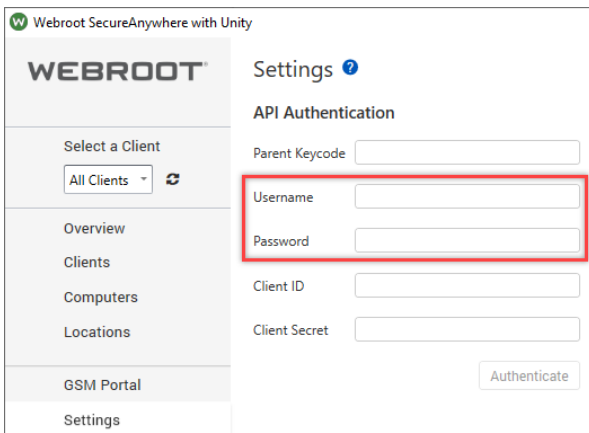
Navigate to **Settings > Account Information** in the GSM and copy and paste the Parent Keycode from the GSM to the Parent Keycode in the plugin. Please ensure no spaces are entered at the end.



The left screenshot shows the 'Webroot SecureAnywhere with Unity' console. The 'Settings' page is active, and the 'API Authentication' section is expanded. The 'Parent Keycode' field is highlighted with a red box. The 'Authenticate' button is visible at the bottom right of the API Authentication section.

The right screenshot shows the 'Webroot SecureAnywhere' console. The 'Settings' page is active, and the 'Account Information' section is expanded. The 'Parent Keycode' field is highlighted with a red box. The 'Download Usage Report' button is visible at the bottom right of the Account Information section.

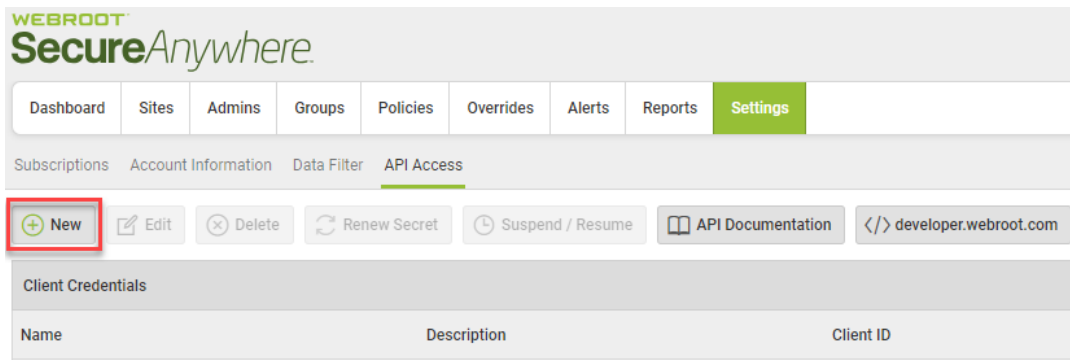
Use the **New Plugin Specific User Credentials** (see Best Practice above). Enter Console **Username** and **Password** in the Authentication Settings for the ConnectWise Automate Plugin.



The screenshot shows the 'Webroot SecureAnywhere with Unity' console. The 'Settings' page is active, and the 'API Authentication' section is expanded. The 'Username' and 'Password' fields are highlighted with a red box. The 'Authenticate' button is visible at the bottom right of the API Authentication section.



Navigate to **Settings > API Access** Tab and click **New** to create new API credentials.



WEBROOT® SecureAnywhere

Dashboard Sites Admins Groups Policies Overrides Alerts Reports **Settings**

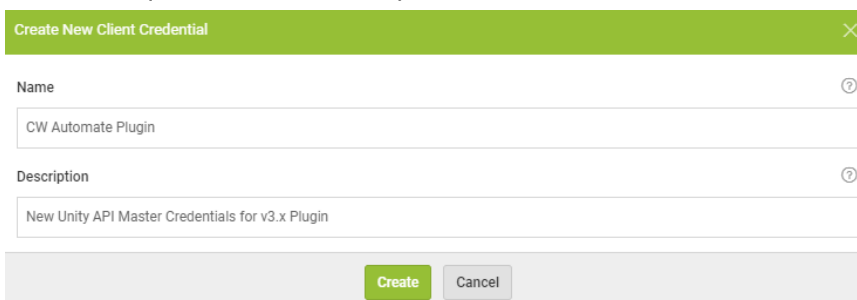
Subscriptions Account Information Data Filter **API Access**

**+ New** Edit Delete Renew Secret Suspend / Resume API Documentation </> developer.webroot.com

Client Credentials

Name	Description	Client ID
------	-------------	-----------

Enter a Unique Name and Description and Click **Create**



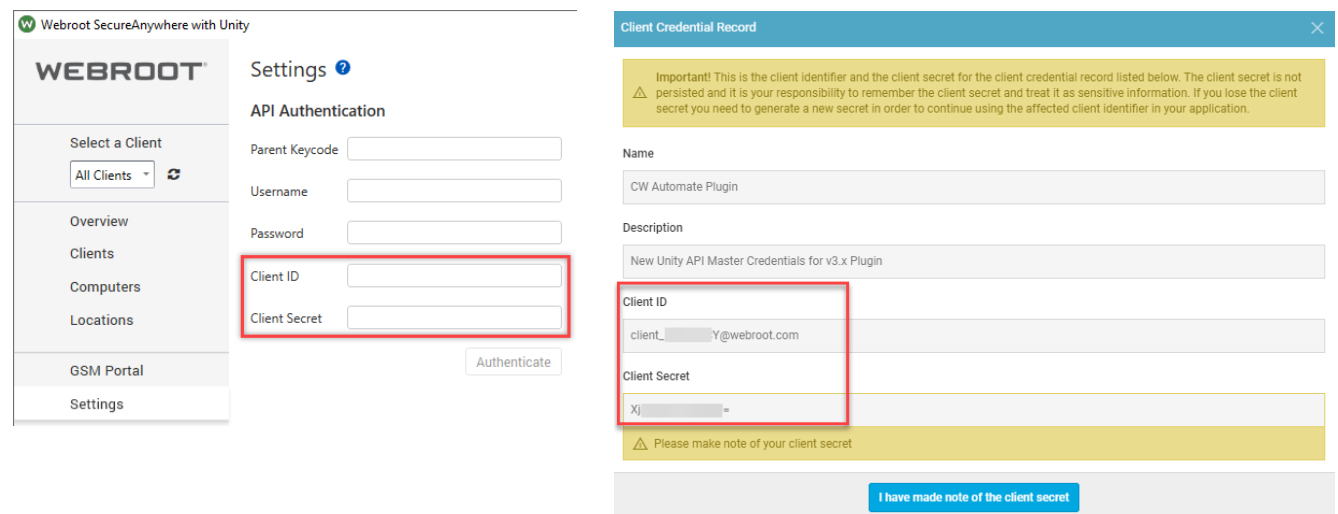
Create New Client Credential

Name ?  
CW Automate Plugin

Description ?  
New Unity API Master Credentials for v3.x Plugin

Create Cancel

Copy and paste **Client Id** and **Client Secret** to the CW Automate Plugin



Webroot SecureAnywhere with Unity

**WEBROOT®** Settings ?

API Authentication

Select a Client  
All Clients

Overview  
Clients  
Computers  
Locations  
GSM Portal  
Settings

Parent Keycode  
Username  
Password  
**Client ID**  
**Client Secret**

Authenticate

**Client Credential Record**

Important! This is the client identifier and the client secret for the client credential record listed below. The client secret is not persisted and it is your responsibility to remember the client secret and treat it as sensitive information. If you lose the client secret you need to generate a new secret in order to continue using the affected client identifier in your application.

Name  
CW Automate Plugin

Description  
New Unity API Master Credentials for v3.x Plugin

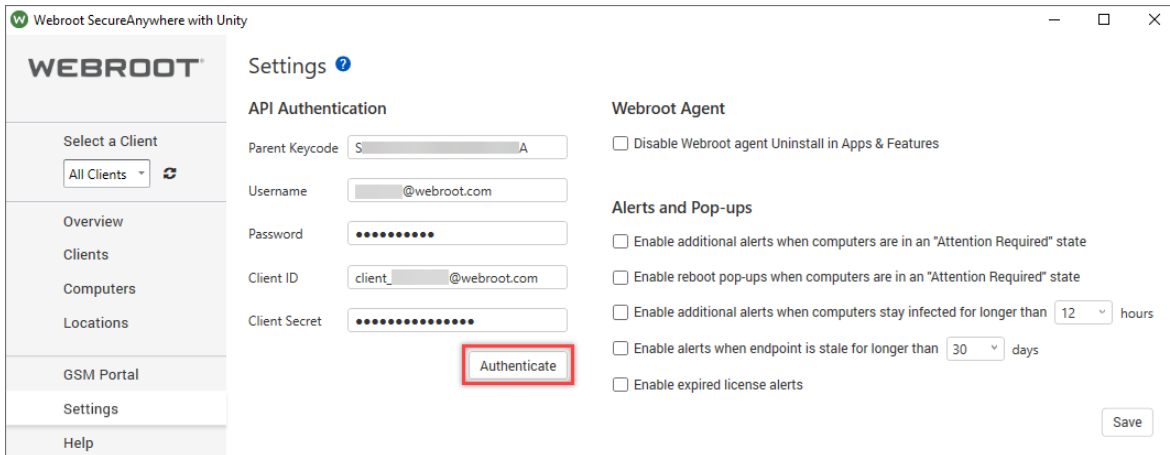
**Client ID**  
client\_...@webroot.com

**Client Secret**  
Xj...=

Please make note of your client secret

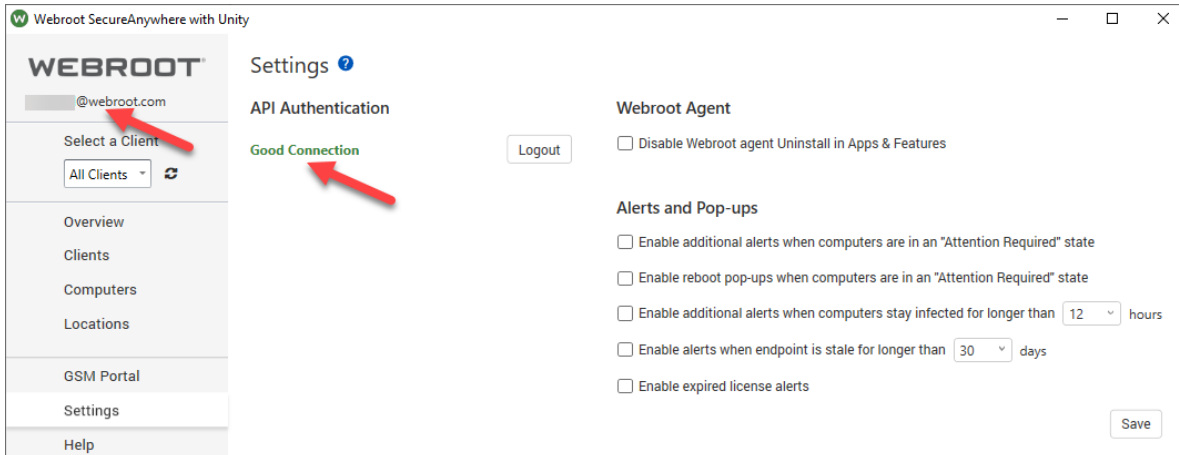
I have made note of the client secret

Once all credentials are entered, click on **Authenticate**.



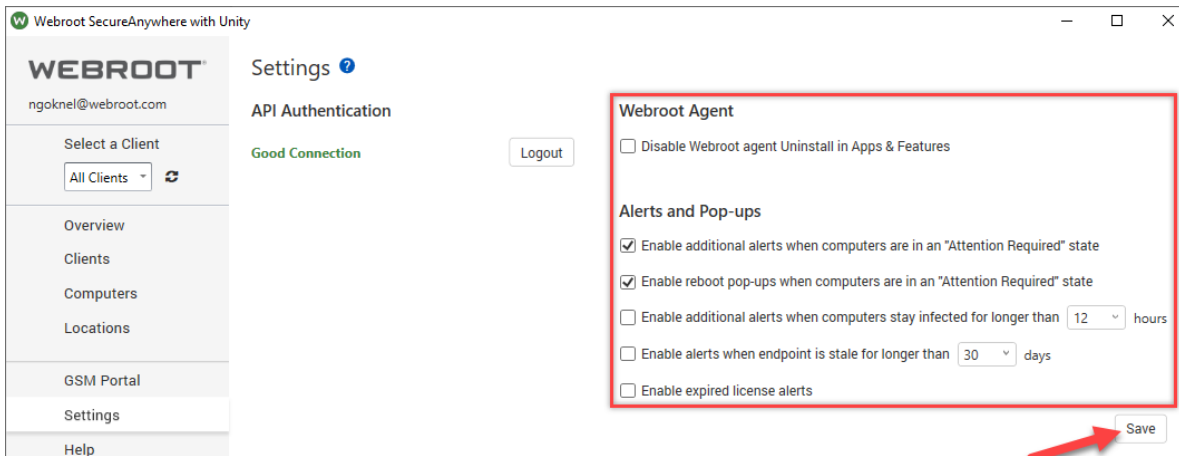
The screenshot shows the 'Settings' window for 'Webroot SecureAnywhere with Unity'. The 'API Authentication' section contains fields for Parent Keycode, Username, Password, Client ID, and Client Secret. The 'Authenticate' button is highlighted with a red rectangle. The 'Webroot Agent' and 'Alerts and Pop-ups' sections are also visible.

When the credentials are successfully authenticated, **Good Connection** and authenticated username will be displayed.



The screenshot shows the 'Settings' window after successful authentication. The 'API Authentication' section now displays 'Good Connection' in green. The authenticated username '@webroot.com' is shown in the top left. Red arrows point to the 'Good Connection' text and the username.

If required, please set the desired settings and click **Save**. We recommend these settings are left at their default values at this stage. When you are more familiar with the plugin and have had a chance to go through the Plugin Walkthrough, you can set these at any time.



The screenshot shows the 'Settings' window with the 'Webroot Agent' and 'Alerts and Pop-ups' sections highlighted by a red rectangle. The 'Save' button is highlighted with a red arrow. The 'Alerts and Pop-ups' section shows several settings that are checked by default.

## Step 3 – Assigning Clients to existing Webroot Sites

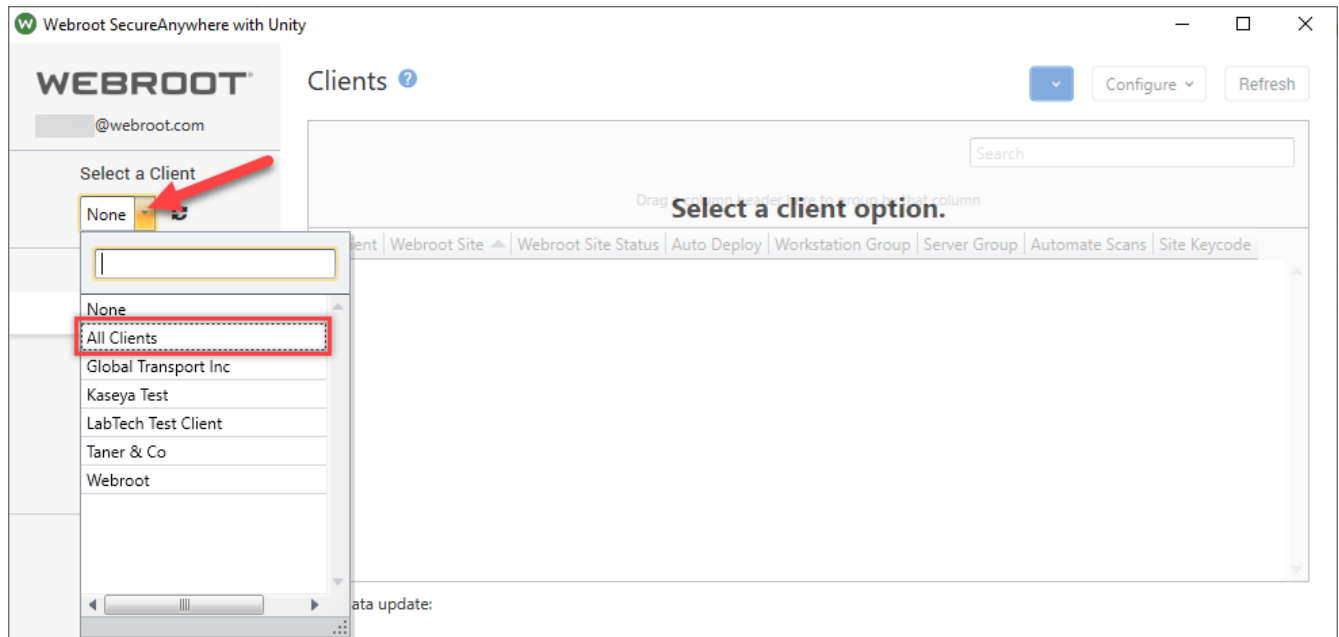
If you have already created Sites in the Webroot Global Site Manager that match your Clients and there is a 1 to 1 relationship between **CW Automate Clients & Webroot Sites**, you must Assign Webroot Sites to Clients within the plugin. This will establish an API connection into the GSM for each Site, pulling in correct data and enabling advanced functionality. Please take your time when assigning Clients to Sites, ensure the correct Clients are assigned to correct Sites.

If you have not yet created Webroot Sites, please go to the next step.

Click on **Clients** tab

Click on **Select a Client**

Either select **All Clients** (recommended for up to 60 Clients) or select individual Clients

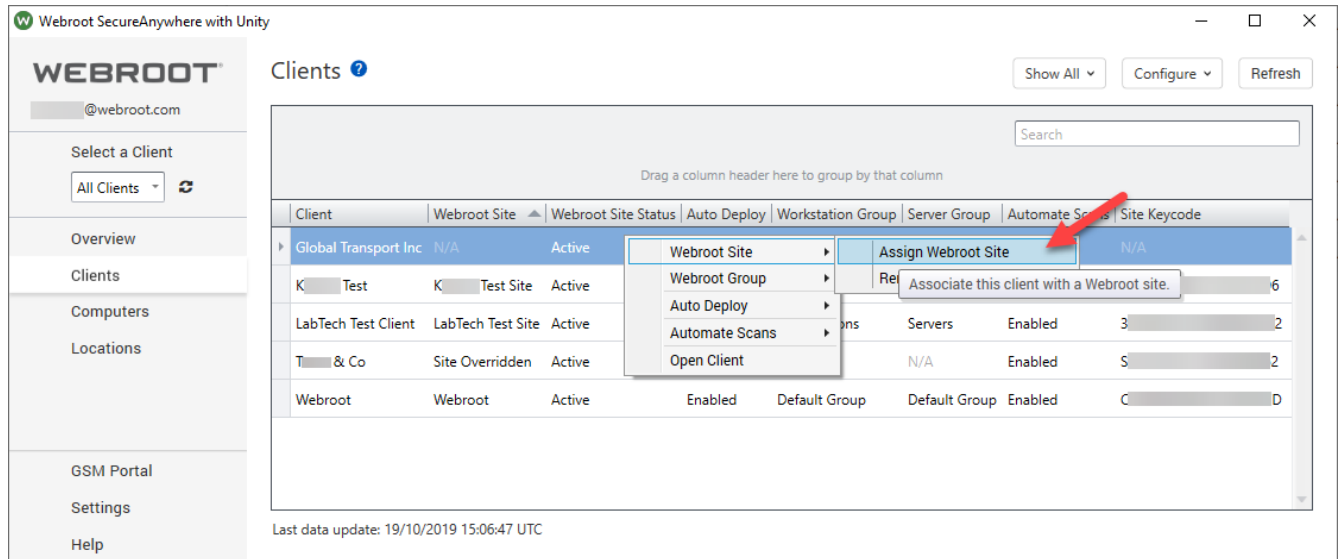


Right click on a specific Client

Select **Webroot site**

Select **Assign Webroot site**

Use the drop-down menu to assign the correct site (assuming you have already created matching sites)



Webroot SecureAnywhere with Unity

**WEBROOT®**  
@webroot.com

Select a Client  
All Clients

Overview  
Clients  
Computers  
Locations  
GSM Portal  
Settings  
Help

**Clients**

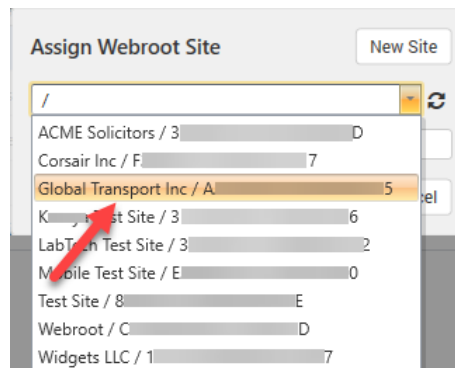
Show All Configure Refresh

Search

Drag a column header here to group by that column

Client	Webroot Site	Webroot Site Status	Auto Deploy	Workstation Group	Server Group	Automate Scans	Site Keycode
Global Transport Inc	N/A	Active					N/A
K Test	K Test Site	Active					6
LabTech Test Client	LabTech Test Site	Active					2
T & Co	Site Overridden	Active					2
Webroot	Webroot	Active	Enabled	Default Group	Default Group	Enabled	D

Last data update: 19/10/2019 15:06:47 UTC



**Assign Webroot Site** New Site

/

- ACME Solicitors / 3 D
- Corsair Inc / F 7
- Global Transport Inc / A 5
- K Test Site / 3 6
- LabTech Test Site / 3 2
- Mobile Test Site / E 0
- Test Site / 8 E
- Webroot / C D
- Widgets LLC / 1 7

## Step 4 – Creating new Webroot sites

If you are a new Webroot user and have not created any matching Sites for your Clients, then you should create New Webroot Sites either directly within the plugin or within the Global Site Manager (GSM).

If you do NOT have a Global Site Manager but only have a Webroot Business Console, please contact your Webroot representative or Webroot support.

To create Sites directly within the plugin for each of your Clients, follow the instructions below:

Click on **Clients** tab

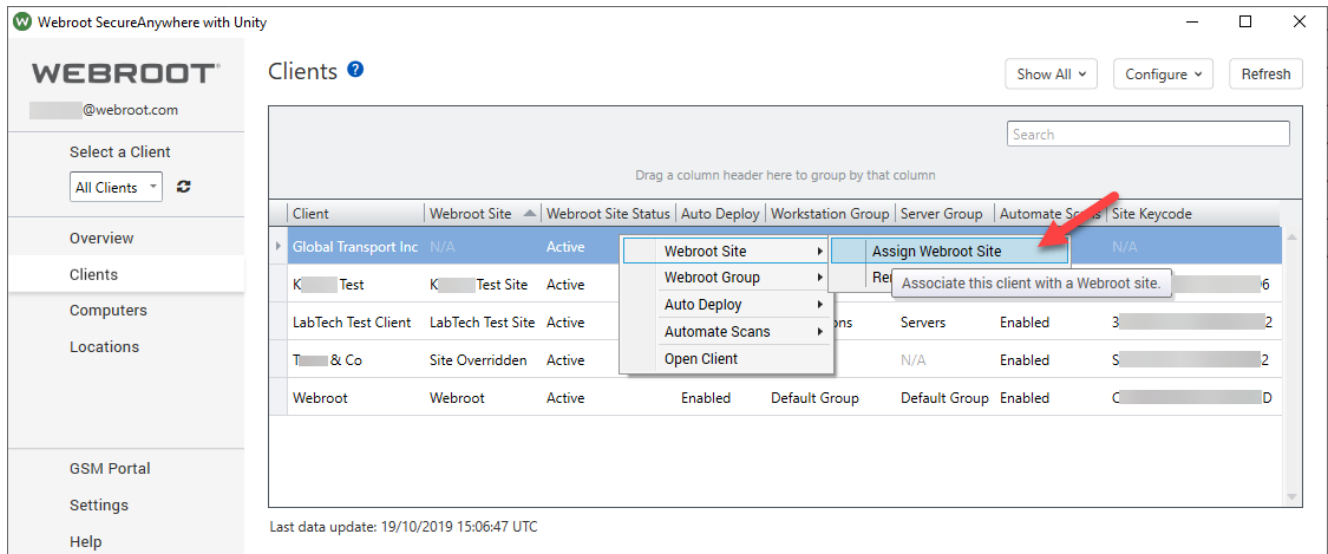
Right click on a specific Client

Select **Webroot site**

Select **Assign Webroot site**

Select **New**

Fill in the required fields and click **Create**



Webroot SecureAnywhere with Unity

**WEBROOT®**  
@webroot.com

Select a Client  
All Clients

Overview  
Clients  
Computers  
Locations

GSM Portal  
Settings  
Help

**Clients**

Show All Configure Refresh

Search

Drag a column header here to group by that column

Client	Webroot Site	Webroot Site Status	Auto Deploy	Workstation Group	Server Group	Automate Scans	Site Keycode
Global Transport Inc	N/A	Active					N/A
K Test	K Test Site	Active					6
LabTech Test Client	LabTech Test Site	Active					2
T & Co	Site Overridden	Active					2
Webroot	Webroot	Active	Enabled	Default Group	Default Group	Enabled	D

Last data update: 19/10/2019 15:06:47 UTC

**Assign Webroot Site**

Manual Site Keycode

**Create Webroot Site**

Site Name

Keycode Type  
☒ Full ☐ 30 day trial  
 Seats **\*Required**

Billing Cycle

Billing Date  
Jan 1

Comments

☐ Include Global Policies  
☐ Include Global Overrides

Default Policy

Report Email Distribution List **\*Required**

## Step 5 – Activating Auto Deploy

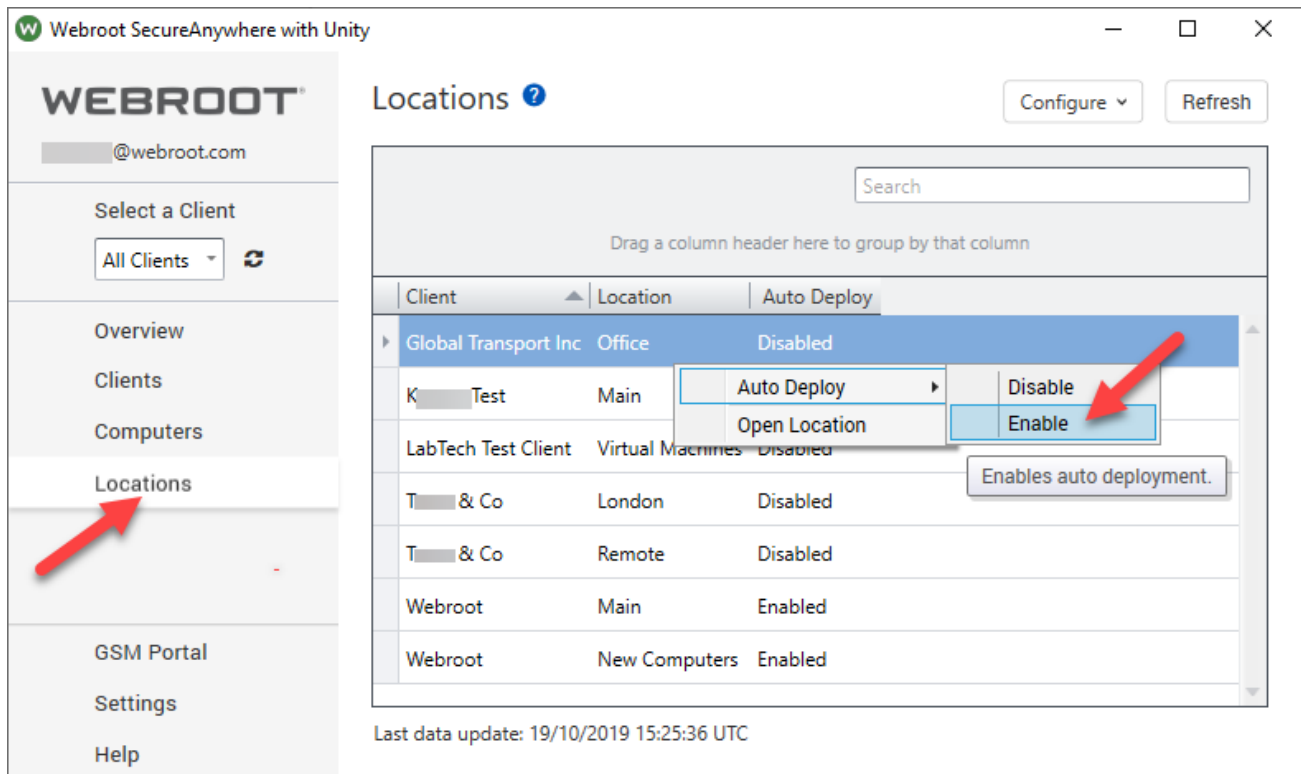
To allow the plugin to install Webroot agents, Auto Deploy setting must be enabled at the CW Automate Location level. The **default** auto deploy setting at **Location level** is **Auto Deploy = Disabled**. When set to Enabled webroot agents will start to deploy to all Computers under that Location, unless specific Computers have their Auto Deploy setting set to Disabled.

To enable Auto Deploy at Location Level, click on **Locations**

Right click on the relevant Location **OR** select multiple locations and use the **Configure** drop down menu

Select **Auto Deploy**

Select **Enable** to Auto Deploy



Webroot SecureAnywhere with Unity

**WEBROOT®**

@webroot.com

Select a Client

All Clients

Overview

Clients

Computers

**Locations**

GSM Portal

Settings

Help

Locations ?

Configure Refresh

Search

Drag a column header here to group by that column

Client	Location	Auto Deploy
Global Transport Inc	Office	Disabled
K Test	Main	Auto Deploy
LabTech Test Client	Virtual Machines	Disabled
T & Co	London	Disabled
T & Co	Remote	Disabled
Webroot	Main	Enabled
Webroot	New Computers	Enabled

Last data update: 19/10/2019 15:25:36 UTC

**Note:** By default, auto deploy is set to:

- Enabled at Client/Site level
- **Disabled** at Location level
- Enabled at Computer level

## Step 6 – Plugin reference & walkthrough

Walk through the rest of the manual and enjoy the powerful new features available in the version 3.x plugin. Jump to the [Plugin Reference & Walkthrough](#) section and go through the rest of the manual.

## SECTION 2 - Upgrade instructions from legacy plugins

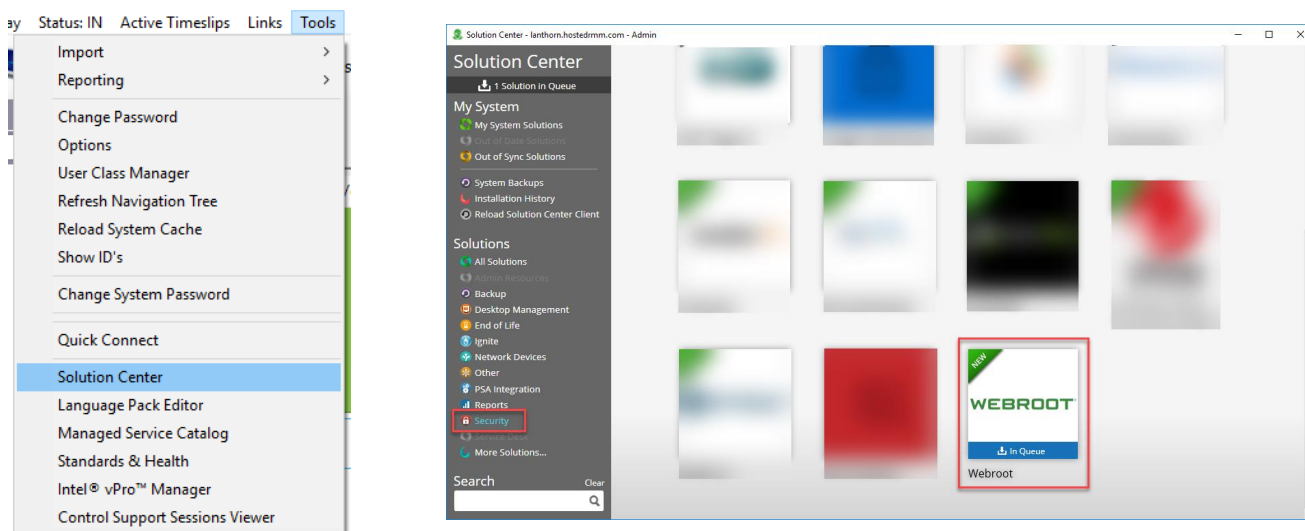
### Step 1 – Upgrading from plugin version 2.5 or older

Important: When upgrading from any previous version of the Webroot plugin to Version 3.x you **MUST** first upgrade your existing plugin to **version 2.5.13** before attempting to upgrade to Version 3.x. Version 2.5.13 can be downloaded from the link below:

Version 2.5.x [http://download.webroot.com/RMM/LabTech/Webroot-Deploy-Solution\\_v2-5.zip](http://download.webroot.com/RMM/LabTech/Webroot-Deploy-Solution_v2-5.zip)

### Step 2 – Obtaining the plugin

If you are upgrading from a previous version the latest of the Webroot plugin can be installed from CW Solution Center. Please select Security and Webroot and follow the standard Solution Center installation instructions.

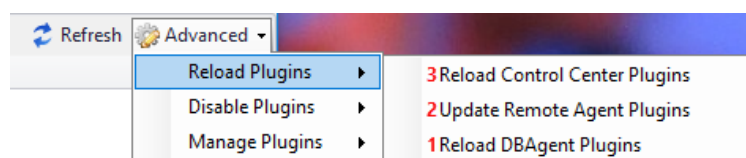


**IMPORTANT NOTE:** After an Upgrade Webroot SecureAnywhere with Unity RA **WebrootRA.dll** is added to the CW Automate plugin manager. Please navigate to **Help > Plugin Manager** within the Control Center and **Enable** “Webroot SecureAnywhere with Unity RA” and restart your Control Center, before proceeding to next step.

✓	Webroot SecureAnywhere with Unity	3.0.1622.8	Webroot Inc.	Webroot SecureAnywhere with Unity		✓	✓	⊘	webroot.dll
✓	Webroot SecureAnywhere with Unity RA	3.0.1622.8	Webroot Inc.	Webroot SecureAnywhere with Unity RA		✓	✓	✓	WebrootRA.dll

Enable  
Disable  
Refresh  
About

**Best Practice:** After the upgrade process above, we recommend re-loading the **Reload DBAgent Plugins**, **Update Remote Agent Plugins** & **Reload Control Center Plugins** in the order shown below.



## Step 3 – What happens after an upgrade from plugin version 2.5

After an upgrade from plugin **version 2.5.13** of the Webroot ConnectWise Automate (CWA) plugin you should expect the following:

- 1- Settings below are automatically transferred across
  - a. The Unique Identifier Setting is set to off
  - b. Alerts and pop-up settings
  - c. Auto-deploy and exceptions settings
  - d. Site keycodes without assignment

Note: Automate Clients will require to be assigned to Webroot Sites for full Unity API functionality

- 2- The plugin core functionality such as auto-deployment of Webroot agents will operate but some portions will not show data and will be replaced by **N/A** and **non-GSM** until Automate Clients are assigned to Webroot Sites



## Step 4 – Plugin settings

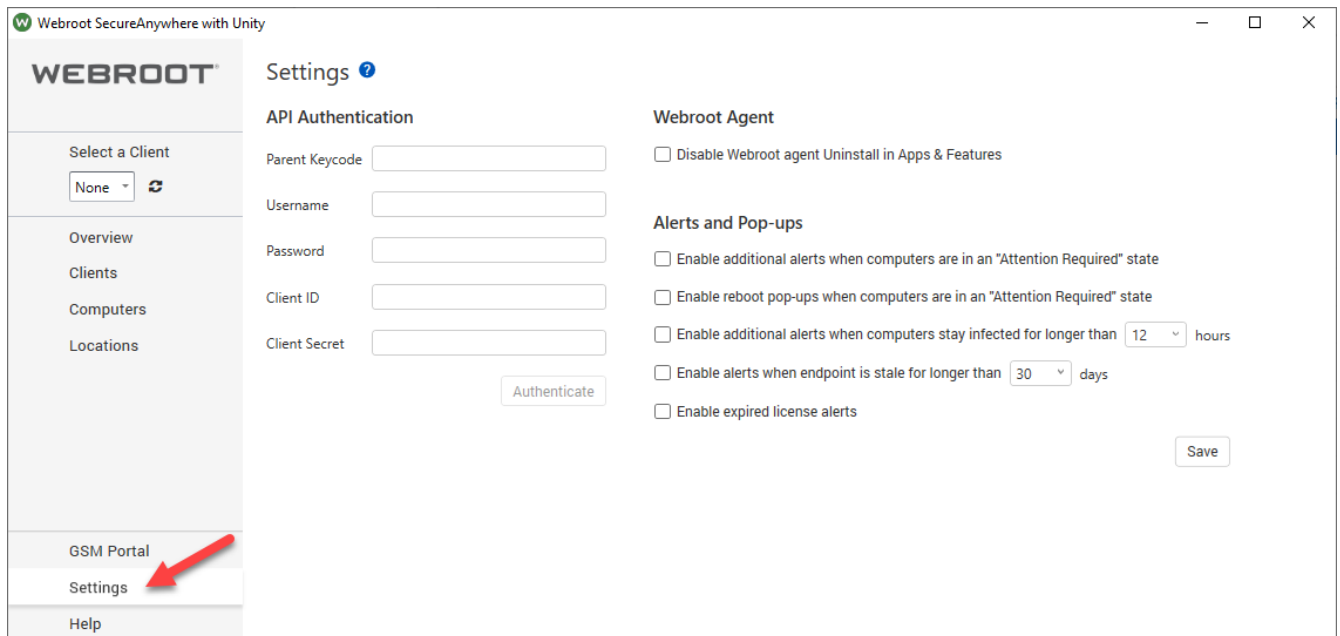
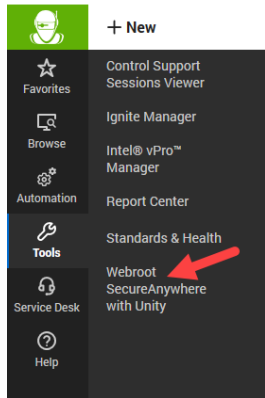
After you have restarted the Automate Control Center, click on **Webroot SecureAnywhere with Unity** to open the plugin dashboard and select **Settings**.

### ConnectWise Automate V11.x

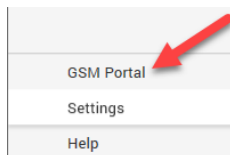


### ConnectWise Automate V12.x

Webroot - https://[redacted].hostedmm.com - U

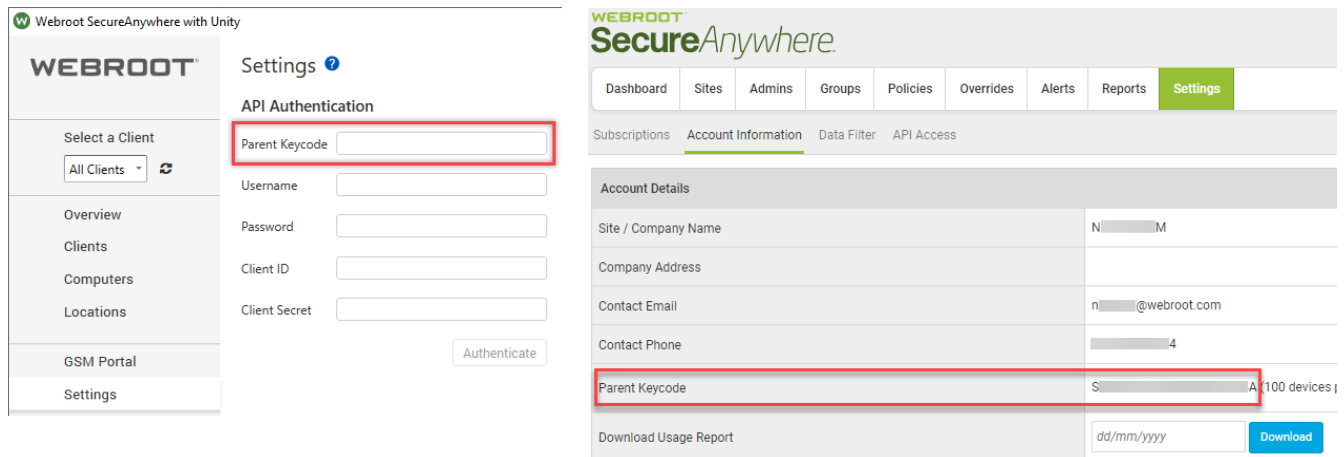


Click on **GSM Portal** to access the Webroot Console and enter your authentication information to access the GSM.



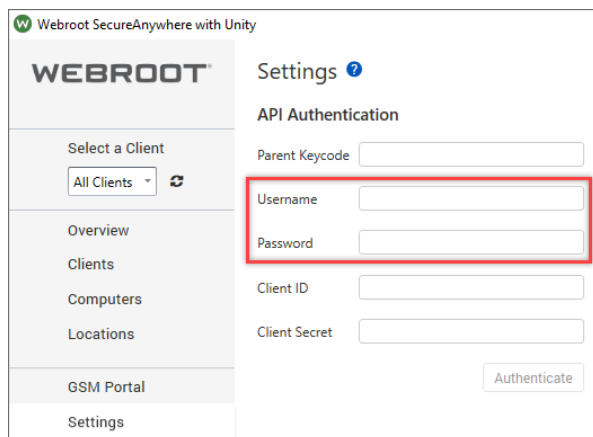
**BEST PRACTICE:** We strongly recommend you create a **NEW USER** with ADMIN rights across **ALL** existing Webroot Sites in the GSM and use the NEW USER Account for Webroot Unity Access for CW Automate. This will then avoid data discrepancies if Unity users do not have Admin rights across some Webroot Sites. Once complete follow instructions below.

Navigate to **Settings > Account Information** and copy and paste the Parent Keycode from the GSM to the Parent Keycode in the plugin. Please ensure no spaces are entered at the end.



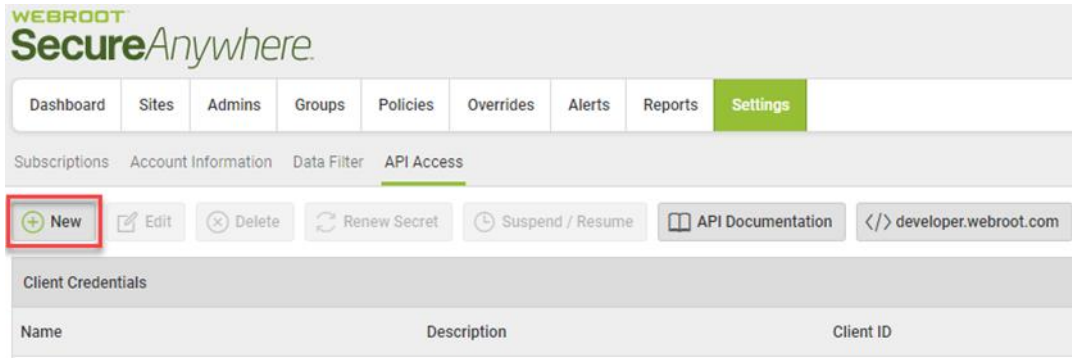
The left screenshot shows the 'Settings' page with the 'API Authentication' section. The 'Parent Keycode' field is highlighted with a red box. The right screenshot shows the 'Account Information' tab, also with the 'Parent Keycode' field highlighted by a red box.

Use the **New Plugin Specific User Credentials** (see Best Practice above). Enter Console **Username** and **Password** in the Authentication Settings for the ConnectWise Automate Plugin.



The screenshot shows the 'Settings' page with the 'API Authentication' section. The 'Username' and 'Password' fields are highlighted by a red box.

Navigate to **Settings > API Access Tab** and click **New** to create new API credentials.



WEBROOT® SecureAnywhere

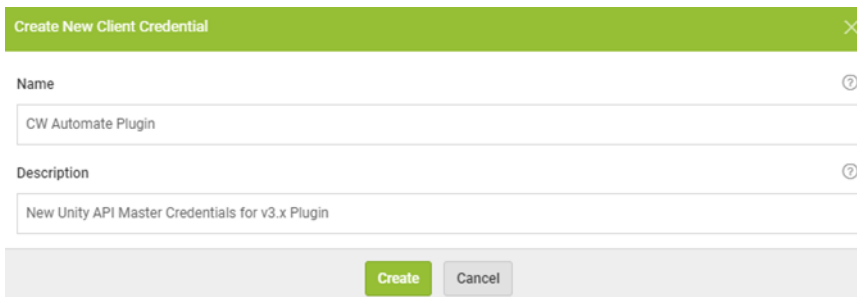
Dashboard Sites Admins Groups Policies Overrides Alerts Reports **Settings**

Subscriptions Account Information Data Filter **API Access**

**New** Edit Delete Renew Secret Suspend / Resume API Documentation </> developer.webroot.com

Client Credentials		
Name	Description	Client ID

Enter a Unique Name and Description and Click **Create**



Create New Client Credential

Name ?

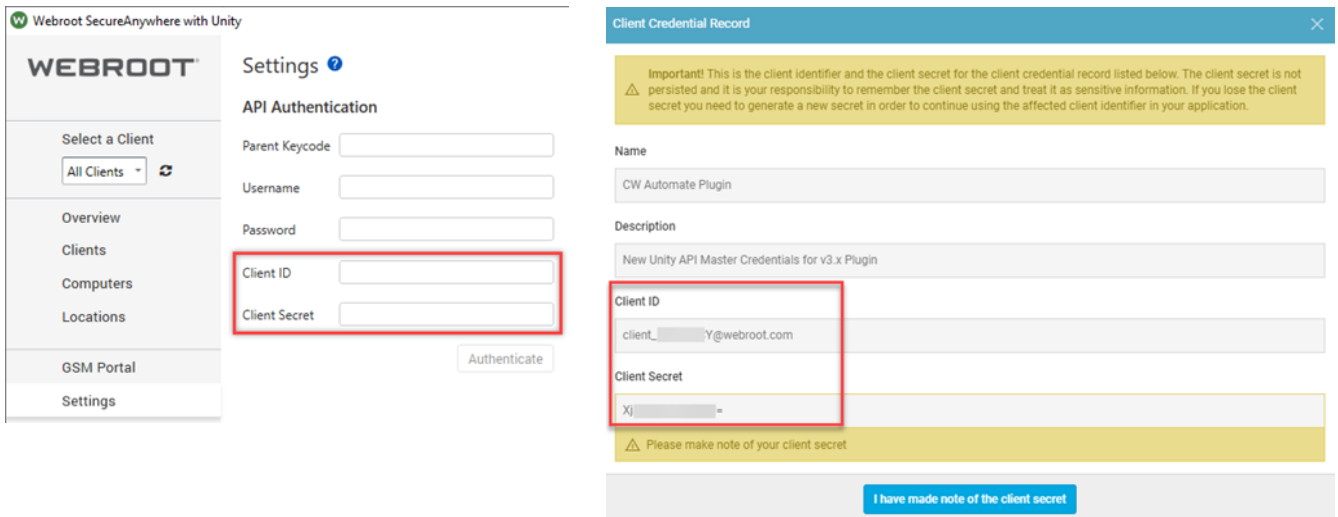
CW Automate Plugin

Description ?

New Unity API Master Credentials for v3.x Plugin

Create Cancel

Copy and paste **Client Id** and **Client Secret** to the CW Automate Plugin



Webroot SecureAnywhere with Unity

**WEBROOT®**

Select a Client

All Clients

Overview

Clients

Computers

Locations

GSM Portal

Settings

**Settings**

**API Authentication**

Parent Keycode

Username

Password

**Client ID**

**Client Secret**

Authenticate

**Client Credential Record**

Important! This is the client identifier and the client secret for the client credential record listed below. The client secret is not persisted and it is your responsibility to remember the client secret and treat it as sensitive information. If you lose the client secret you need to generate a new secret in order to continue using the affected client identifier in your application.

Name

CW Automate Plugin

Description

New Unity API Master Credentials for v3.x Plugin

**Client ID**

client\_...@webroot.com

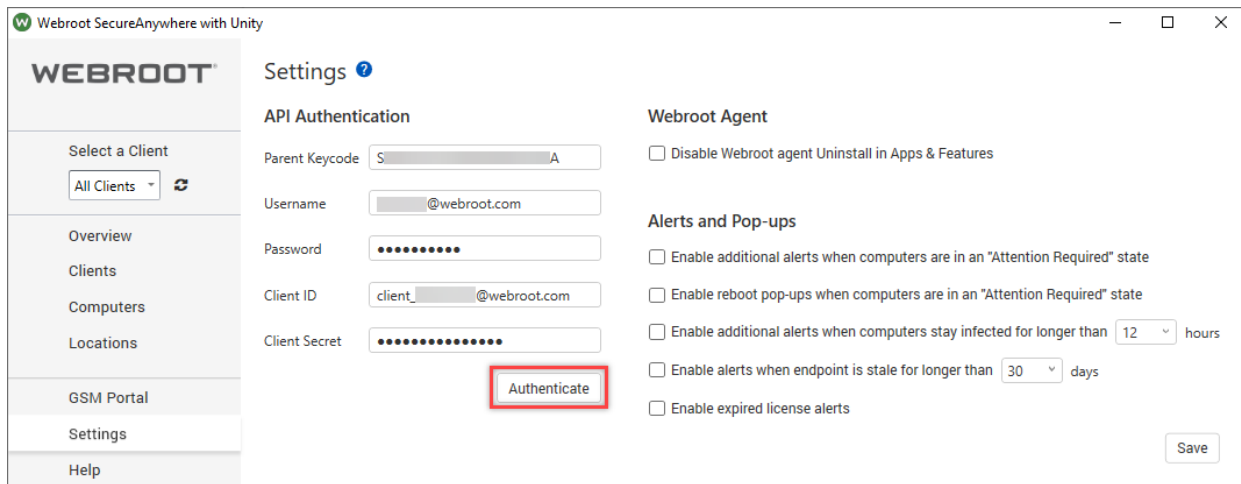
**Client Secret**

xj...=

Please make note of your client secret

I have made note of the client secret

Once all credentials are entered, click on **Authenticate**.



Webroot SecureAnywhere with Unity

**WEBROOT®**

Select a Client  
All Clients

Overview  
Clients  
Computers  
Locations

GSM Portal  
Settings  
Help

**Settings**

**API Authentication**

Parent Keycode: S...A

Username: @webroot.com

Password: .....

Client ID: client\_@webroot.com

Client Secret: .....

**Authenticate**

**Webroot Agent**

☐ Disable Webroot agent Uninstall in Apps & Features

**Alerts and Pop-ups**

☐ Enable additional alerts when computers are in an "Attention Required" state

☐ Enable reboot pop-ups when computers are in an "Attention Required" state

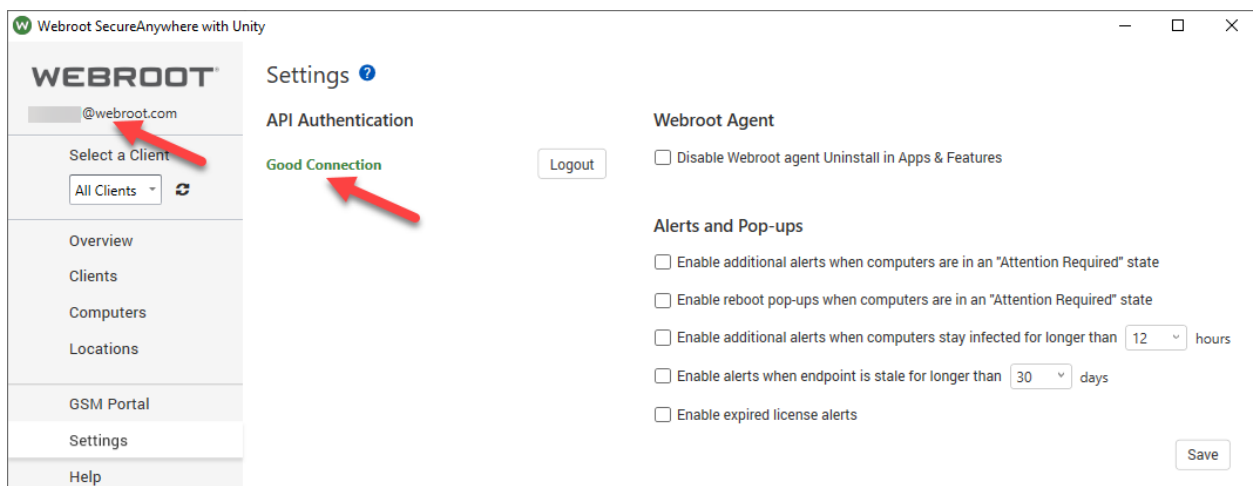
☐ Enable additional alerts when computers stay infected for longer than 12 hours

☐ Enable alerts when endpoint is stale for longer than 30 days

☐ Enable expired license alerts

**Save**

When the credentials are successfully authenticated, **Good Connection** and authenticated username will be displayed.



Webroot SecureAnywhere with Unity

**WEBROOT®**  
@webroot.com

Select a Client  
All Clients

Overview  
Clients  
Computers  
Locations

GSM Portal  
Settings  
Help

**Settings**

**API Authentication**

Good Connection

Logout

**Webroot Agent**

☐ Disable Webroot agent Uninstall in Apps & Features

**Alerts and Pop-ups**

☐ Enable additional alerts when computers are in an "Attention Required" state

☐ Enable reboot pop-ups when computers are in an "Attention Required" state

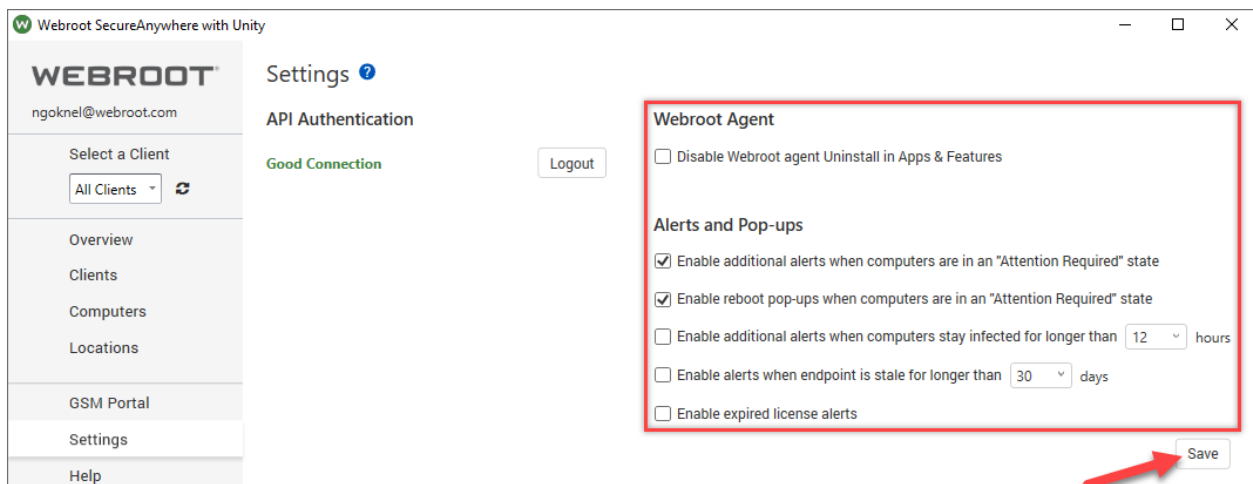
☐ Enable additional alerts when computers stay infected for longer than 12 hours

☐ Enable alerts when endpoint is stale for longer than 30 days

☐ Enable expired license alerts

**Save**

If required, please set the desired settings and click **Save**.



Webroot SecureAnywhere with Unity

**WEBROOT®**  
ngoknel@webroot.com

Select a Client  
All Clients

Overview  
Clients  
Computers  
Locations

GSM Portal  
Settings  
Help

**Settings**

**API Authentication**

Good Connection

Logout

**Webroot Agent**

☐ Disable Webroot agent Uninstall in Apps & Features

**Alerts and Pop-ups**

☒ Enable additional alerts when computers are in an "Attention Required" state

☒ Enable reboot pop-ups when computers are in an "Attention Required" state

☐ Enable additional alerts when computers stay infected for longer than 12 hours

☐ Enable alerts when endpoint is stale for longer than 30 days

☐ Enable expired license alerts

**Save**

## Step 5 – Assigning Clients to existing Webroot Sites

If you have already created Sites in the Webroot Global Site Manager that match your Clients and there is a 1 to 1 relationship between **CW Automate Clients & Webroot Sites**, you must Assign Webroot Sites to Clients within the plugin. This will establish an API connection into GSM for each Site, pulling in correct data and enabling advanced functionality. Please take your time when assigning Clients to Sites, ensure the correct Clients are assigned to correct Sites.

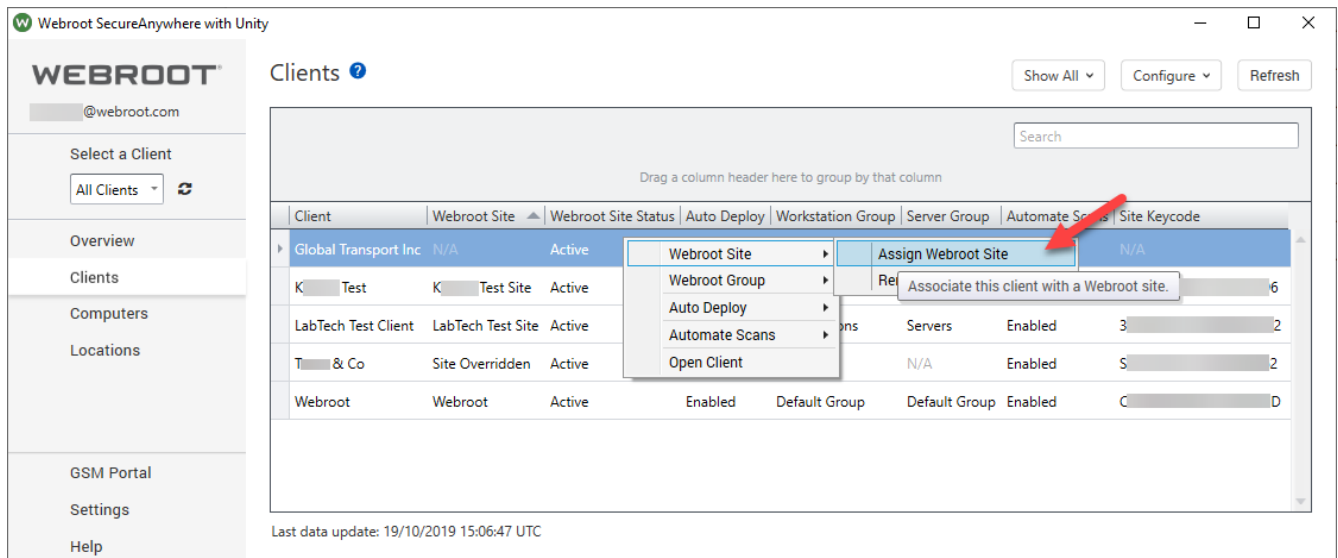
Click on **Clients** tab

Right click on a specific Client

Select **Webroot site**

Select **Assign Webroot site**

Use the drop down menu to assign the correct site (ensure keycode matches the imported key from previous version)



Webroot SecureAnywhere with Unity

**WEBROOT®**  
@webroot.com

Select a Client  
All Clients

Overview  
Clients  
Computers  
Locations

GSM Portal  
Settings  
Help

**Clients**

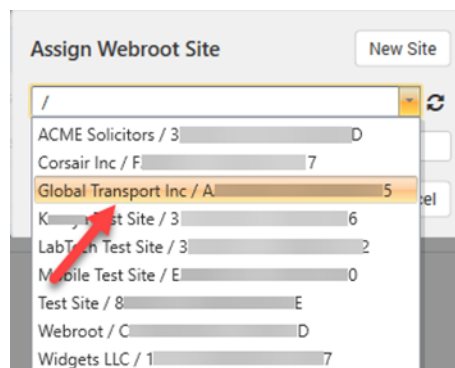
Show All Configure Refresh

Search

Drag a column header here to group by that column

Client	Webroot Site	Webroot Site Status	Auto Deploy	Workstation Group	Server Group	Automate Scans	Site Keycode
Global Transport Inc	N/A	Active					N/A
K... Test	K... Test Site	Active					6
LabTech Test Client	LabTech Test Site	Active					2
T... & Co	Site Overridden	Active					2
Webroot	Webroot	Active	Enabled	Default Group	Default Group	Enabled	D

Last data update: 19/10/2019 15:06:47 UTC



**Assign Webroot Site** New Site

/

- ACME Solicitors / 3 D
- Corsair Inc / F 7
- Global Transport Inc / A 5
- K... Test Site / 3 6
- LabTech Test Site / 3 2
- Mobile Test Site / E 0
- Test Site / 8 E
- Webroot / C D
- Widgets LLC / 1 7

## Step 6 – Creating new Webroot sites

If you are currently mapping **Webroot Groups to Automate Clients** then you must create **New Webroot Sites** either directly within the plugin or within the Global Site Manager (GSM) and move the endpoints to the new Webroot Sites via Change Keycode command in the Webroot console.

If you do NOT have a Global Site Manager but only have a Webroot Business Console, please contact your Webroot representative or support.

To create Sites directly within the plugin, follow the instructions below:

Click on **Clients** tab

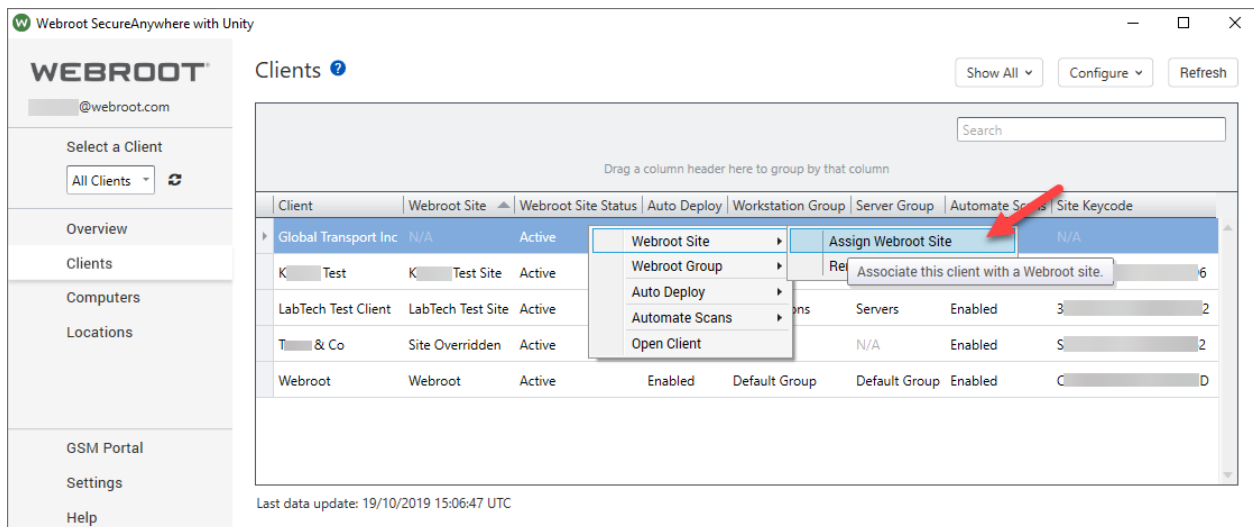
Right click on a specific Client

Select **Webroot site**

Select **Assign Webroot site**

Select **New**

Fill in required fields and click **Create**



Webroot SecureAnywhere with Unity

**WEBROOT®**  
@webroot.com

Select a Client  
All Clients

Overview  
Clients  
Computers  
Locations

GSM Portal  
Settings  
Help

**Clients**

Show All Configure Refresh

Search

Drag a column header here to group by that column

Client	Webroot Site	Webroot Site Status	Auto Deploy	Workstation Group	Server Group	Automate Scans	Site Keycode
Global Transport Inc	N/A	Active					N/A
K Test	K Test Site	Active					6
LabTech Test Client	LabTech Test Site	Active					
T & Co	Site Overridden	Active					2
Webroot	Webroot	Active	Enabled	Default Group	Default Group	Enabled	D

Last data update: 19/10/2019 15:06:47 UTC

**Assign Webroot Site**

New Site

/

Manual Site Keycode

Save Cancel

**Create Webroot Site**

Site Name  
Global Transport Inc

Keycode Type  
☒ Full ☐ 30 day trial  
 Seats \*Required

Billing Cycle  
Annually

Billing Date  
Jan 1

Comments  
Created by CW Automate

☐ Include Global Policies  
☐ Include Global Overrides

Default Policy  
High Security Policy

Report Email Distribution List \*Required

Create Cancel

## Step 7 – Activating auto deploy

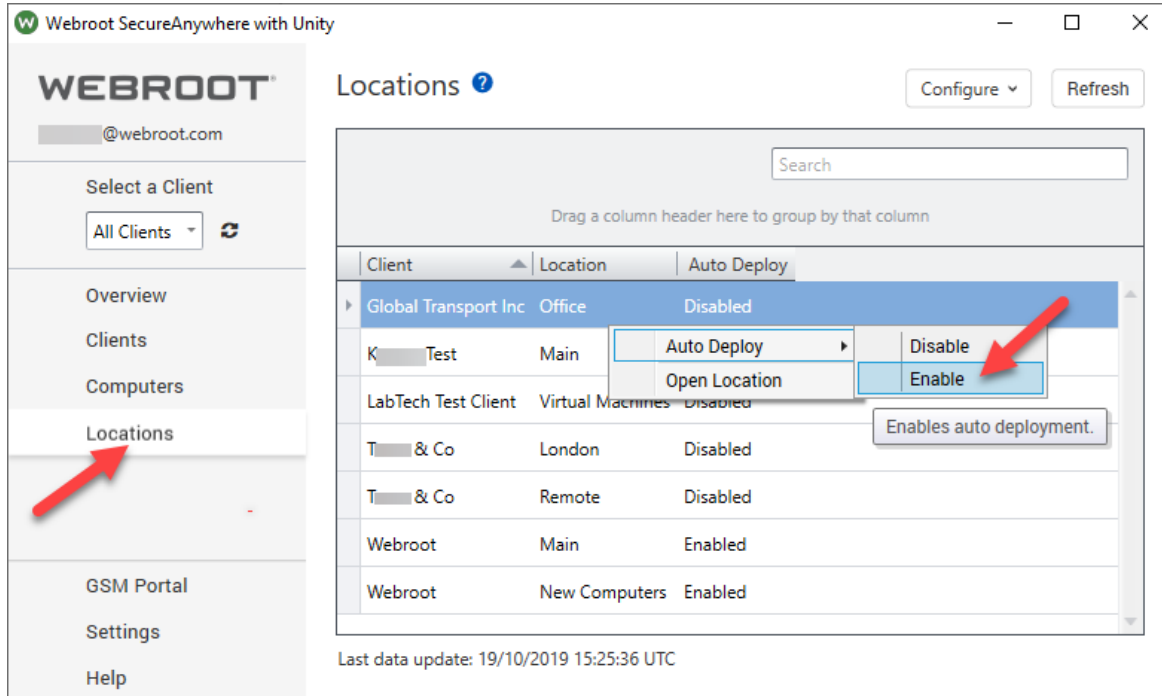
To allow the plugin to install Webroot agents, Auto Deploy setting must be enabled at the CW Automate Location level. The **default auto deploy setting at Location level is Auto Deploy = Disabled**. When set to Enabled webroot agents will start to deploy to all Computers under that Location, unless specific Computers have their Auto Deploy setting set to Disabled.

To enable Auto Deploy at Location Level, click on **Locations** tab

Right click on the relevant Location **OR** select multiple locations and use the **Configure** drop down menu

Select **Auto Deploy**

Select **Enable** to Auto Deploy



Webroot SecureAnywhere with Unity

**WEBROOT®**  
@webroot.com

Select a Client  
All Clients

Overview  
Clients  
Computers  
**Locations**

GSM Portal  
Settings  
Help

Locations ?

Configure Refresh

Search

Drag a column header here to group by that column

Client	Location	Auto Deploy
Global Transport Inc	Office	Disabled
K Test	Main	Auto Deploy
LabTech Test Client	Virtual Machines	Disabled
T & Co	London	Disabled
T & Co	Remote	Disabled
Webroot	Main	Enabled
Webroot	New Computers	Enabled

Last data update: 19/10/2019 15:25:36 UTC

**Note:** By default, auto deploy is set to:

- Enabled at Client/Site level
- **Disabled** at Location level
- Enabled at Computer level

## Step 8 – Plugin walkthrough

Walk through the rest of the manual and enjoy the powerful new features available in the version 3.x plugin. Jump to the [Plugin Reference & Walkthrough](#) section and go through the rest of the manual.

## SECTION 3 - Plugin Reference & Walkthrough

Webroot plugin version 3.x is our most advanced plugin to date and makes use of the Webroot Unity API, unleashing more features than previously possible. These include Policy Assignment, Site Creation, Workstation & Server Group policy assignment and many more. The plugin walkthrough will take you through the features available.

**Note:** This plugin is compatible with CW Automate v10.5 and above.

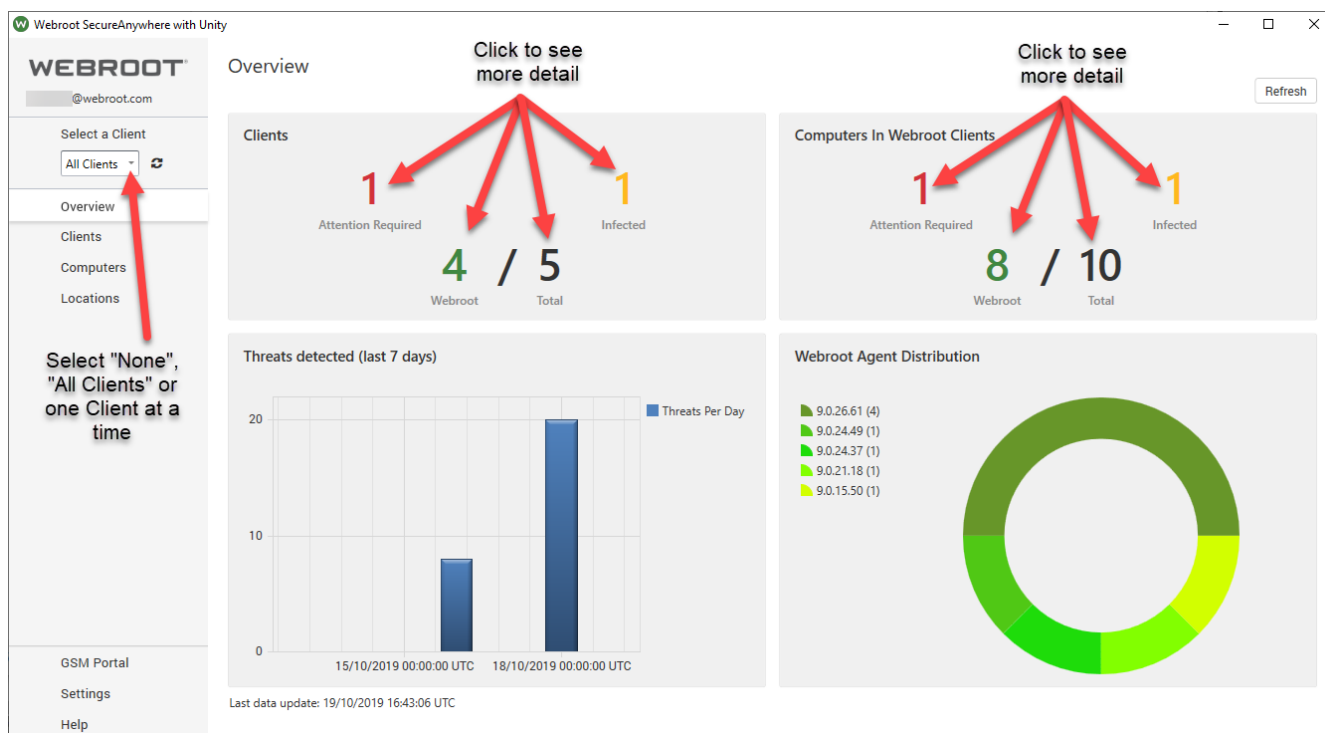
**Note:** This plugin includes a separate Remote Agent plugin dll and should be noted when adding the plugin via the Plugin Manager.

## Dashboard

The dashboard contains everything needed to configure and use the plugin including all options for clients, computers, locations, plugin settings and help links. The client, computer and location pages all contain right click options which are also available in the upper right as Configure and Action options. There are also various filters in the upper right-hand corner to help quickly view only the data desired.

### Overview tab

The Overview tab displays a summary of the overall installation. The user, for example can easily identify if a Client is without Webroot protection and can navigate to the necessary tab for quick configuration, with just a single click. If certain infections have been active for longer than 24 hours, the user is alerted visually with the Attention Required indicator; a single click will navigate the user to the infected computer for further action. Quick navigation is possible from any of the numbers displayed within the “Clients” and “Computers in Webroot Clients” tiles.



Select “None”, “All Clients” (recommended for MSPs with up to 60 Clients) or one Client at a time, recommended for larger MSPs for more efficient working. The selection is persistent if plugin is Closed and re-opened.



## Clients

- **Infected** – This displays the count of clients that contain a computer in the "Infected" state. When the Webroot agent detects a threat, it will block the threat. Most threats, such as real-time or inactive threats are removed in under 1 minute. Some threats require a clean scan before the endpoint is declared malware free. Sometimes, threats are too deeply embedded in the system to be removed immediately without causing system instability and Webroot agent may require a reboot to fully remove the infection. After the usual daily scan and reboot, most infections are automatically and safely removed without any intervention.
- **Attention Required** – Displays the count of clients that contain a computer in the "Attention Required" state. To keep the malware reporting noise down to a minimum, we have created a new "Attention Required" flag specifically designed for MSP environments. This flag is raised if an endpoint remains infected after 2 contiguous 12-hour checks. If the endpoint is rebooted or performs a scan at the point during any of the checks, the counter will be reset for another 12 hours. **In practice, the "Attention Required" flag will be true (1) if the endpoint remains infected after about 36 hours (without being rebooted or shut down).** This ensures the endpoint has gone through at least 1 reboot/scan cycle before raising the "Attention Required" flag. You can choose to take either manual or automatic action if you wish, such as initiating another scan or to inform the end user to reboot. Some actions such as running a reboot request for the user may be automated. See Settings Section.  
**Important Note:** The "Attention Required" flag is distinctly different than the "Needs Attention" state in the Webroot Console, which is set as soon as an infection is detected. Each indicator works independently.
- **Webroot** – This displays the count of clients that are assigned to a Webroot site (has a Webroot site key).
- **Total** – This displays the total count of Automate clients.

## Computers in Webroot Clients

- **Attention Required** – This displays the count of computers in the "Attention Required" state. See "Attention Required" in Clients above for full explanation.
- **Infected** – This displays the count of computers in the "Infected" state. See "Infected" in Clients above for full explanation.
- **Webroot** – This displays the count of computers with Webroot installed that are contained in a CWA client assigned to a Webroot site.
- **Total** – This displays the total count of computers that are contained in a CWA client assigned to a Webroot site.

Note: Only computers that have a Webroot Site key assigned via the Clients tab will be added to the total.

## Threats Detected (last 7 days)

This will display a bar chart with a count of threats detected over the last seven days.

## Webroot Agent Distribution

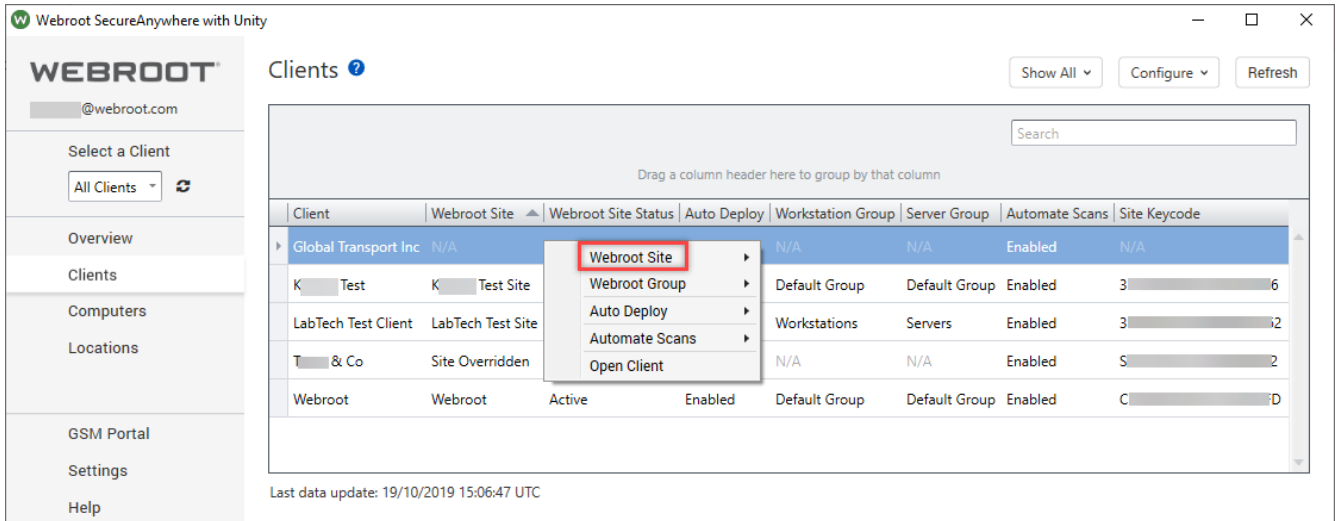
This will display a pie chart with different Webroot software version being identified.

## Clients tab

The Clients tab lists all clients available in ConnectWise Automate and allows easy configuration of Webroot sites. The following options are available within the Clients tab:

- Assigning/Removing a Webroot site
  - Assigning an Existing site to a Client
  - Creating a new site and assigning to a Client
  - Using a non-GSM manually entered site key (**for temporary use only**)
  - Removing a site
- Auto-Installation of new endpoints to
  - Workstation Group
  - Server Group
- Auto-Deploy Enable/Disable at Client Level
- ConnectWise Automate initiated Scans Enable/Disable

## Webroot Site



Webroot SecureAnywhere with Unity

**WEBROOT®**  
@webroot.com

Select a Client  
All Clients

Overview  
Clients  
Computers  
Locations  
GSM Portal  
Settings  
Help

Clients

Show All Configure Refresh

Search

Drag a column header here to group by that column

Client	Webroot Site	Webroot Site Status	Auto Deploy	Workstation Group	Server Group	Automate Scans	Site Keycode
Global Transport Inc	N/A			N/A	N/A	Enabled	N/A
K Test	K Test Site			Default Group	Default Group	Enabled	3 6
LabTech Test Client	LabTech Test Site			Workstations	Servers	Enabled	3 i2
T & Co	Site Overridden			N/A	N/A	Enabled	S 2
Webroot	Webroot	Active	Enabled	Default Group	Default Group	Enabled	C D

Last data update: 19/10/2019 15:06:47 UTC

## Webroot site > Assign an Existing Webroot Site to a Client

If you have already created Sites in the Webroot Global Site Manager (GSM) that match your Automate Clients and there is a 1 to 1 relationship between **CW Automate Clients & Webroot Sites**, you can Assign Webroot Sites to Clients within the plugin. This process is deliberately manual to ensure absolute accuracy. When all Clients are Assigned to Sites, an API connection to the GSM will be established, pulling in correct data and enabling advanced functionality. Please take your time when assigning Clients to Sites, ensure the correct Clients are assigned to correct Sites.

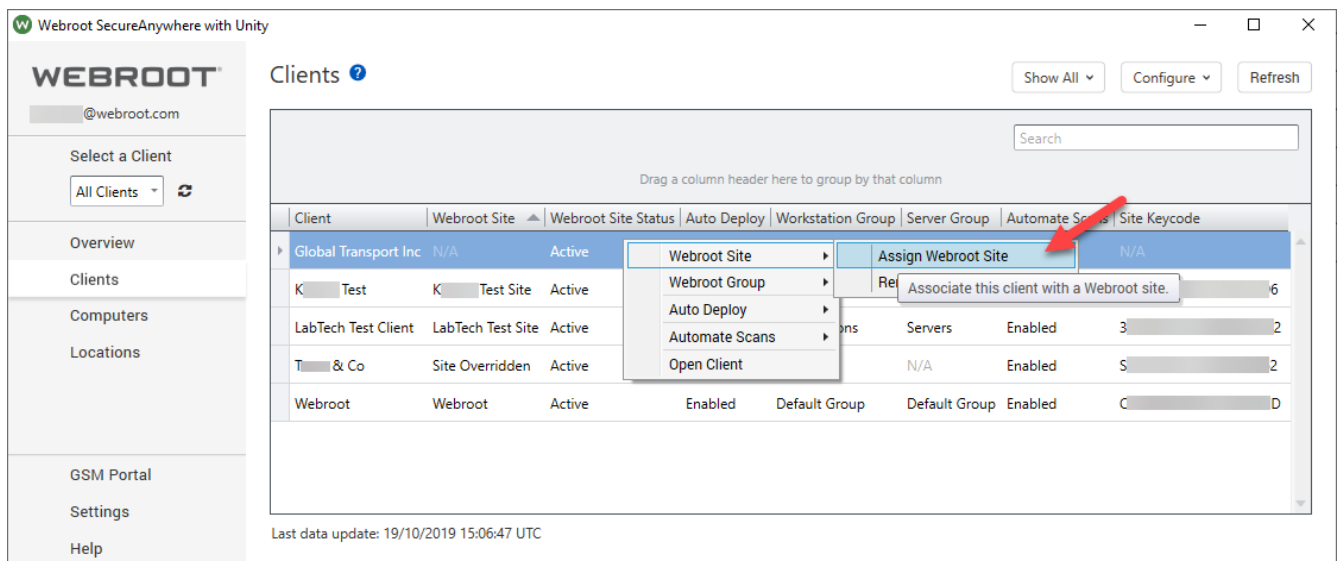
Click on **Clients** tab

Right click on a specific Client

Select **Webroot site**

Select **Assign Webroot site**

Use the drop down menu to assign the correct site (ensure keycode matches the imported key from previous version)



Webroot SecureAnywhere with Unity

WEBSITE: @webroot.com

Select a Client: All Clients

Overview

Clients

Computers

Locations

GSM Portal

Settings

Help

Clients

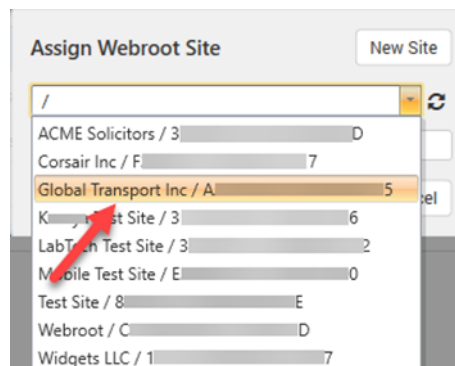
Show All Configure Refresh

Search

Drag a column header here to group by that column

Client	Webroot Site	Webroot Site Status	Auto Deploy	Workstation Group	Server Group	Automate Scans	Site Keycode
Global Transport Inc	N/A	Active					N/A
K Test	K Test Site	Active					
LabTech Test Client	LabTech Test Site	Active					
T & Co	Site Overridden	Active					
Webroot	Webroot	Active	Enabled	Default Group	Default Group	Enabled	C

Last data update: 19/10/2019 15:06:47 UTC



Assign Webroot Site

New Site

/

- ACME Solicitors / 3 D
- Corsair Inc / F 7
- Global Transport Inc / A 5
- K Test Site / 3 6
- LabTech Test Site / 3 2
- Mobile Test Site / E 0
- Test Site / 8 E
- Webroot / C D
- Widgets LLC / 1 7

## Webroot Site > Creating a New Webroot Site and assigning it to a Client

To create Sites directly within the plugin:

Click on **Clients** tab

Right click on a specific Client

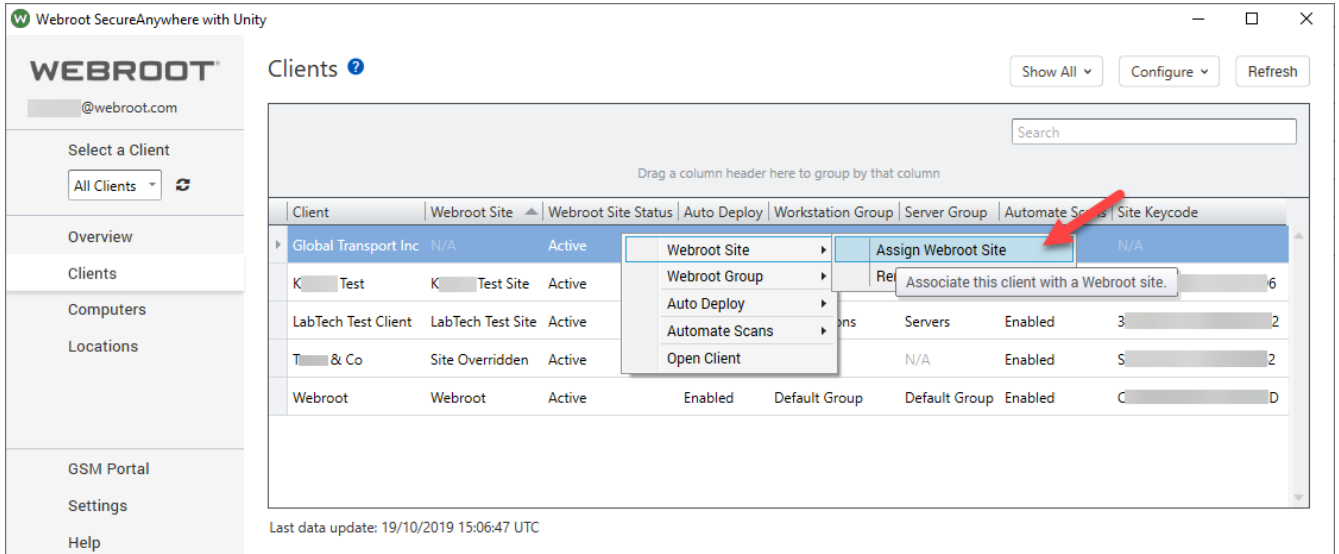
Select **Webroot site**

Select **Assign Webroot site**

Select **New**

Fill in required fields and click **Create**

This process ensures the correct Client name is pulled in automatically from CW Automate reducing errors



Webroot SecureAnywhere with Unity

**WEBROOT®**  
@webroot.com

Select a Client  
All Clients

Overview  
Clients  
Computers  
Locations  
GSM Portal  
Settings  
Help

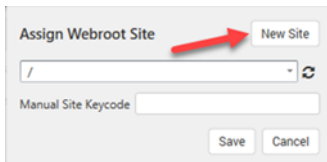
Clients

Search

Drag a column header here to group by that column

Client	Webroot Site	Webroot Site Status	Auto Deploy	Workstation Group	Server Group	Automate Scans	Site Keycode
Global Transport Inc	N/A	Active					N/A
K Test	K Test Site	Active					6
LabTech Test Client	LabTech Test Site	Active					2
T & Co	Site Overridden	Active					2
Webroot	Webroot	Active	Enabled	Default Group	Default Group	Enabled	D

Last data update: 19/10/2019 15:06:47 UTC



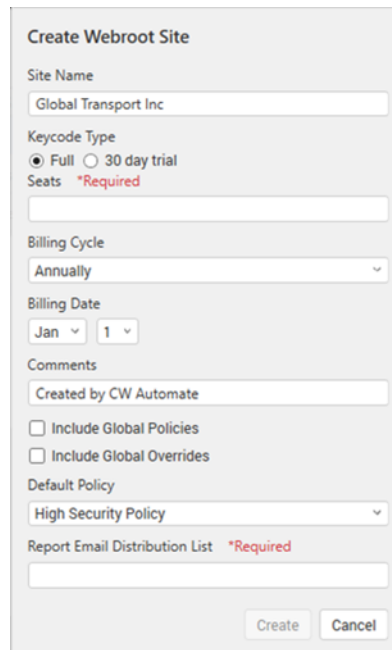
Assign Webroot Site

New Site

/

Manual Site Keycode

Save Cancel



Create Webroot Site

Site Name  
Global Transport Inc

Keycode Type  
☒ Full ☐ 30 day trial

Seats \*Required

Billing Cycle  
Annually

Billing Date  
Jan 1

Comments  
Created by CW Automate

☐ Include Global Policies  
☐ Include Global Overrides

Default Policy  
High Security Policy

Report Email Distribution List \*Required

Create Cancel

**Note:** When a new site is created via the plugin, it may not show up in the site dropdown list immediately. The refresh button may need to be clicked a couple times to reload the updated site list.

## Webroot Site > Use a non-GSM manually entered site key

The plugin allows users to enter a manual keycode for temporary use under exceptional circumstances, such as when a Site is not part of the same Webroot GSM Console as the Unity API or during an upgrade from an older version of the plugin. Users can then deploy endpoints to these sites via the plugin, maintaining backward compatibility with older versions of the plugin.

**NOTE:** Manually entered keys cannot be tied to a GSM Unity API is tied to, advanced functionality using the Unity API will not be possible with manually entered keys weather they are part of a GSM or not and all manually entered keys will be shown as non-GSM within the computers tab.

To use a manually entered site key

Click on **Clients** tab

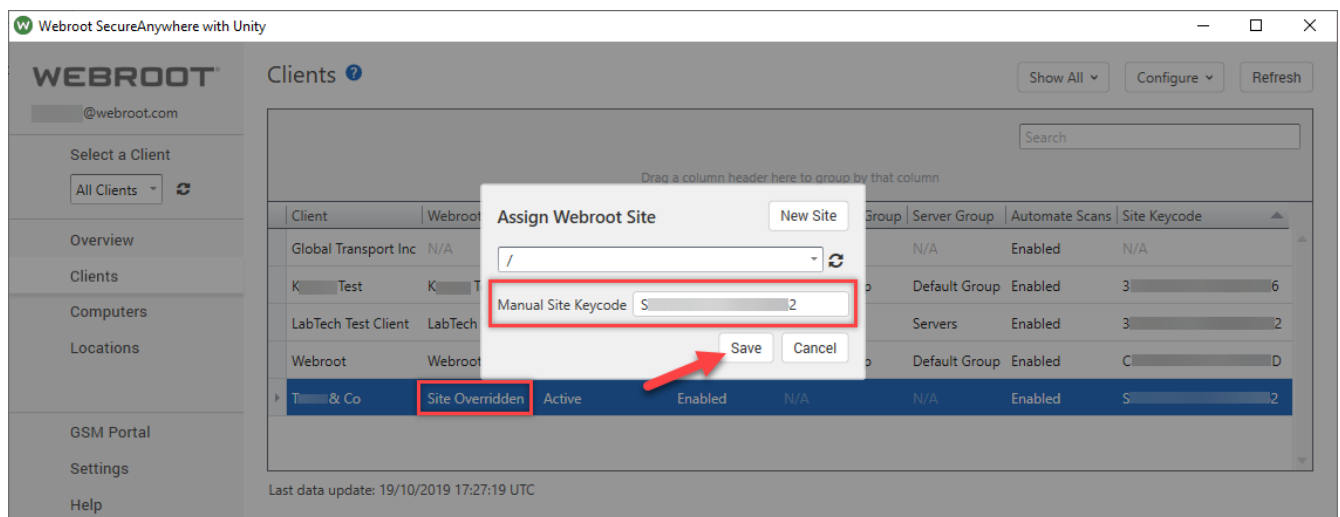
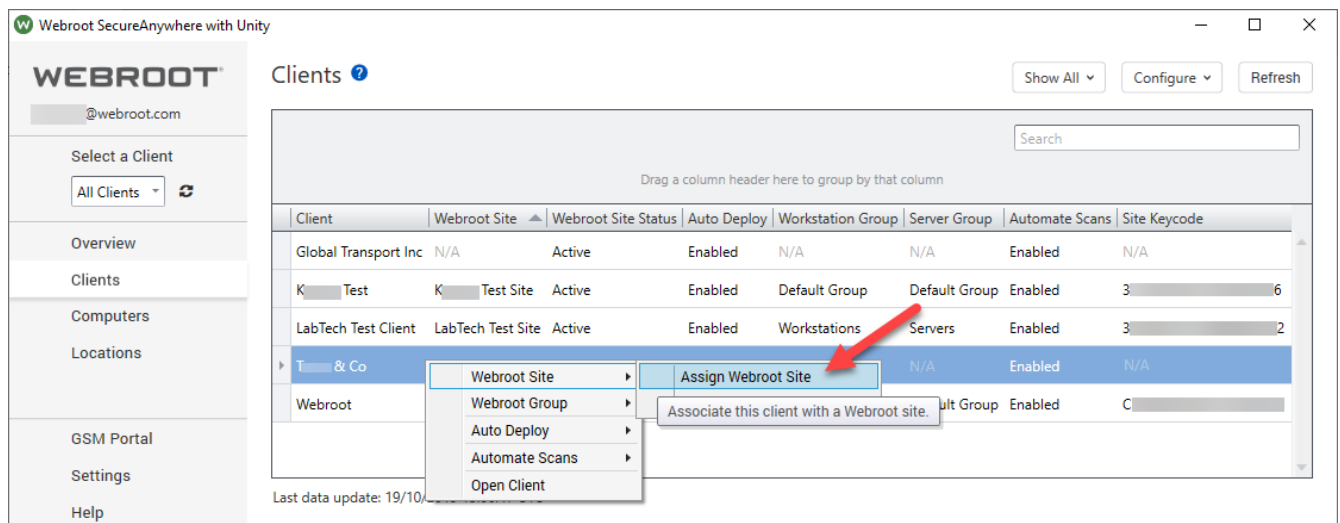
Right click on a specific Client

Select **Webroot site**

Select **Assign Webroot site**

Click within Manual Site Keycode and enter **Manual Keycode**

Click **Save**



Once a manual key is assigned, the **Webroot Site** will show as **Site Overridden**.

## Webroot Site > Remove Webroot Site

To disassociate a Client from the Webroot Site, follow the process below.

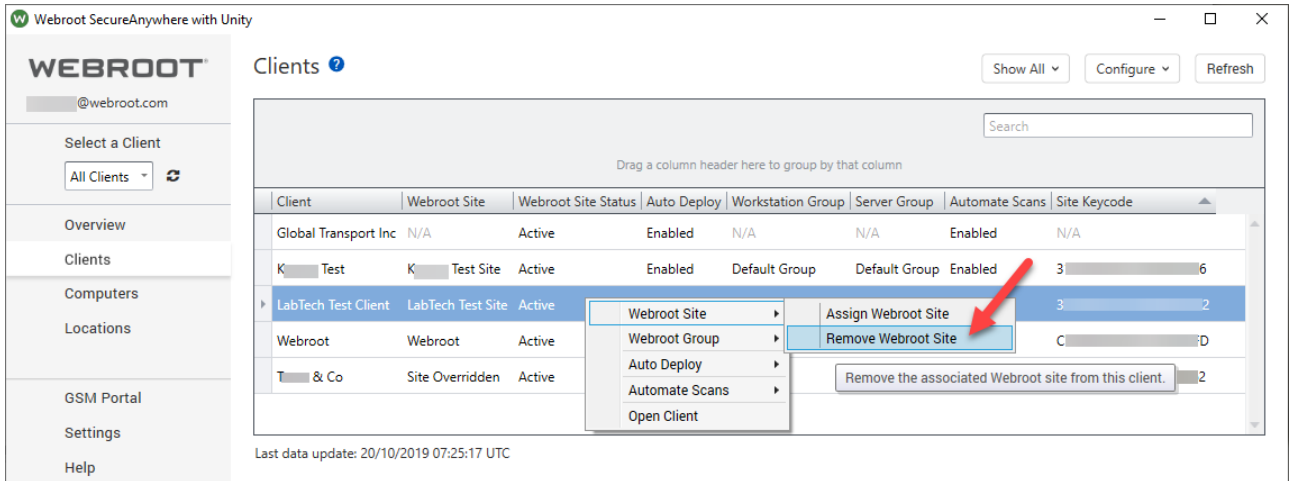
Click on **Clients** tab

Right click on a specific Client

Select **Webroot site**

Select **Remove**

Site will be removed immediately from the plugin



Webroot SecureAnywhere with Unity

**WEBROOT®**  
@webroot.com

Select a Client  
All Clients

Overview  
Clients  
Computers  
Locations  
GSM Portal  
Settings  
Help

Clients

Show All Configure Refresh

Search

Drag a column header here to group by that column

Client	Webroot Site	Webroot Site Status	Auto Deploy	Workstation Group	Server Group	Automate Scans	Site Keycode
Global Transport Inc	N/A	Active	Enabled	N/A	N/A	Enabled	N/A
K Test	K Test Site	Active	Enabled	Default Group	Default Group	Enabled	3 6
LabTech Test Client	LabTech Test Site	Active					3 2
Webroot	Webroot	Active					C D
T & Co	Site Overridden	Active					2

Webroot Site  
Webroot Group  
Auto Deploy  
Automate Scans  
Open Client

Assign Webroot Site  
Remove Webroot Site

Remove the associated Webroot site from this client.

Last data update: 20/10/2019 07:25:17 UTC

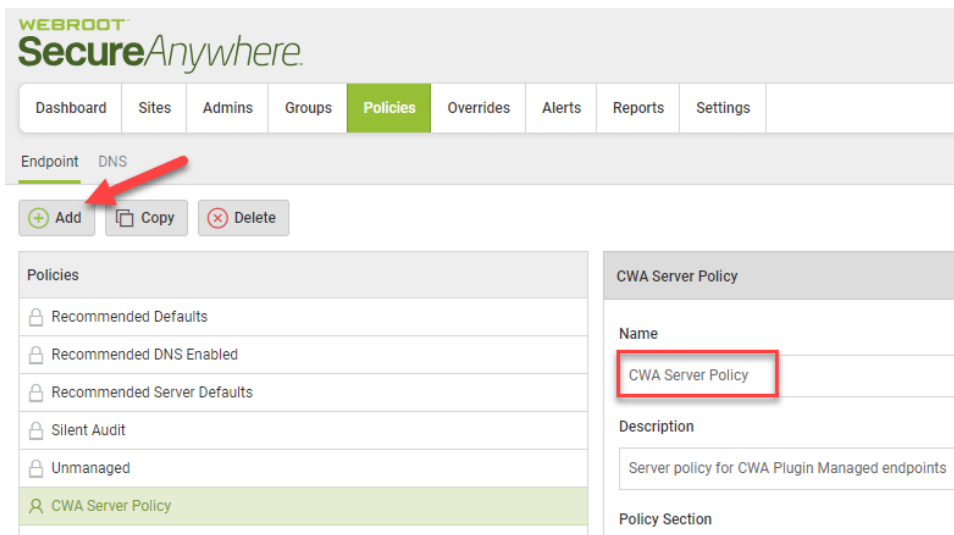
**NOTE:** The Site Removal action does NOT deactivate the site in the GSM and if needed the same site or another site can be associated to a Client again.

## Webroot group – Auto Deploy to Group Policy

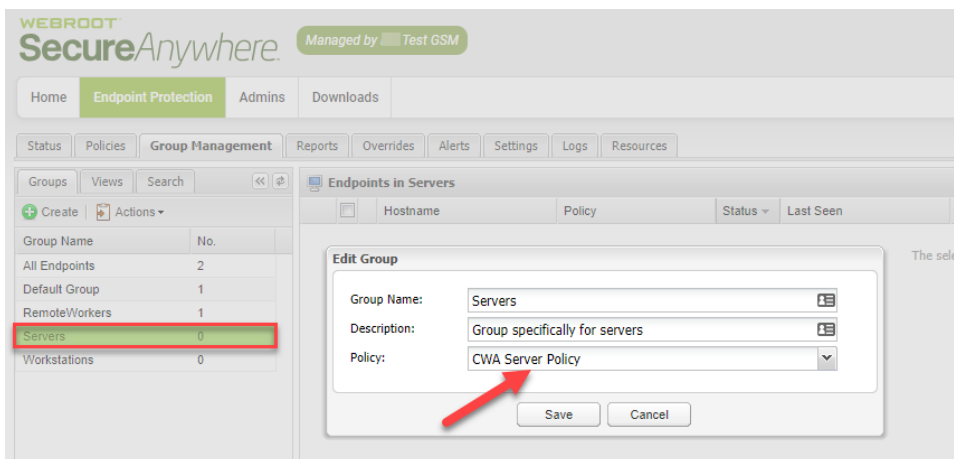
To assign different Webroot policies to Servers and/or Workstations in addition to the Default Webroot Site Policy, specific Webroot Groups can be created in the Webroot Console on a per site basis and those groups can be assigned within the plugin.

Follow the following process to automatically assign Server and Workstation policies when **new computers** are added via the ConnectWise Automate plugin. Note: Existing computers that have registered with the Webroot Console will NOT pick up the group policy, and they will need to have their policy manually changed either in the plugin or in the Webroot Console.

**Step 1** - Create either a new Global Server Policy in the GSM or use the existing Default Server Policy. In the example below, we have created a new Global Server Policy called **CWA Server Policy** within the GSM.



**Step 2** - Create a Server Group in the Site Console and assign a server policy to it, e.g. CWA Server Policy



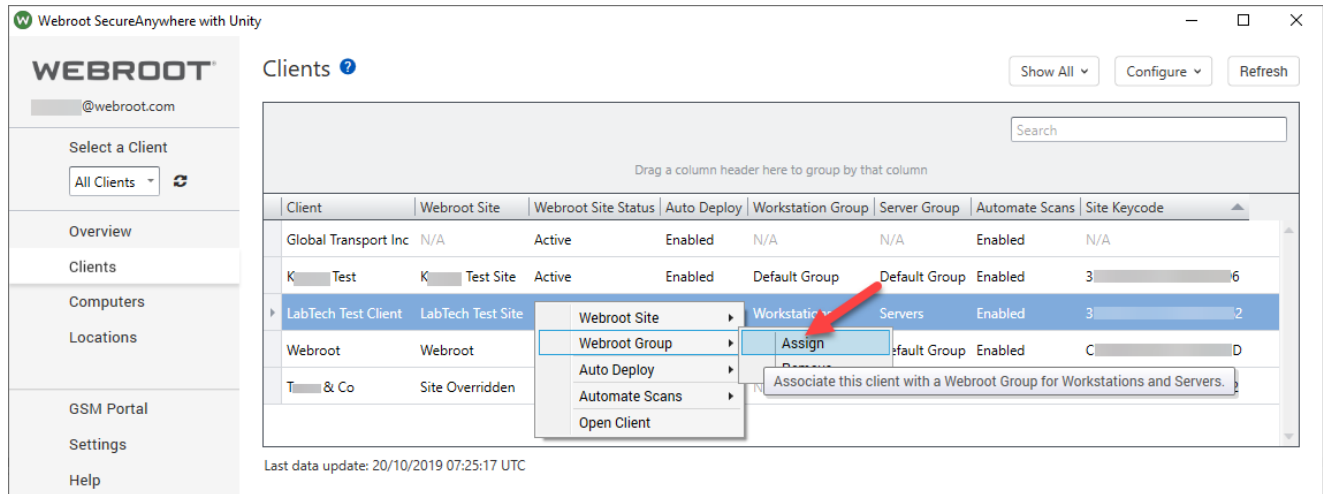
**Step 3** – Assign the new Server Group created in the Webroot Console to the Plugin Server Group.

Click on **Clients** tab

Right click on a specific Client

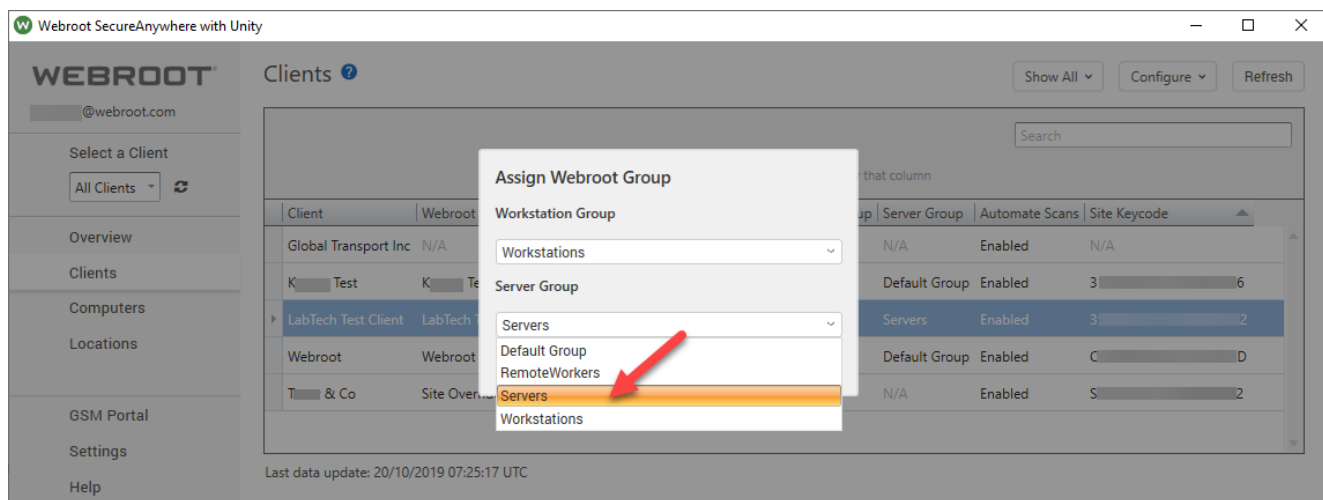
Select **Webroot Group**

Select **Assign**



Click on **Server Group** drop down menu

Select the newly created group (e.g. **Servers**)



Any new Servers will now pick up the CWA Server Policy automatically when Webroot Clients are deployed automatically.

Workstation policies can be assigned in a similar manner or the Workstation policy can be assigned to the Default Site Policy.



## Auto Deploy

The Webroot Automate plugin is designed to automatically install Webroot endpoint security software on endpoints that have the Automate agent software installed. **Auto deploy is Disabled by default at the Location level.** Enabling Auto deploy at Location level will turn on auto deploy for ALL endpoint in that Location. If you wish to restrict the deployment of Webroot security software the specific endpoints, then this must be done at the Computer level by Disabling auto deploy to specific endpoints such as Servers, BEFORE enabling Auto deploy at the Location level.

Auto deploy can be enabled or disabled at three different levels:

Client – Enabled by default  
 Location – **Disabled** by default  
 Computer – Enabled by default

The above arrangement provides complete flexibility in Enabling/Disabling Auto Deploy at any level depending on specific requirements. For example, if you want to accidentally avoid Webroot deployment to a Client, then Disable at Client level as illustrated below.

**NOTE:** Auto deploy will ONLY work if ALL levels are set to Enable.

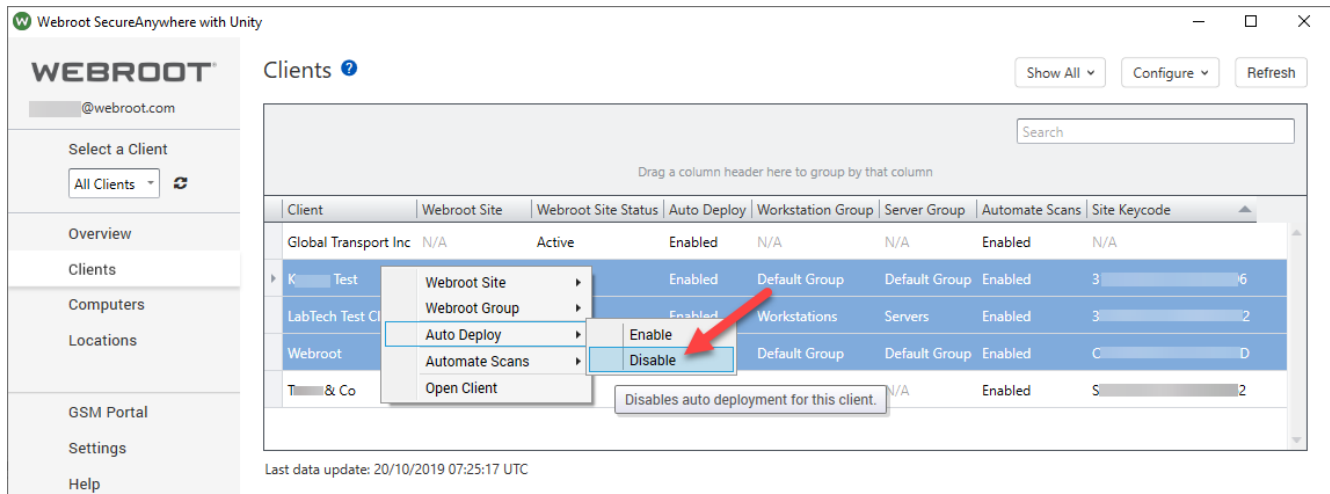
To Enable or Disable Auto Deploy follow the steps below:

Click on **Clients** tab

Right click on a specific Client or highlight a number of Clients as illustrated below

Select **Auto Deploy**

Select **Enable** or **Disable**



Client	Webroot Site	Webroot Site Status	Auto Deploy	Workstation Group	Server Group	Automate Scans	Site Keycode
Global Transport Inc	N/A	Active	Enabled	N/A	N/A	Enabled	N/A
K... Test	Webroot Site	Enabled	Enabled	Default Group	Default Group	Enabled	3...6
LabTech Test Cl	Webroot Group	Enabled	Enabled	Workstations	Servers	Enabled	3...2
Webroot	Auto Deploy	Enable	Disable	Default Group	Default Group	Enabled	C...D
T... & Co	Automate Scans	Disable				Enabled	S...2
	Open Client						

Disables auto deployment for this client.

Last data update: 20/10/2019 07:25:17 UTC

With the above example we have selected 3 Clients and Auto Deploy has been Enabled.

**Note:** If Auto Deploy is disabled at Location or at Computer level, Auto Deploy will not work by just Enabling at Client level.

## Automate scans

You can run Webroot security scans directly within the plugin. If you want the ability to scan any Webroot endpoint from the plugin, then Automate scans must be Enabled.

**Note:** Automate scans are totally independent from Webroot Policy or Webroot Console initiated scans.

Automate scans can be Enabled or Disabled at two different levels:

**Client** – Enabled by default

**Computer** – Enabled by default

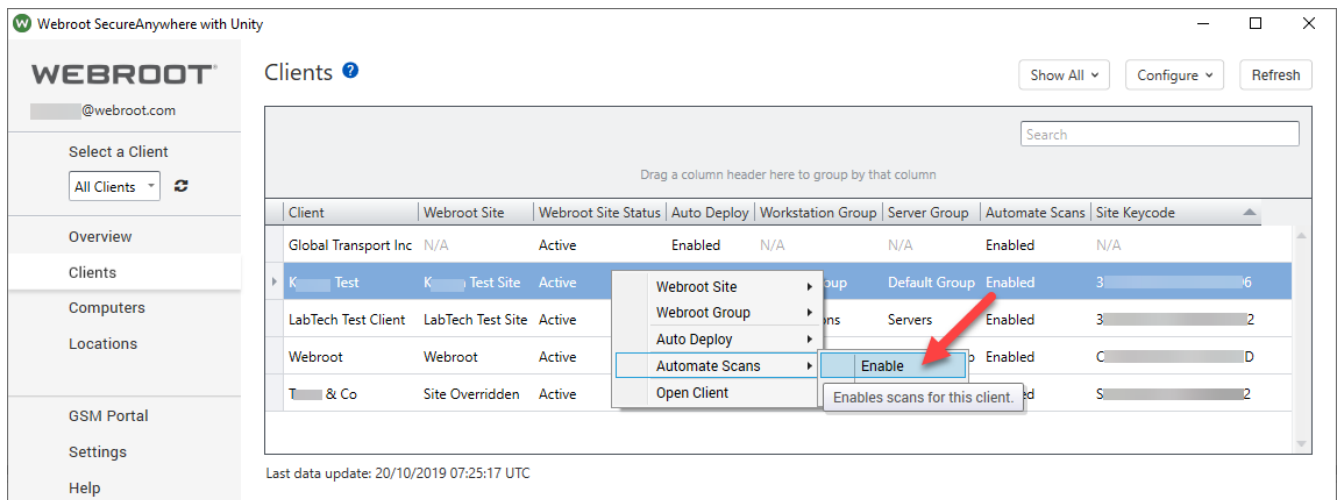
To Enable or Disable ConnectWise Automate plugin initiated scans follow the steps below:

Click on **Clients** tab

Right click on a specific Client or highlight a number of Clients

Select **Automate Scans**

Select **Enable** or **Disable**



Webroot SecureAnywhere with Unity

**WEBROOT®**  
@webroot.com

Select a Client  
All Clients

Overview  
Clients  
Computers  
Locations  
GSM Portal  
Settings  
Help

Clients

Show All Configure Refresh

Search

Drag a column header here to group by that column

Client	Webroot Site	Webroot Site Status	Auto Deploy	Workstation Group	Server Group	Automate Scans	Site Keycode
Global Transport Inc	N/A	Active	Enabled	N/A	N/A	Enabled	N/A
K... Test	K... Test Site	Active	Webroot Site	Group	Default Group	Enabled	3...6
LabTech Test Client	LabTech Test Site	Active	Webroot Group	ns	Servers	Enabled	3...2
Webroot	Webroot	Active	Auto Deploy			Enabled	C...D
T... & Co	Site Overridden	Active	Automate Scans			Enable	S...2

Enables scans for this client.

Last data update: 20/10/2019 07:25:17 UTC

- **Enable** – This will Enable scans from any of the trigger scan ConnectWise Automate scripts or plugin based Webroot agent commands.
- **Disable** – This will Disable scans from any of the trigger scan ConnectWise Automate scripts or plugin based Webroot agent commands.

**Note:** If scans are Disabled on Computer level, it will override the Client level being Enabled or vice versa.

## Computers tab

The computers tab displays all selected computers that have a ConnectWise Automate Client installed and allows you to see a range of Webroot status information. Additionally, it allows the user to initiate a range of actions and configurations, as seen below:

- Webroot agent commands
- Webroot agent policy setting
- Auto deploy
- Automate scans
- Open computer

## Send Agent Command

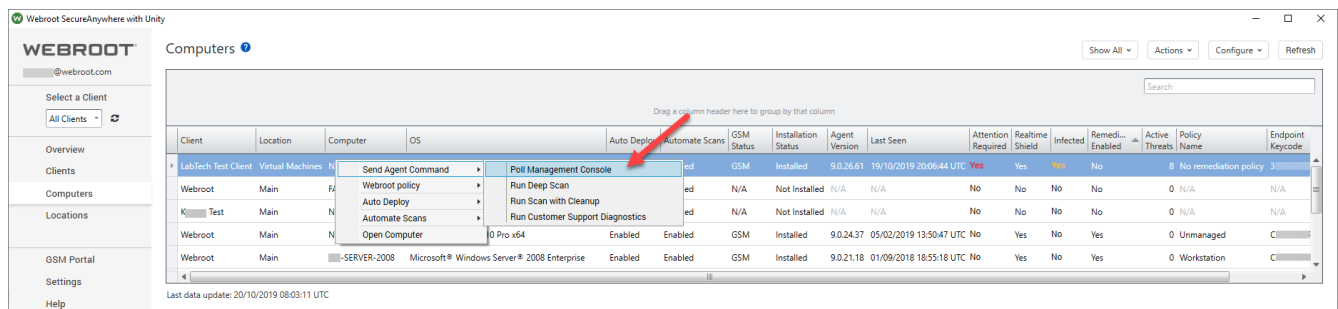
To send an agent command

Click on **Computer** tab

Right click on a specific Computer or highlight a number of Computers

Select **Send Agent Command**

Select one of four commands e.g. **Poll Management Console**



- **Poll Management Console** – This will send a direct Automate command to set the registry key HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\WRData\Actions:UpdateNow value to 1.
- **Run Deep Scan** – This queues the Webroot 3.x - Trigger Deep Scan script to run immediately.  
Note: Automate scans must be Enabled at both Client and Computer level for this action to work.
- **Run Scan with Cleanup** – This queues the Webroot 3.x - Trigger Scan with Cleanup script to run immediately.  
Note: Automate scans must be Enabled at both Client and Computer level for this action to work.
- **Run Customer Support Diagnostics** – This will prompt for an e-mail address, auto filling with the logged in user's saved e-mail address, then queue the Webroot 3.x - Customer Support Diagnostics script to run immediately.

## Webroot Policy

You can set or change a Webroot policy permanently or temporarily from the ConnectWise Automate plugin, on one or more endpoints at the same time. The policy will be applied to the computer almost immediately.

To set a new policy

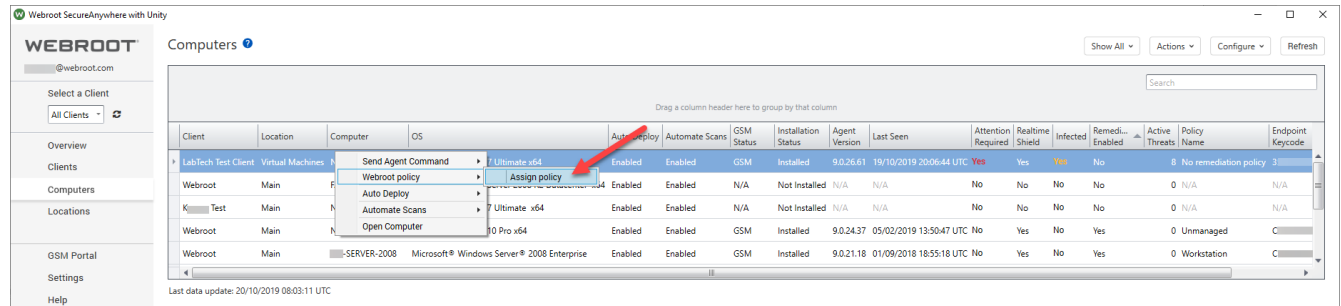
Click on **Computer** tab

Right click on a specific Computer or highlight a number of Computers

Select **Webroot Policy**

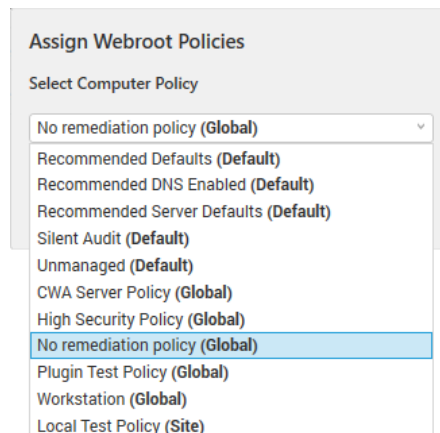
Select **Assign Policy**

Select the policy **Poll Management Console**



Click the drop down menu

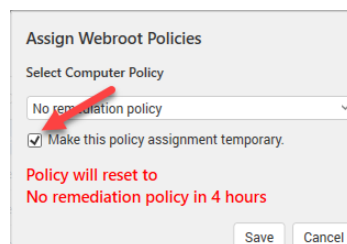
Click on the policy to be assigned e.g. **No remediation policy**



**NOTE:** There are different policy types such as Local, Default & Global. If multiple Computers are selected, only the policies that are common across ALL computers will be shown.

If you wish to set a policy **temporarily**, then

Check the box **Make this policy assignment temporary**



The policy assignment will go back to the original setting indicated in red within 4 hours.

## Auto Deploy

The Automate plugin is designed to automatically install Webroot endpoint security software whenever an Automate client is installed. Auto deploy is **Enabled** by default at the **Computer** level. Enabling Auto deploy at Location level will turn on auto deploy for ALL endpoints at that Location. If you wish to restrict the deployment of Webroot security software on specific endpoints, then this must be done at the Computer level by Disabling auto deploy to specific endpoints such as Servers, BEFORE enabling Auto deploy at the Location level.

Auto deploy can be enabled or disabled at three different levels:

Client – Enabled by default  
Location – **Disabled** by default  
Computer – Enabled by default

The above arrangement provides complete flexibility in Enabling/Disabling Auto Deploy at any level depending on specific requirements.

**NOTE:** Auto deploy will ONLY work if ALL levels are set to **Enable**.

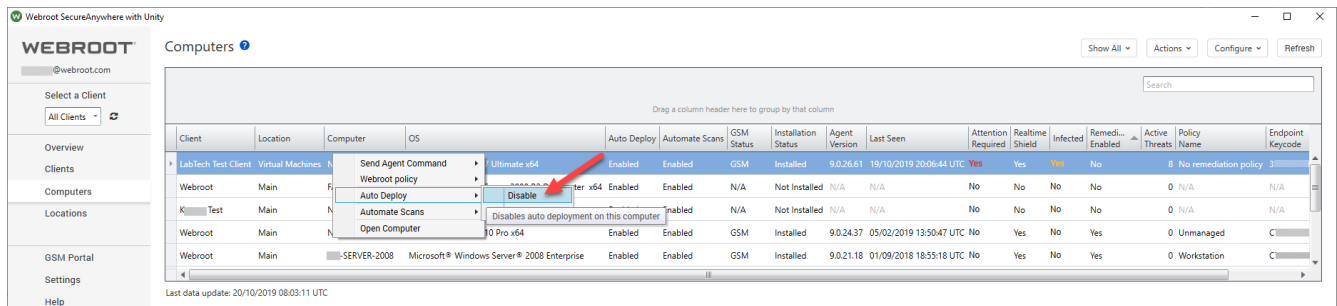
To Enable or Disable Auto Deploy follow the steps below:

Click on **Computers** tab

Right click on a specific Computer or highlight a number of Computers

Select **Auto Deploy**

Select **Enable** or **Disable**



Client	Location	Computer	OS	Auto Deploy	Automate Scans	GSM Status	Installation Status	Agent Version	Last Seen	Attention Required	Realtime Shield	Infected	Remediation	Active Threats	Policy Name	Endpoint Keycode
LabTech Test Client	Virtual Machines	Send Agent Command	Ultimate x64	Enabled	Enabled	GSM	Installed	9.0.26.61	18/10/2019 20:06:44 UTC	Yes	Yes	Yes	No	0	No remediation policy	3
Webroot	Main	Webroot policy	Ultimate x64	Enabled	Enabled	N/A	Not Installed	N/A	N/A	No	No	No	No	0	N/A	N/A
Webroot	Main	Auto Deploy	Ultimate x64	Enabled	Enabled	N/A	Not Installed	N/A	N/A	No	No	No	No	0	N/A	N/A
Webroot	Main	Automate Scans	Ultimate x64	Enabled	Enabled	GSM	Installed	9.0.24.37	05/02/2019 13:50:47 UTC	No	Yes	No	Yes	0	Unmanaged	C
Webroot	Main	Open Computer	10 Pro x64	Enabled	Enabled	GSM	Installed	9.0.21.18	01/09/2018 18:55:18 UTC	No	Yes	No	Yes	0	Workstation	C

- **Disable** – This will exclude the selected computer/s from automatic installation of the Webroot software.
- **Enable** – This will enable automatic installation of the Webroot software on the selected computer/s.

## Automate scans

You can run Webroot security scans directly within the plugin. If you want the ability to scan any Webroot endpoint from the plugin, then Automate scans must be Enabled.

**Note:** Automate scans are totally independent from Webroot Policy or Webroot Console initiated scans.

Automate scans can be Enabled or Disabled at two different levels:

**Client** – Enabled by default

**Computer** – Enabled by default

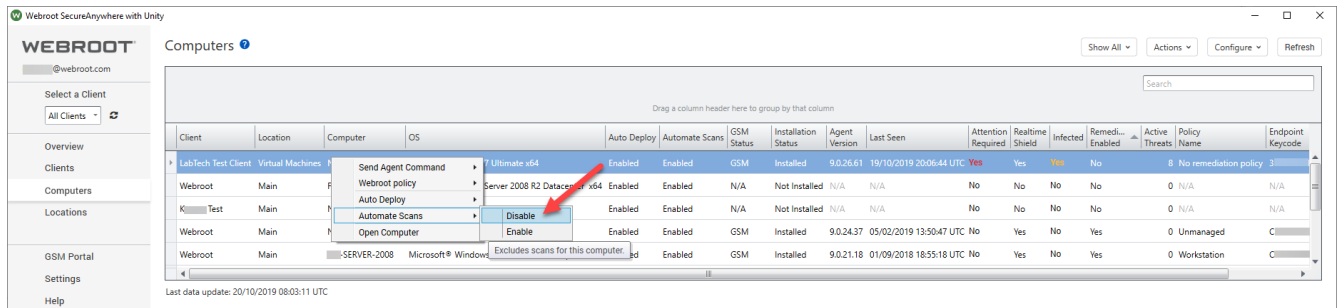
To Enable or Disable ConnectWise Automate plugin initiated scans follow the steps below:

Click on **Computer** tab

Right click on a specific Computer or highlight a number of Computers

Select **Automate Scans**

Select **Enable** or **Disable**



The screenshot shows the Webroot console interface. On the left is a sidebar with navigation options: Overview, Clients, Computers, Locations, GSM Portal, Settings, and Help. The main area is titled 'Computers' and contains a table of system information. A right-click context menu is displayed over one of the rows, with options including 'Send Agent Command', 'Webroot policy', 'Auto Deploy', 'Automate Scans', and 'Open Computer'. The 'Automate Scans' option is expanded, showing 'Disable' and 'Enable' sub-options. A red arrow points to the 'Disable' option. The table columns include Client, Location, Computer, OS, Auto Deploy, Automate Scans, GSM Status, Installation Status, Agent Version, Last Seen, Attention Required, Realtime Shield, Infected, Remediation, Active Threats, Policy Name, and Endpoint Keycode.

- **Enable** – This will Enable scans from any of the trigger scan ConnectWise Automate scripts or plugin based Webroot agent commands.
- **Disable** – This will Disable scans from any of the trigger scan ConnectWise Automate scripts or plugin based Webroot agent commands.

**Note:** If scans are Disabled on Computer level, it will override the Client level being Enabled or vice versa.

## Locations

The locations dashboard allows you to set Auto Deployment options, as well as directly open the location from the dashboard.

## Auto Deploy

The Automate plugin is designed to automatically install Webroot endpoint security software whenever an Automate client is installed. Auto deploy is **Enabled** by default at **Computer** level. Enabling Auto deploy at Location level will turn on auto deploy for ALL endpoints in that Location. If you wish to restrict the deployment of Webroot security software the specific endpoints, then this must be done at the Computer level by Disabling auto deploy to specific endpoints such as Servers, BEFORE enabling Auto deploy at the Location level.

Auto deploy can be enabled or disabled at three different levels:

Client – Enabled by default

Location – **Disabled** by default

Computer – Enabled by default

The above arrangement provides complete flexibility in Enabling/Disabling Auto Deploy at any level depending on specific requirements.

NOTE: Auto deploy will ONLY work if ALL levels are set to **Enable**.

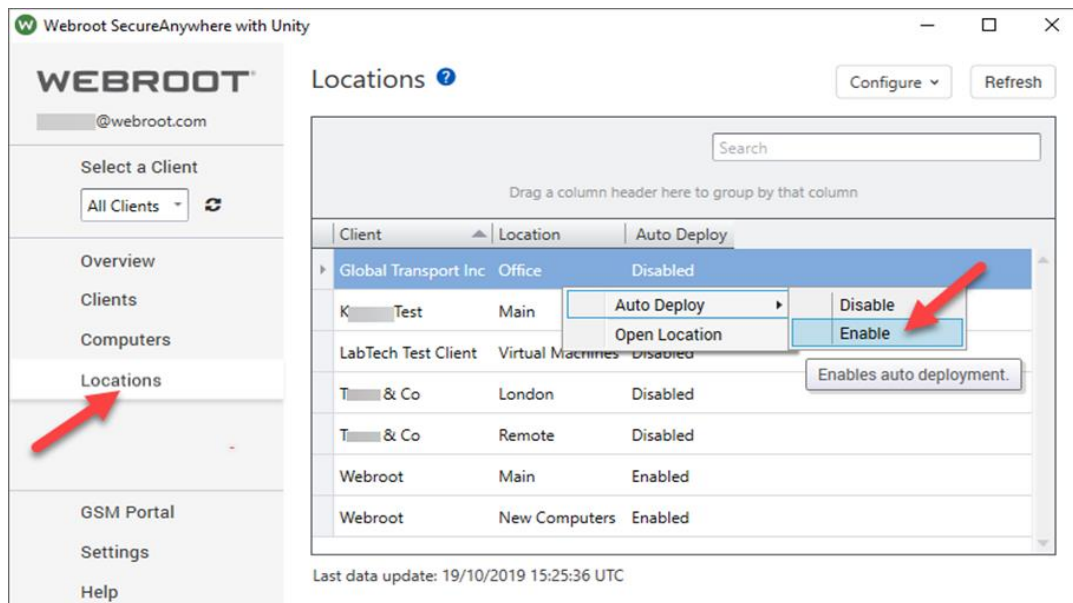
To Enable or Disable Auto Deploy follow the steps below:

Click on **Location** tab

Right click on a specific Location or highlight a number of Locations

Select **Auto Deploy**

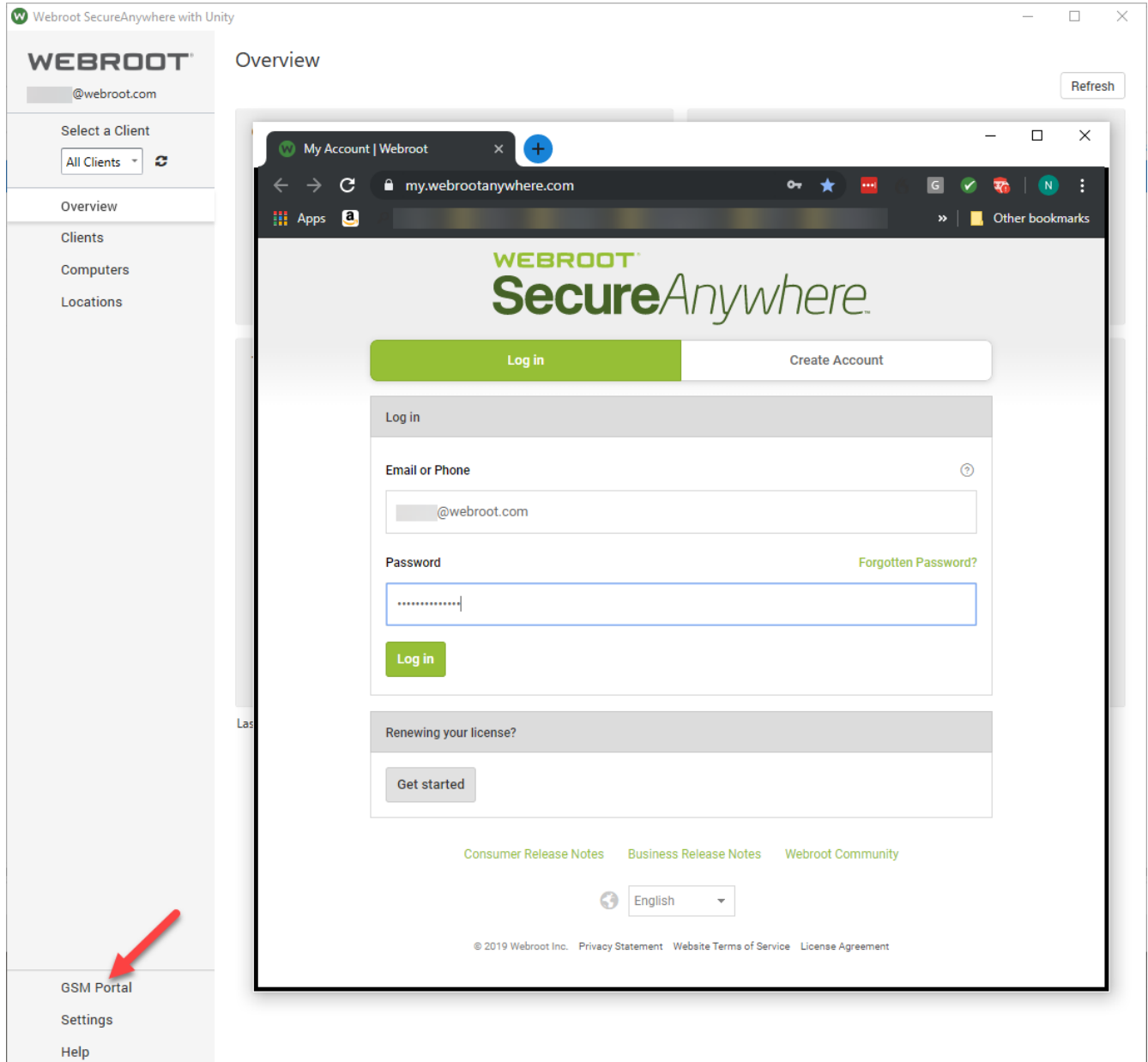
Select **Enable** or **Disable**



- **Disable** – This will exclude the selected Location/s from automatic installation of the Webroot software.
- **Enable** – This will enable automatic installation of the Webroot software on the selected Location/s.

## GSM Portal

This feature launches the default system browser to the URL <https://my.webrootanywhere.com/> to allow additional admin tasks from the GSM console.





## Settings

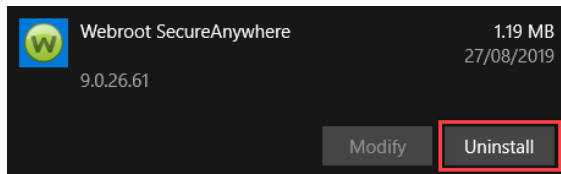
The settings tab allows you to enter the Webroot Unity API credentials as well as set a number of additional alerts and actions.

### API Authentication

Allows the ability to enter and save Webroot Unity API credentials. Please click [here](#) for a video explanation.

### Webroot Agent

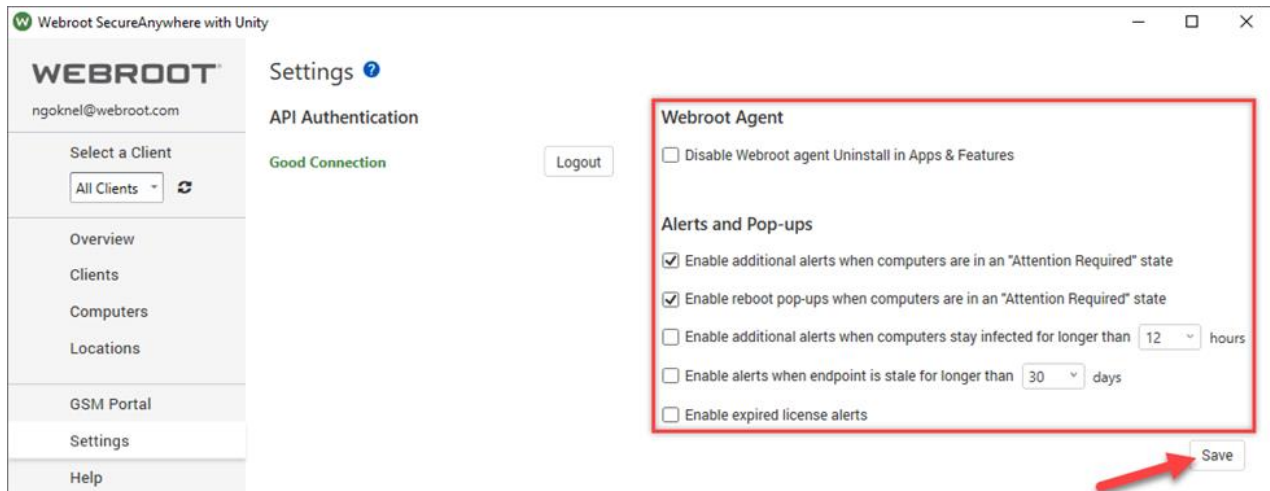
The **Disable Webroot agent Uninstall in Apps & Features** setting, when checked removes the Uninstall feature within Windows.



**NOTE:** This feature is OFF by default and is only applied **during installation of the Webroot agent**.

### Alerts and Pop-ups

Alerts and Pop-ups will allow you to enable/disable alerts from monitors.



- **Enable additional alerts when computers are in an “Attention Required” state**

Tied to the “Webroot 3 – Attention Required” monitor that will create an actionable ticket for techs.

To keep the malware reporting noise down to a minimum, we have created a new “Attention Required” alert specifically designed for MSP environments. This alert is raised if an endpoint remains infected after 2 contiguous 12-hour checks from the point of infection detection. If the endpoint is switched off during one of the 12-hour checks or in the process of performing a scan at the end of a 12 check, the counter will be reset for another 12 hours. In practice, the “Attention Required” alert will be true if the endpoint remains infected after about 36 hours. This ensures the endpoint has gone through at least 1 reboot/scan cycle before raising the Attention Required flag.

**Important Note:** The “Attention Required” flag in the plugin is distinctly different than the “Needs Attention or Devices Requiring Attention” state in the Webroot Console, which is set as soon as an infection is detected. Each indicator works independently.

- **Enable reboot pop-ups when computers are in an “Attention Required” state**

Tied to the “Webroot 3 – Attention Required” monitor that will create an actionable ticket for techs.

Sometimes, for the Webroot agent to fully remediate a persistent threat, or to declare an endpoint free of malware, one or more reboot cycles may be needed. If users do not shutdown their PCs overnight then it could remain infected. Enabling the “reboot pop-up alert” after the “Attention Required” flag is set will ensure a pop-up alert is sent to the end users’ device at midday, informing the user to reboot.

- **Enable additional alerts when computers stay infected for longer than x hours**

Tied to the “Webroot 3 – Active Infection” monitor that will create an actionable ticket for techs.

When a Webroot agent stays infected for longer than the amount of hours defined (2, 8, 12, 24) an additional alert will be triggered via the “Webroot - Active Infection” Internal Monitor. This alert is useful for customers who need to be informed of persistent infections as quickly as possible.

- **Enable alerts when endpoint is stale for longer than x days**

Tied to the “Webroot 3 – Stale Agents” monitor that will create an actionable ticket for techs.

If a Webroot agent fails to successfully check-in to the Webroot cloud for longer than the days defined (7, 15, 30, 60, 90) an alert will be triggered via the “Webroot - Stale Agents” Internal Monitor.

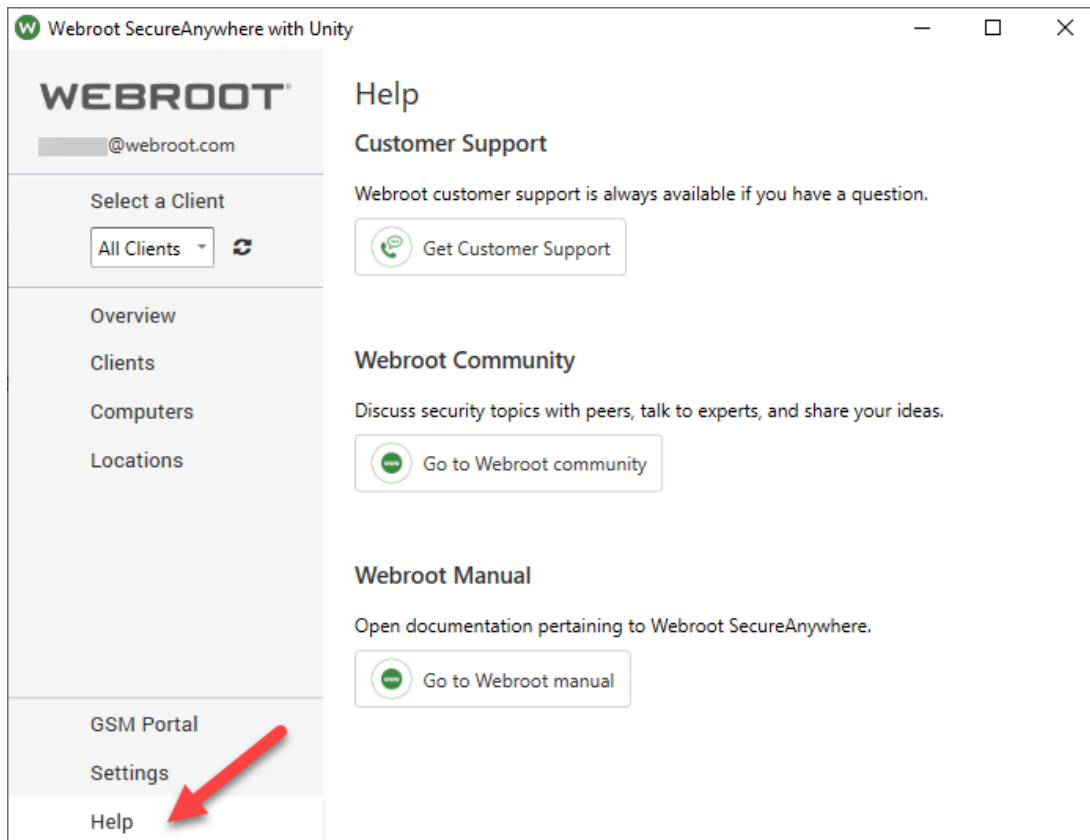
- **Enable expired license alerts**

Tied to the “Webroot 3 – License Expired” monitor that will create an actionable ticket for techs.

When a Webroot agent’s license expires it will trigger an alert via the “Webroot - License Expired” Internal Monitor. Under normal circumstances all licenses are tied to the GSM Parent Key and should not expire, however, if you notice this alert, then it could indicate an issue with the endpoint.

## Help

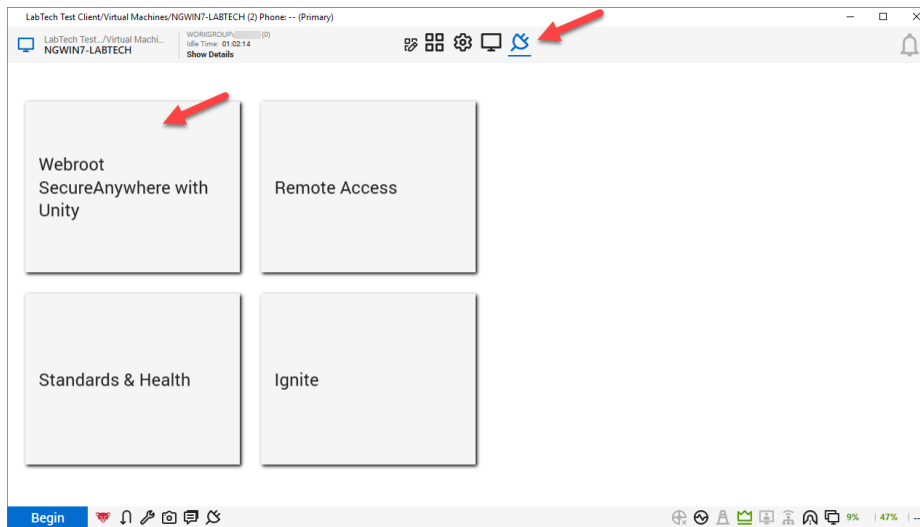
- **Customer Support** – The Get Customer Support button opens the systems default browser to:  
<http://www.webrootanywhere.com/howcanwehelpbusiness.asp>
- **Webroot Community** – The Go to Webroot Community button opens the systems default browser to:  
<https://community.webroot.com/t5/Business/ct-p/ent0>
- **Webroot Manual** – The Go to Webroot Manual button opens the PDF manual page in the default reader:  
[https://download.webroot.com/RMM/Webroot\\_Integration\\_for\\_ConnectWise\\_Automate\\_User\\_Guide\\_v3-0.pdf](https://download.webroot.com/RMM/Webroot_Integration_for_ConnectWise_Automate_User_Guide_v3-0.pdf)



## Computer Plugin Page

The computer plugin page provides additional details about the endpoint state such as shield status, scan statistics and agent status. Endpoint specific settings such as auto deploy, automate scans and endpoint policy can also be set.

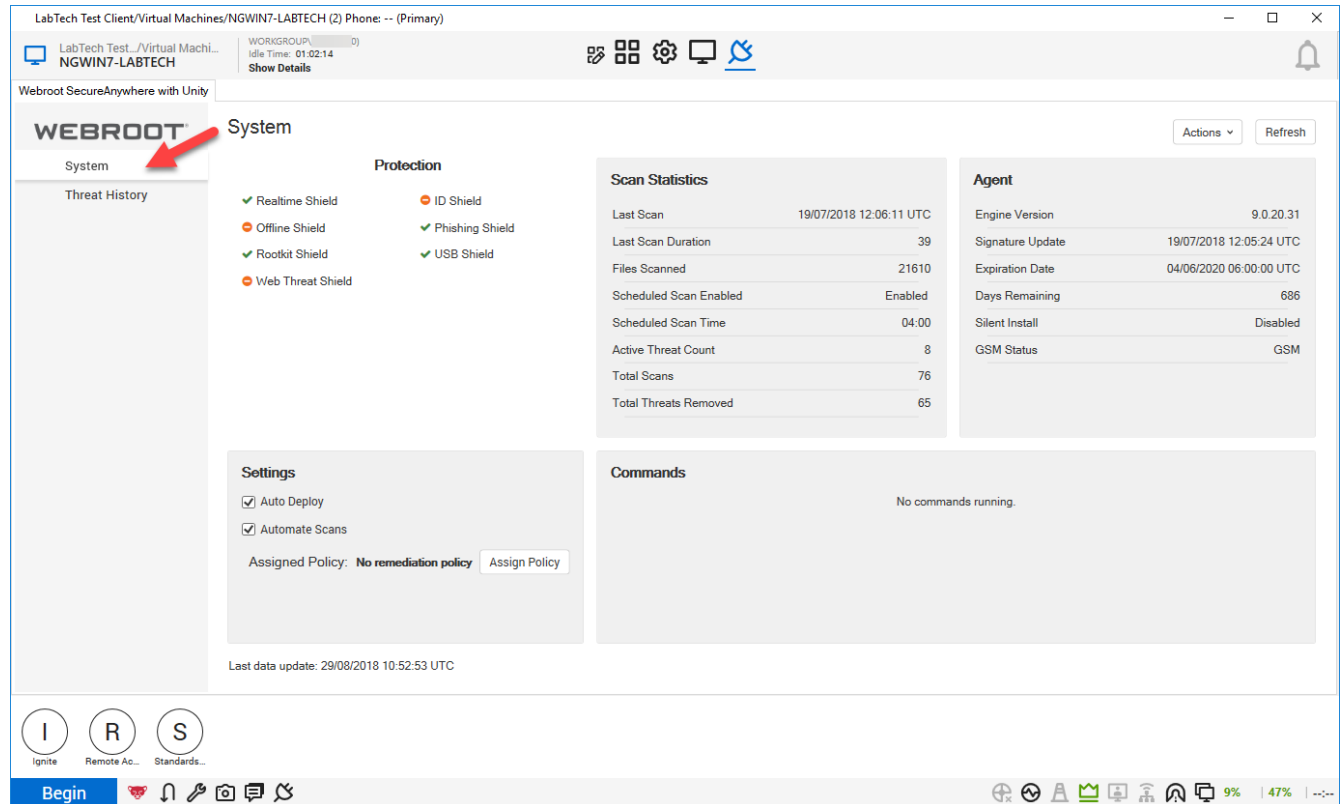
To access the Computer plugin page, open a specific computer either within the Webroot plugin, for example, by double clicking on a computer and then click on the plugin icon and select Webroot SecureAnywhere with Unity



The computer plugin page is broken into two parts, System and Threat History.

## System

This page contains details about the Webroot agent, gives the ability to Enable Auto Deploy and Automate Scans, set a permanent or temporary Webroot Policy, as well as issue all Webroot agent commands available in the plugin via the Action drop down menu.



LabTech Test Client/Virtual Machines/NGWIN7-LABTECH (2) Phone: -- (Primary)

LabTech Test Client/Virtual Machines/NGWIN7-LABTECH

WORKGROUP\... Idle Time: 01:02:14 Show Details

Webroot SecureAnywhere with Unity

**WEBROOT®** System

System Threat History

**Protection**

- Realtime Shield
- Offline Shield
- Rootkit Shield
- Web Threat Shield
- ID Shield
- Phishing Shield
- USB Shield

**Scan Statistics**

Last Scan	19/07/2018 12:06:11 UTC
Last Scan Duration	39
Files Scanned	21610
Scheduled Scan Enabled	Enabled
Scheduled Scan Time	04:00
Active Threat Count	8
Total Scans	76
Total Threats Removed	65

**Agent**

Engine Version	9.0.20.31
Signature Update	19/07/2018 12:05:24 UTC
Expiration Date	04/06/2020 06:00:00 UTC
Days Remaining	686
Silent Install	Disabled
GSM Status	GSM

**Settings**

- ☒ Auto Deploy
- ☒ Automate Scans

Assigned Policy: **No remediation policy** Assign Policy

**Commands**

No commands running.

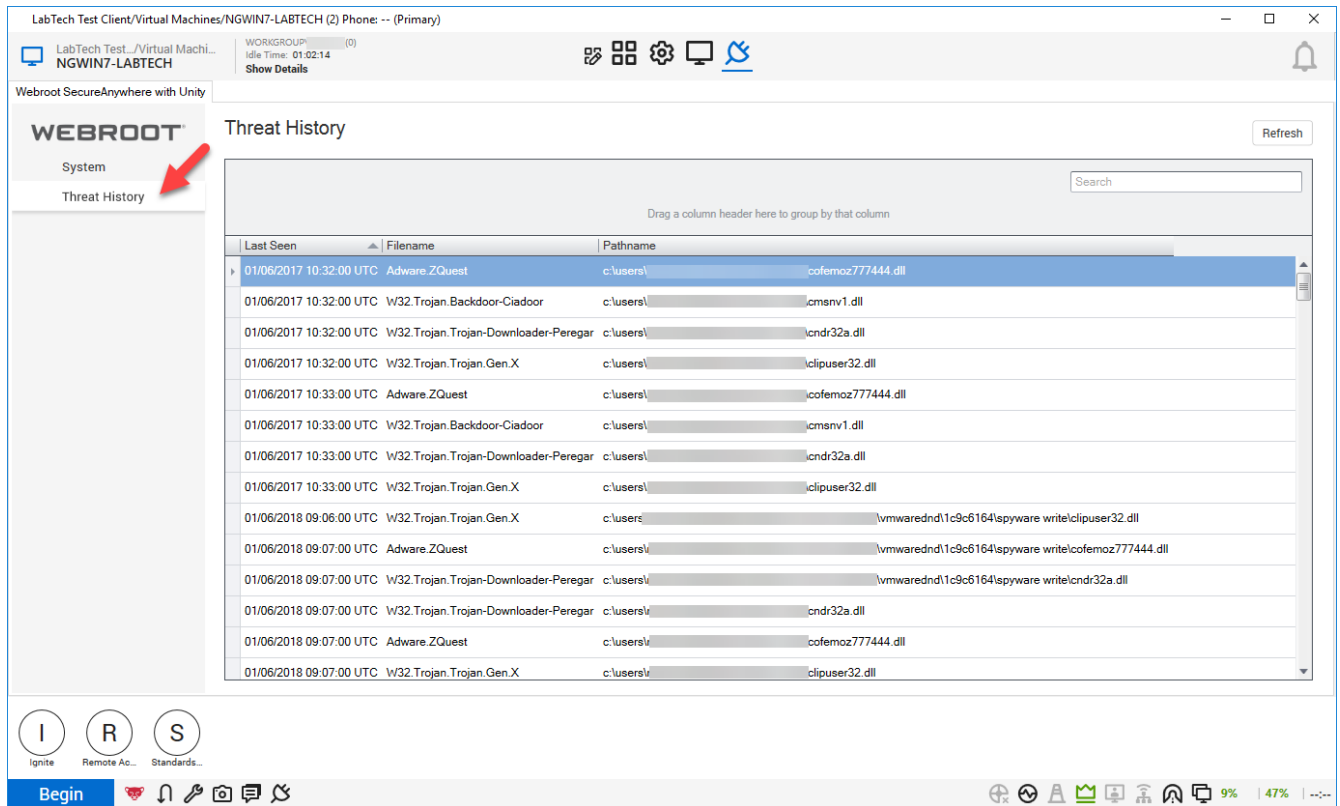
Last data update: 29/08/2018 10:52:53 UTC

Ignite Remote Ac... Standards...

Begin

## Threat History

This contains all threat information and details on that Webroot agent.



LabTech Test Client/Virtual Machines/NGWIN7-LABTECH (2) Phone: -- (Primary)

WORKGROUP: (0)  
Idle Time: 01:02:14  
Show Details

Webroot SecureAnywhere with Unity

**WEBROOT**

System

Threat History

Threat History

Refresh

Search

Drag a column header here to group by that column

Last Seen	Filename	Pathname
01/06/2017 10:32:00 UTC	Adware.ZQuest	c:\users\...\cofemoz777444.dll
01/06/2017 10:32:00 UTC	W32.Trojan.Backdoor-Ciador	c:\users\...\cmenv1.dll
01/06/2017 10:32:00 UTC	W32.Trojan.Trojan-Downloader-Peregar	c:\users\...\cndr32a.dll
01/06/2017 10:32:00 UTC	W32.Trojan.Trojan.Gen.X	c:\users\...\clipuser32.dll
01/06/2017 10:33:00 UTC	Adware.ZQuest	c:\users\...\cofemoz777444.dll
01/06/2017 10:33:00 UTC	W32.Trojan.Backdoor-Ciador	c:\users\...\cmenv1.dll
01/06/2017 10:33:00 UTC	W32.Trojan.Trojan-Downloader-Peregar	c:\users\...\cndr32a.dll
01/06/2017 10:33:00 UTC	W32.Trojan.Trojan.Gen.X	c:\users\...\clipuser32.dll
01/06/2018 09:06:00 UTC	W32.Trojan.Trojan.Gen.X	c:\users\...\vmwarendnd1c9c6164\spyware\write\clipuser32.dll
01/06/2018 09:07:00 UTC	Adware.ZQuest	c:\users\...\vmwarendnd1c9c6164\spyware\write\cofemoz777444.dll
01/06/2018 09:07:00 UTC	W32.Trojan.Trojan-Downloader-Peregar	c:\users\...\vmwarendnd1c9c6164\spyware\write\cndr32a.dll
01/06/2018 09:07:00 UTC	W32.Trojan.Trojan-Downloader-Peregar	c:\users\...\cndr32a.dll
01/06/2018 09:07:00 UTC	Adware.ZQuest	c:\users\...\cofemoz777444.dll
01/06/2018 09:07:00 UTC	W32.Trojan.Trojan.Gen.X	c:\users\...\clipuser32.dll

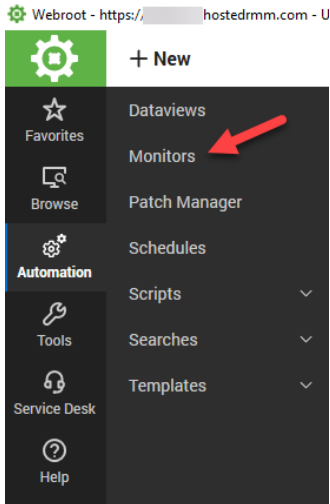
Ignite Remote Ac... Standards...

Begin

9% 47%

## Monitors

1. With the plugin installed, from the Main Toolbar of the Automate Control Center, click the **Monitors** button.

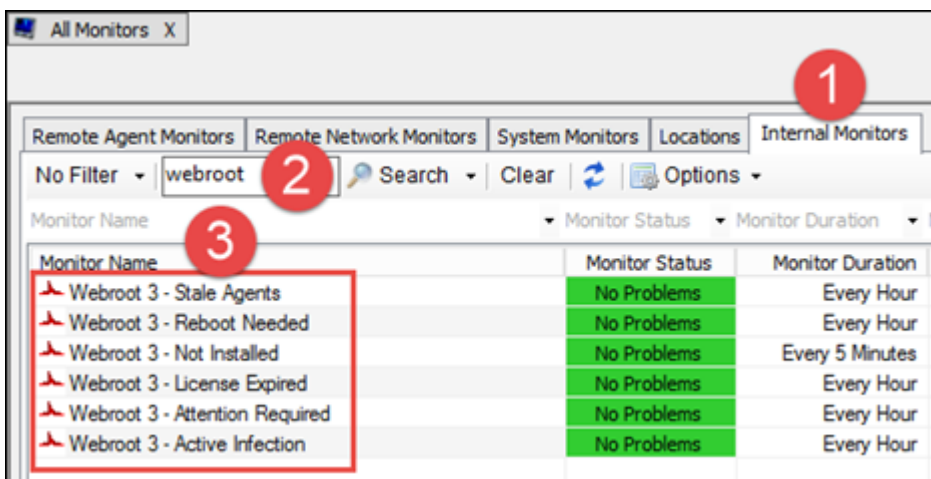


This will display all the Automate monitors.

2. Click the **Internal Monitors** tab.
3. Filter on webroot.

You should see six monitors:

- Webroot 3 - Stale Agents
- Webroot 3 - Reboot Needed
- Webroot 3 - Not Installed
- Webroot 3 - License Expired
- Webroot 3 - Attention Required
- Webroot 3 - Active Infection



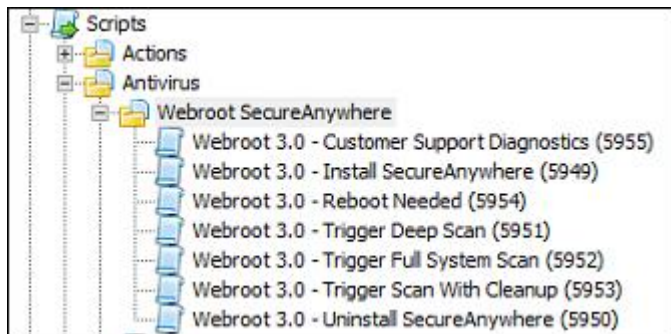
## CW Automate Group

The ConnectWise Automate group created is Webroot SecureAnywhere and will contain all computers from the Automate system that have Webroot installed on them. It's a sub-group of Antivirus Management group.

## Scripts

The CWA scripts created are:

- Webroot 3.x - Customer Support Diagnostics
- Webroot 3.x - Install SecureAnywhere
- Webroot 3.x - Reboot Needed
- Webroot 3.x - Trigger Deep Scan
- Webroot 3.x - Trigger Full System Scan
- Webroot 3.x - Trigger Scan With Cleanup
- Webroot 3.x - Uninstall SecureAnywhere





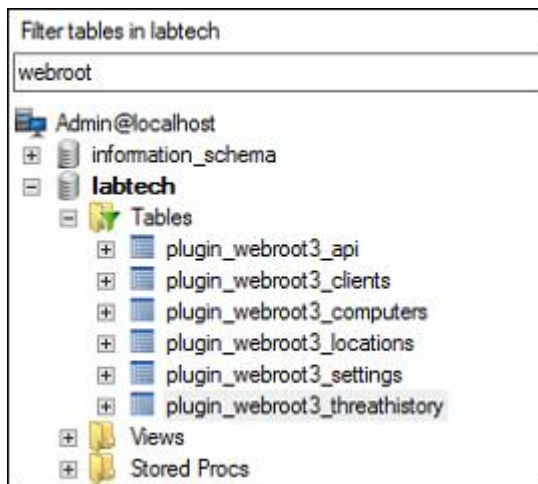
## Database Tables

If you have direct access to your database, you can verify the needed table were created.

The following database tables should have been created:

- plugin\_webroot3\_api
- plugin\_webroot3\_clients
- plugin\_webroot3\_computers
- plugin\_webroot3\_locations
- plugin\_webroot3\_settings
- plugin\_webroot3\_threathistory

Each database table has a default settings row. All checkboxes are saved as 0 or 1 in the database (0 = unchecked, 1 = checked). The default settings row data should match the settings page.

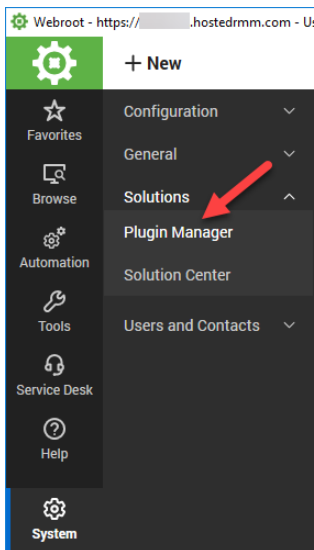
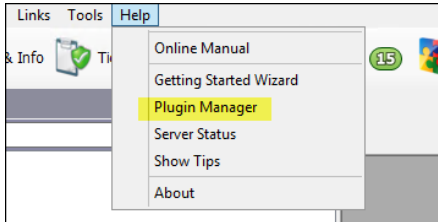


## Adding/Updating Plugin via Plugin Manager

To add or update a plugin via the LabTech Plugin Manager follow these steps in the LabTech Control Center.

**To add or update the plugin:**

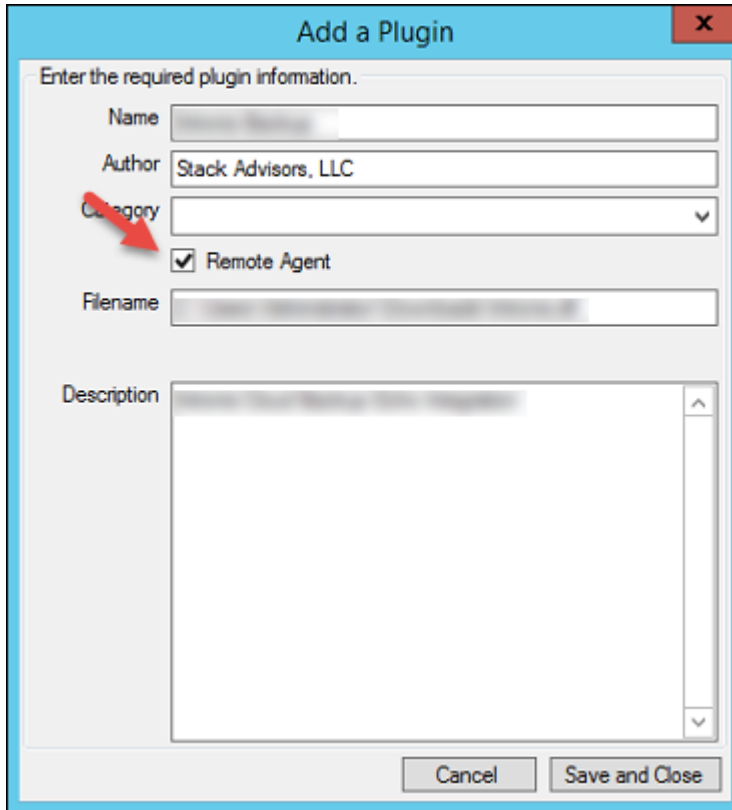
1. Log in to the LabTech Control Center.
2. From the Help menu, select **Plugin Manager**.



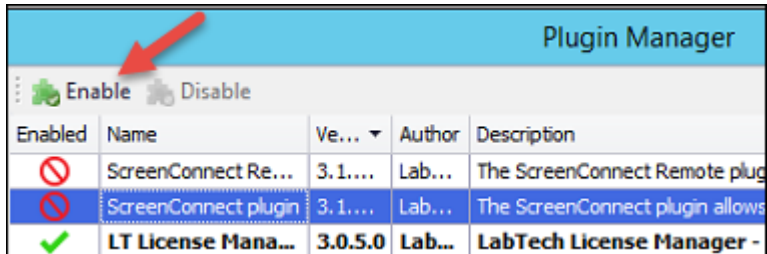
3. Select **Advanced -> Manage Plugins -> Add Plugin or Update Plugin**.



- When adding a new plugin — If it has Remote agent functionality, you must select the Remote Agent checkbox before clicking the Save and Close button.



- When adding a new plugin — After the plugin is added and displays in the Plugin Manager, select the plugin, then click the Enable icon.

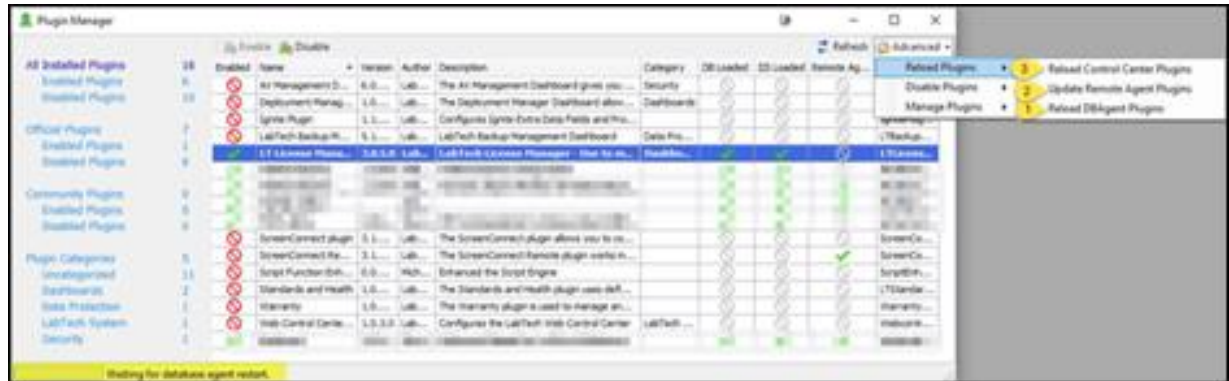


Enabled	Name	Ve...	Author	Description
	ScreenConnect Re...	3.1....	Lab...	The ScreenConnect Remote plug
	ScreenConnect plugin	3.1....	Lab...	The ScreenConnect plugin allows
	LT License Mana...	3.0.5.0	Lab...	LabTech License Manager -

- When updating a plugin, you must select the desired plugin in the table.
- Reload the Plugins. This will ensure the plugin has fully loaded on the server and remote systems.

5. Select **Advanced -> Reload Plugins -> Reload DBAgent Plugins**, then select **Update Remote Agent Plugins**, then select **Reload Control Center Plugins**.

- The order in which the reloads happen should be as described.
- When the Remote Agent and DBAgent are updated/reloaded it will restart the database agent, wait for that to finish restarting before moving on to the next update/reload.



## Known issues

There are no known issues with this release.