

COMODO
CYBERSECURITY



**SECURE INTERNET
GATEWAY**

Comodo Secure Internet Gateway

Software Version 2.13

Administrator Guide

Guide Version 2.13.100620

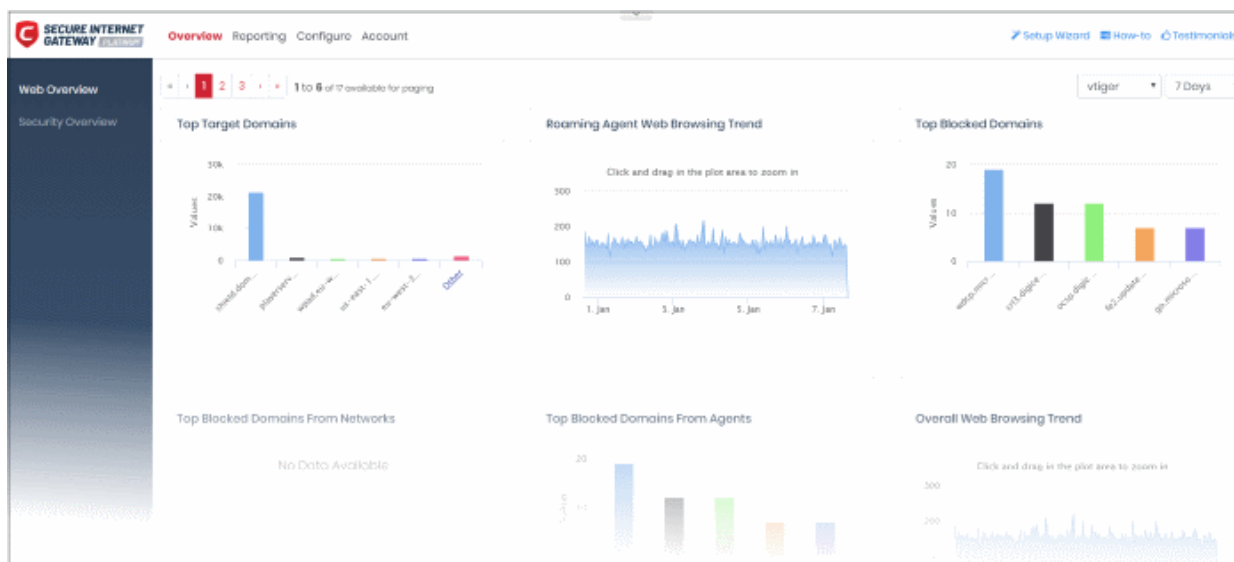
Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction to Comodo Secure Internet Gateway	3
1.1 Purchase a License	4
1.2 Login to Secure Internet Gateway	18
1.3 Setup Options Explained	19
1.3.1 Tutorial to Add Networks to Secure Internet Gateway	19
1.3.2 Tutorial to Add Roaming Endpoints to Secure Internet Gateway	22
1.3.3 Tutorial to Add Mobile Devices	23
1.3.4 Tutorial to Deploy CSIG Virtual Appliances	24
1.3.5 Setup Wizard - Add Networks	26
1.3.6 Setup Local Resolver Virtual Machines and Import Sites	30
2 The Admin Console	38
3 The Dashboard	41
3.1 Web Overview	41
3.2 Security Overview	64
3.3 View Logs	73
4 Add Networks, Roaming Endpoints and Mobile Devices	76
4.1 Add Networks	77
4.2 Add Roaming Endpoints	85
4.3 Add Mobile Devices	97
4.4 Manage Imported Sites and Virtual Appliances	118
4.4.1 Add Internal Networks	120
4.4.2 Add Internal Domains	124
5 Manage CSIG Rules	127
5.1 Manage Security Rules	128
5.2 Manage Category Rules	131
5.3 Manage Domain Blacklist and Whitelist	135
5.4 Manage Block Pages	141
5.5 Manage Cloud Browser Settings	158
6 Apply Policies to Networks and Roaming/Mobile Devices	161
7 Domain Classification Requests	168
8 View Protection Details by Customer	174
9 Reports	174
10 Read Testimonials	176
11 View Account Details	177
About Comodo Security Solutions	179

1 Introduction to Comodo Secure Internet Gateway

Comodo Secure Internet Gateway (CSIG) is an enterprise web filtering solution that provides comprehensive, DNS based security for networks of all sizes. The solution scans all inbound and outbound web traffic to provide real time protection against the latest threats. CSIG also features advanced reporting, custom B/W lists and a granular policy manager which allows you to create location-specific policies.



Features

- Default rules which provide blanket protection from malware, botnets and harmful sites for networks and roaming/mobile devices.
- Website categories which make it easy to create a custom filtering policy.
- Create your own domain blacklists and whitelists.
- Configure rules so your users can visit websites in a virtual session. Virtual sessions protect the host machine from attacks from blocked/harmful websites.
- Fast import of networks and roaming devices. Local resolvers can encrypt and forward DNS queries from endpoints to Secure Internet Gateway DNS servers.
- Advanced reporting grants full visibility of events on your Secure Internet Gateway perimeter.
- Easy to setup. Just set your DNS servers to Secure Internet Gateway.

Guide Structure

This guide takes you through the configuration and use of Secure Internet Gateway and is broken down into the following main sections:

- **Introduction**
 - **Purchase a License**
 - **Login to Secure Internet Gateway**
 - **Setup Options Explained**
 - **Tutorial to Add Networks to Secure Internet Gateway**
 - **Tutorial to Add Roaming Endpoints to Secure Internet Gateway**
 - **Tutorial to Add Mobile Devices**

- **Tutorial to Deploy CSIG Virtual Appliances**
- **Setup Wizard - Add Networks**
- **Setup Local Resolver Virtual Machines and Import Sites**
- **The Admin Console**
- **The Dashboard**
 - **Web Overview**
 - **Security Overview**
 - **View Logs**
- **Add Networks, Roaming Endpoints and Mobile Devices**
 - **Add Networks**
 - **Add Roaming Endpoints**
 - **Add Mobile Devices**
 - **Manage Imported Sites and Virtual Appliances**
 - **Add Internal Networks**
 - **Add Internal Domains**
- **Manage CSIG Rules**
 - **Manage Security Rules**
 - **Manage Category Rules**
 - **Manage Domain Blacklist and Whitelist**
 - **Manage Block Pages**
 - **Manage Cloud Browser Settings**
- **Apply Policies to Networks and Roaming / Mobile Devices**
- **Domain Classification Requests**
- **View Protection Details by Customer**
- **Reports**
- **Read Testimonials**
- **View Account Details**

1.1 Purchase a License

Two types of license are available for Secure Internet Gateway:

- **Gold** - Free for enterprises and MSPs.
- **Platinum** - Paid version with several additional features

Click here to compare packages.

There are two ways to obtain a license:

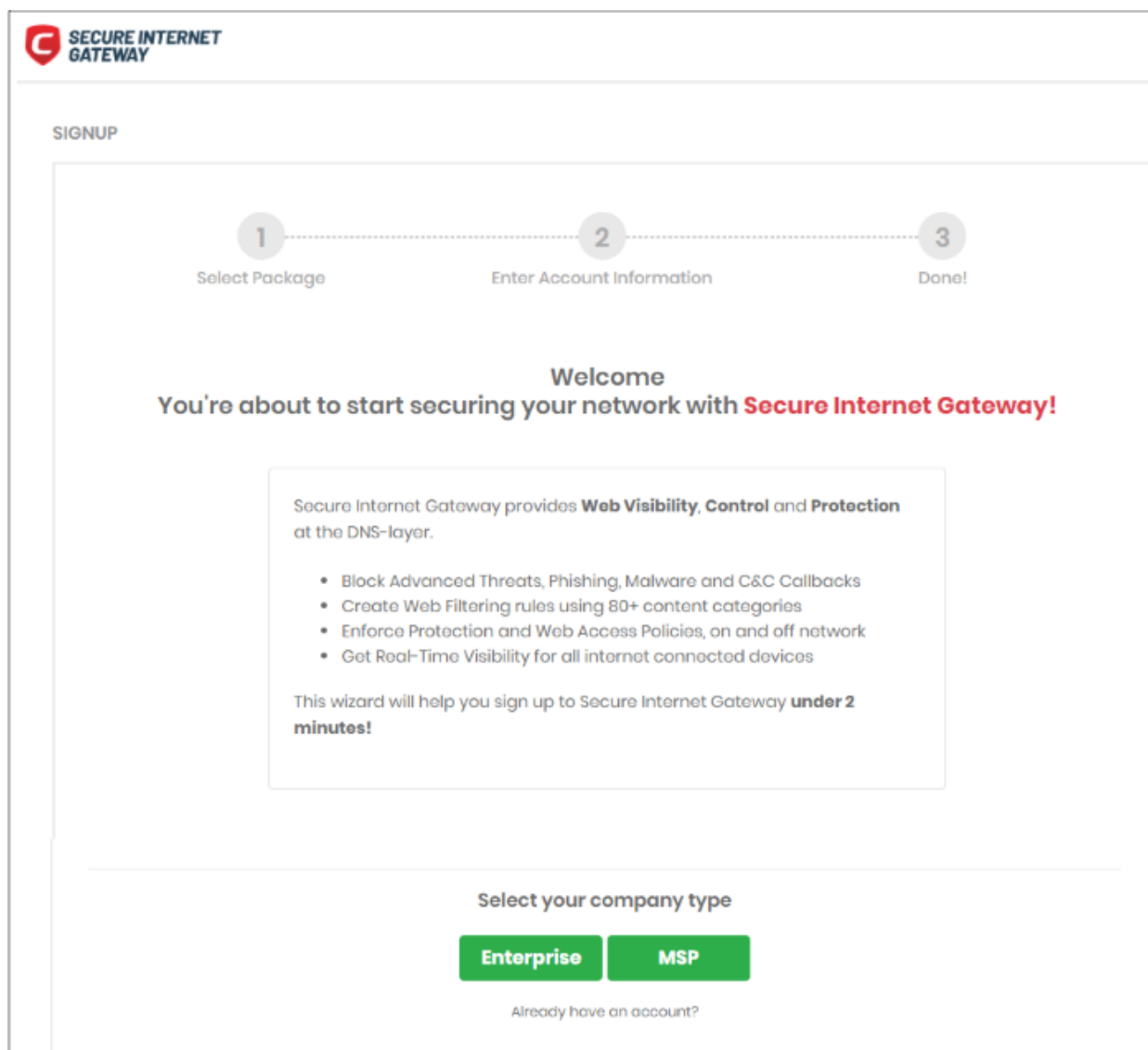
- **Stand-alone customers** - Sign-up for a free license at <https://cdome.comodo.com/dns-internet-security.php>.
- **Comodo One / Itarian / Dragon customers** (enterprise and MSP licenses) - Secure Internet Gateway is automatically activated in your account

Stand-alone Customers:

Sign up for a Gold license

- Visit <https://cdome.comodo.com/dns-internet-security.php>.
- Click 'Start Now'

- You are taken to the sign-up page:



- Click 'Enterprise' to open the package selection page
- Click 'Get Started for Free' in the first column:

1
Select Package

2
Enter Account Information

3
Done!

Secure Internet Gateway Gold

— Free —

Free up to 300,000 DNS Requests per Month

Available for Enterprises & MSPs

Active Directory not supported

Does not include:

- ✗ Internal IP/Subnet/IP Block Based Polices
- ✗ Internal IP Based Visibility & Monitoring
- ✗ Encrypt All DNS Traffic
- ✗ Secure Internet Gateway DNS Resolver Virtual Appliances

GET STARTED FOR FREE

🗨️ Free, No Credit Card Required

← Previous

Secure Internet Gateway Platinum

— for Enterprises —

24 x 7 x 365 Platinum Support

Includes:

- ✓ Create Internal IP, Subnet, IP Block and Site Based Policies
- ✓ Internal IP Based Visibility & Monitoring
- ✓ Encrypt All DNS Traffic
- ✓ Install Secure Internet Gateway DNS Resolves Virtual Appliances to your Sites.
- ✓ Bypass Domains to Internal DNS Servers(Needed for Active Directory Sites)
- ✓ Control DNS Egress Points of your Networks by Sites and DNS Servers.

BUY NOW

[1 Month Trial Option](#)

Secure Internet Gateway Platinum

— for MSPs —

24 x 7 x 365 Platinum Support

Includes:

- ✓ Granularly Control, Monitor & Manage Multiple Companies from a Single Dashboard
- ✓ Create Internal IP, Subnet, IP Block and Site Based Polices
- ✓ Internal IP Based Visibility & Monitoring
- ✓ Encrypt All DNS Traffic
- ✓ Install Secure Internet Gateway DNS Resolves Virtual Appliances to your Sites.
- ✓ Bypass Domains to Internal DNS Servers(Needed for Active Directory Sites)
- ✓ Control DNS Egress Points of your Networks by Sites and DNS Servers.

BUY NOW

[1 Month Trial Option](#)

- Next, provide your account details and accept the end user license agreement:

1 Select Package 2 Enter Account Information 3 Done!

Please Enter Customer Details

Email Password Confirm Password

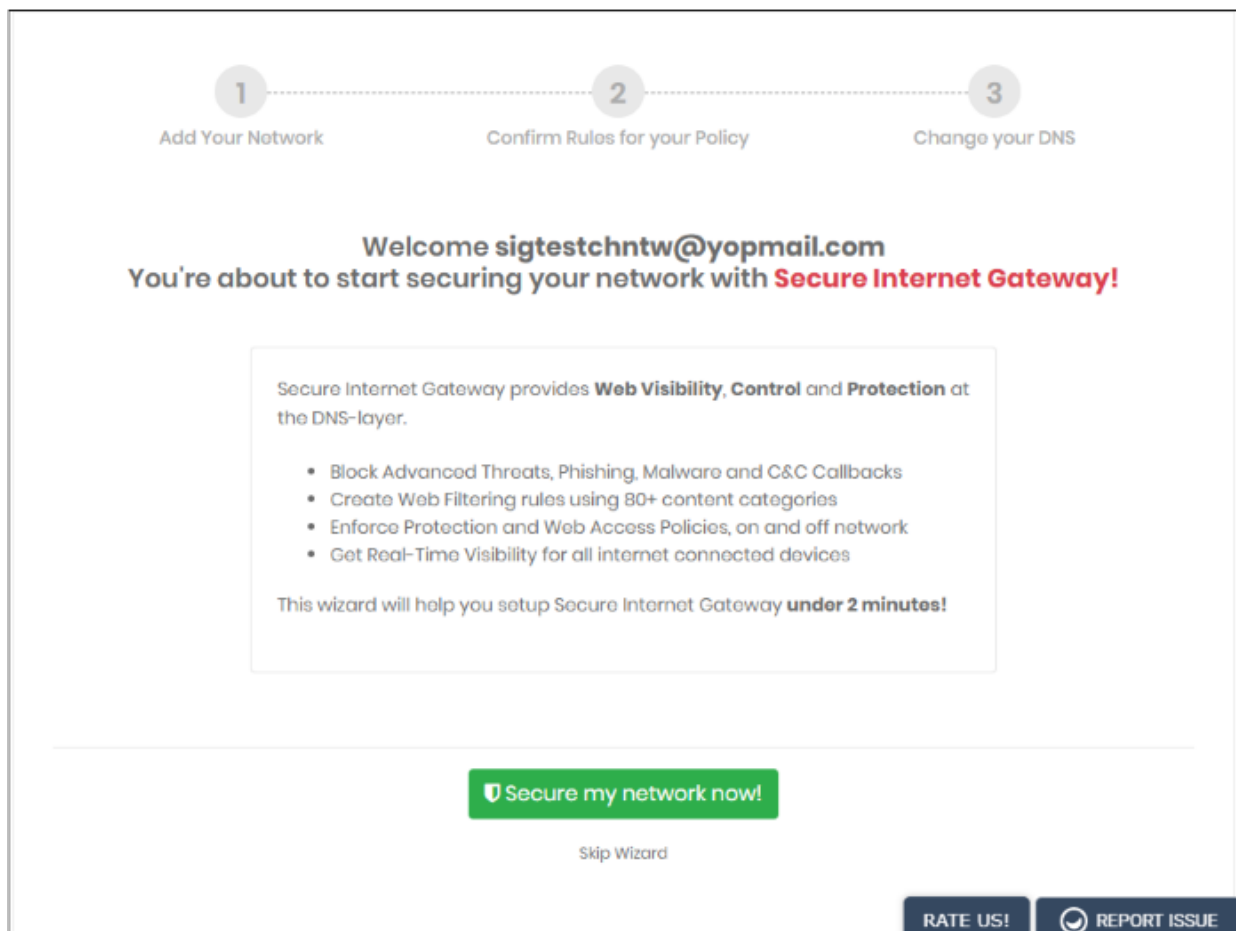
I have read and agree to the **End User license/Service Agreement**

← Previous ✓ Finish

- **Email** - Enter your contact mail address. Order confirmations and license keys are sent to this address. This address doubles up as your Secure Internet Gateway username.
- **Password** and **Confirm Password** - Create a passphrase to login to Secure Internet Gateway.
- **End user license agreement** - Read and agree to the terms and conditions.
- Click 'Finish'

The license confirmation screen is shown for 5 seconds before the setup wizard starts

- Click 'Secure my network now!' to start the wizard. See **Setup Wizard - Add Networks** for help with this.



- Click 'Skip Wizard' if you plan to enroll your network later.

Purchase a Platinum package

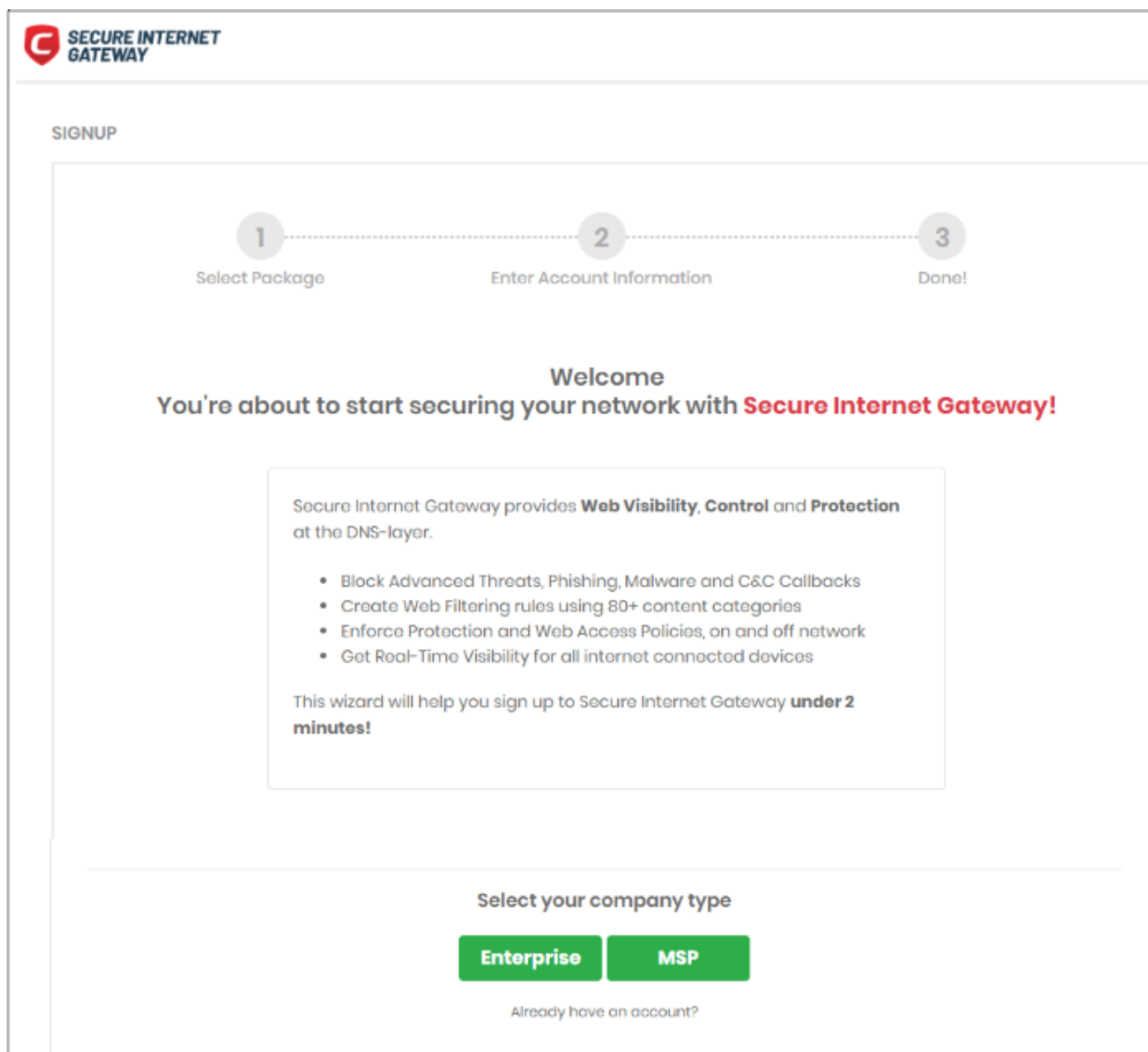
There are two ways to get a platinum license:

- Signup for a new license
- Upgrade a Gold license - Existing customers can upgrade their license in the Secure Internet Gateway interface. Open Secure Internet Gateway > Click 'Account' > 'Buy'

The rest of this section explains how to buy a new Platinum license.

Purchase a new Platinum license

- Visit <https://cdome.comodo.com/dns-internet-security.php>.
- Click 'Start Now'
- You are taken to the sign-up page:



- Click 'Enterprise'
- This opens the package selection page:

1 Select Package

2 Enter Account Information

3 Done!

Secure Internet Gateway Gold

— Free —

Free up to 300,000 DNS Requests per Month

Available for Enterprises & MSPs

Active Directory not supported

Does not include:

- ✗ Internal IP/Subnet/IP Block Based Polices
- ✗ Internal IP Based Visibility & Monitoring
- ✗ Encrypt All DNS Traffic
- ✗ Secure Internet Gateway DNS Resolver Virtual Appliances

GET STARTED FOR FREE

Free, No Credit Card Required

← Previous

Secure Internet Gateway Platinum

— for Enterprises —

24 x 7 x 365 Platinum Support

Includes:

- ✓ Create Internal IP, Subnet, IP Block and Site Based Policies
- ✓ Internal IP Based Visibility & Monitoring
- ✓ Encrypt All DNS Traffic
- ✓ Install Secure Internet Gateway DNS Resolves Virtual Appliances to your Sites.
- ✓ Bypass Domains to Internal DNS Servers(Needed for Active Directory Sites)
- ✓ Control DNS Egress Points of your Networks by Sites and DNS Servers.

BUY NOW

[1 Month Trial Option](#)

Secure Internet Gateway Platinum

— for MSPs —

24 x 7 x 365 Platinum Support

Includes:

- ✓ Granularly Control, Monitor & Manage Multiple Companies from a Single Dashboard
- ✓ Create Internal IP, Subnet, IP Block and Site Based Polices
- ✓ Internal IP Based Visibility & Monitoring
- ✓ Encrypt All DNS Traffic
- ✓ Install Secure Internet Gateway DNS Resolves Virtual Appliances to your Sites.
- ✓ Bypass Domains to Internal DNS Servers(Needed for Active Directory Sites)
- ✓ Control DNS Egress Points of your Networks by Sites and DNS Servers.

BUY NOW

[1 Month Trial Option](#)

- Click 'Buy Now' under 'Secure Internet Gateway Platinum for Enterprises'
- The next step is to provide your account details and accept the end user license agreement.

1 Select Package 2 Enter Account Information 3 Done!

Please Enter Customer Details

Email	Password	Confirm Password
<input type="text"/>	<input type="text"/>	<input type="text"/>

I have read and agree to the **End User license/Service Agreement**

[← Previous](#) [→ Choose License](#)

- **Email** - Enter your contact mail address. Order confirmations and license keys are sent to this address. This address doubles up as your Secure Internet Gateway username.
 - **Password** and **Confirm Password** - Enter a passphrase for logging-in to your Secure Internet Gateway account. This also serves as password for your Comodo account
 - **End user license agreement** - Read and agree to the terms and conditions.
- Click 'Choose License'

The next step is to configure your package and provide your payment information:

1 ————— **2** ————— **3**

Select Package Enter Account Information Done!

Secure Internet Gateway Platinum

Select License Period

Monthly	Yearly
---------	--------

of Users

5

Please enter the actual number of users you have in your network so that your service will not be interrupted.

Total Price (\$ 29.38 per user)
\$ 146.90

Credit Card Details

Credit Card No.

Cardholder Name

CVV **Expiration Date**

	01 ▼	2019 ▼
--	------	--------

SALES: +1(888)551-1531

Finish ✓

- **Select License Period** - Choose monthly or yearly

- **Number of users** - Specify exactly how many users you want to protect.
- Enter your payment card information and click 'Finish'.
- You will receive order confirmation and license emails.

You can now login to Secure Internet Gateway at <https://shield.dome.comodo.com/login>.

Comodo One / Dragon and ITarian Customers

- Comodo One customers - <https://one.comodo.com/>
- Comodo Dragon customers - <https://platform.comodo.com/app/login>
- ITarian customers - <https://www.itarian.com/>

A Secure Internet Gateway Gold license is automatically activated in your account when you sign-up for a C1 / Dragon / ITarian account.

Upgrade to a Platinum license

- Login to your C1 / Dragon / ITarian account
- Click 'Management' > 'Applications'
- Select 'Secure Internet Gateway' then click 'Subscriptions' > 'Add New Subscription'

The screenshot shows the 'Applications' management page. At the top, there are two module cards: 'Endpoint Manager' and 'Secure Internet Gateway'. The 'Secure Internet Gateway' card is highlighted with a red border. Below the cards is a toggle for 'Show all hidden modules'. A navigation bar contains 'Subscriptions', 'Usage', 'Billing', and 'Settings'. The 'Subscriptions' tab is selected and circled in red. Below the navigation bar, there is a 'Subscription List' section with a green '+ Add New Subscription' button circled in red. A table displays subscription details:

ID:	Dome Shield GOLD MSP	FREE	ACTIVE
65b7fcd	5	TRIAL	
961	Start Date: 01/08/2020	Unlimited	

To the right of the table is a 'Details' section showing 'ITarian License Account Username: tester321@yopmail.com' and 'Module Name'.

- The account username is pre-populated.
- Enter your C1 / Dragon / ITarian password and click 'Login'

Buy New Subscription Secure Internet Gateway

- 1. Login
- 2. ITarian Account
- 3. Configure Subscription
- 4. Customer Information
- 5. Payment Options
- 6. Order Summary

Login

Login *

tester321@yopmail.com

Password *

[Forgot Password](#)

Login

- **Activate Selected** - Platinum licenses bought via your Comodo Accounts Manager (CAM) account can be activated for use in Comodo One / Dragon / ITarian.
- **Buy New** - Purchase a new Platinum license.

Buy New Subscription Secure Internet Gateway

- 1. Login
- 2. ITarian Account
- 3. Configure Subscription
- 4. Customer Information
- 5. Payment Options
- 6. Order Summary

Subscriptions assigned to this ITarian Account

You do not have any available license to activate. Please continue purchasing by clicking 'BUY NEW' button.

IN-USE ID: 378538ab-5c72-4d6c-a41c-a0c32deb3abe
Dome Shield GOLD MSP
Start Date: 01/08/2020

Back [Activate Selected](#) [Buy New](#)

- Select the number of users you require and the term of the license:

Buy New Subscription Secure Internet Gateway

1. Login
2. ITarian Account
3. Configure Subscription
4. Customer Information
5. Payment Options
6. Order Summary

Configure Subscription

Amount of Users Users

1	100	250	500	1000	2500	5000	10000	25000	10000000
\$29.38	\$25.78	\$21.02	\$16.20	\$14.98	\$14.40	\$13.82	\$13.18	\$12.60	
per user	per user	per user	per user	per user	per user	per user	per user	per user	

Select Period

1 month

3 months

6 months

1 year

2 years

3 years

\$29.38 per 4 users for 1 year = \$117.52

\$117.52

Back Next >

- Click 'Next' and complete the customer information form.

Buy New Subscription Secure Internet Gateway

1. Login
2. ITarian Account
3. Configure Subscription
4. Customer Information
5. Payment Options
6. Order Summary

Customer Information

Company Name

Company Website

Phone Number *

Street Address *

Street Address 2

City *

Country *

State or Province

Postal Code *

Billing Information

The same as Contact Information

Terms and Conditions

I have read and agree the [End User License/Service Agreement](#).

Back Next >

- Agree to the terms and conditions and click 'Next'

- Complete your payment details

Buy New Subscription Secure Internet Gateway

1. Login
2. ITarian Account
3. Configure Subscription
4. Customer Information
5. Payment Options
6. Order Summary

Order Confirmation

PRODUCT	LICENSE PERIOD	FULL PRICE
Dome Shield Platinum for MSP(1-99 Users)	1 Year	\$117.52
TOTAL		\$117.52

Payment Options

Credit Card Number

Card Holder Name

Expiration Date

CW

[What is it?](#)

When paying by credit card, the billing information should be exactly as it appears on your credit card statement. For credit card verification, please ensure that your first and last name are entered as they appear on your card.

Back Next >

- Click 'Next' to place your order. Your license will be added to your account.
- The next step is to activate the new license
 - Click 'Management' > 'Applications'
 - Select 'Secure Internet Gateway' then click the 'Subscriptions' tab
 - Click 'Add New Subscription'
 - Enter your C1 / Dragon / ITarian password and click 'Login'
 - The Secure Internet Gateway licenses added to your account are shown as a list
 - Select the new license and click 'Activate Selected'

Compare Secure Internet Gateway Packages

Secure Internet Gateway - Package Details			
Feature	Gold -Free - Enterprises & MSPs	Platinum For Enterprises	Platinum For MSPs
Control, monitor & manage multiple companies	✘	✘	✔
Create internal IP, subnet, IP block and site based policies	✘	✔	✔

Secure Internet Gateway - Package Details			
Feature	Gold -Free - Enterprises & MSPs	Platinum For Enterprises	Platinum For MSPs
Monitoring of internal IPs	✘	✓	✓
Encrypt all DNS traffic	✘	✓	✓
Resolve virtual appliances to your sites.	✘	✓	✓
Bypass domains to internal DNS servers (needed for Active Directory sites)	✘	✓	✓
Control DNS egress points of your networks by site and DNS server.	✘	✓	✓

All packages include the following:

- Anycast DNS
- Protection against advanced threats
- Stop malicious domain requests and IP responses
- Off-network protection
- Enforce policies & gain visibility
- Customizable block pages
- Real-time, full customizable reporting
- Protect mobile devices (iOS and Android)
- Domain filtering
- Use real-time updated Threat Intelligence of Comodo Threat Research Labs
- Multi-office & roaming user protection
- 24 x 7 email support

DNS Requests Limitation for Licenses

- **Platinum License**
 - Unlimited DNS requests
- **Gold license**
 - DNS requests are capped at 300 K per month for the account. Account = requests from all your endpoints/networks.
 - DNS requests are mainly used up by first-time requests to external sites. Subsequent requests for the same site are handled by the local cache until TTL expires.
 - Requests to the Secure Internet Gateway Portal are *not* included in the 300 K limit.
 - The request count is reset to zero at the beginning of each month.
 - Once 300 K limit is reached within a month:
 - You need to upgrade to Platinum license to continue the service.
 - After this point the request count will not be reset to zero at the beginning of each month.

[Click here](#) for more information about CSIG license package details.

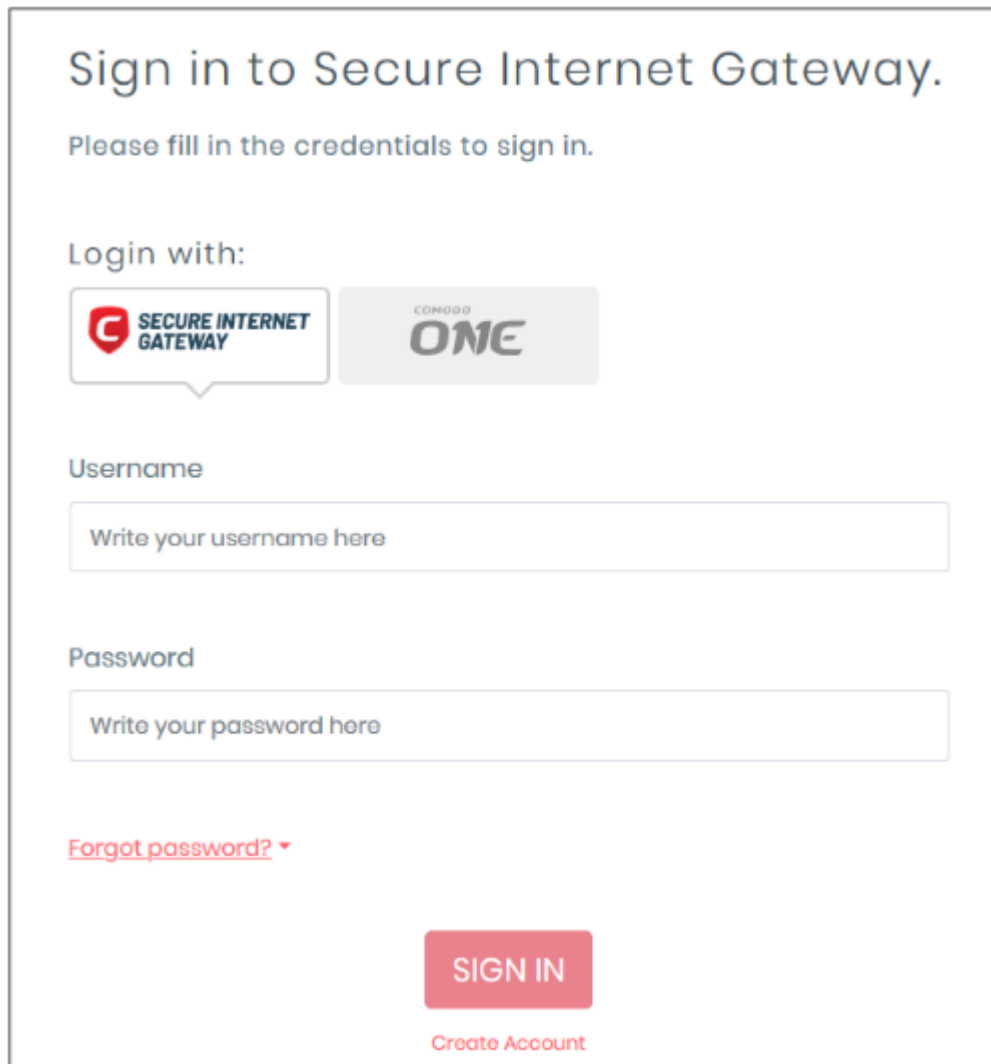
1.2 Login to Secure Internet Gateway

You can login at the **stand-alone portal**, or via the **C1/ Dragon/ ITarian portal**.

Stand-alone portal

This applies to enterprise customers who bought a license from <https://cdome.comodo.com/>.



- Login at <https://shield.dome.comodo.com/login> and select 'Secure Internet Gateway'



Sign in to Secure Internet Gateway.

Please fill in the credentials to sign in.

Login with:

Username

Password

[Forgot password?](#) ▾

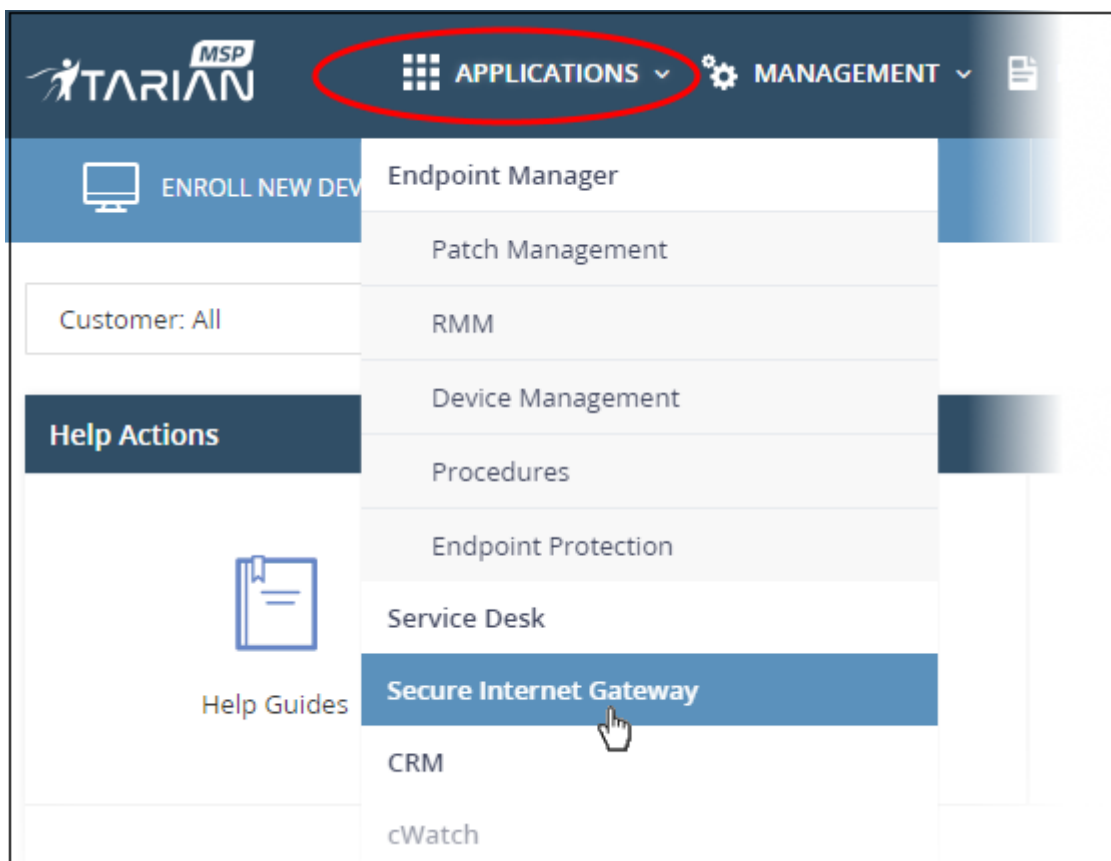
SIGN IN

[Create Account](#)

- Username and password are case sensitive. Make sure you use the correct case.

Comodo One / Dragon / ITarian Portal

- Login to your C1, Dragon or ITarian account:
 - Comodo One customers - <https://one.comodo.com/app/login>
 - Comodo Dragon customers - <https://platform.comodo.com/app/login>
 - ITarian customers - <https://www.itarian.com/app/msp/login>
- Username and password are case sensitive. Please make sure that you use the correct case.
- Click 'Applications' > 'Secure Internet Gateway' to open the CSIG interface.



1.3 Setup Options Explained

There are three alternative ways you can setup Secure Internet Gateway protection:

1. Setup wizard

- Click 'Setup Wizard' at the top-right of the interface to get started
- Follow the steps to add your networks
- Click [here for help](#) with the wizard

2. Manual

- Click 'How-to' at the top-right of the interface
- There are four tutorials - [add networks](#), [add roaming endpoints](#), [add mobile devices](#) and [how to deploy local resolver virtual appliances](#).

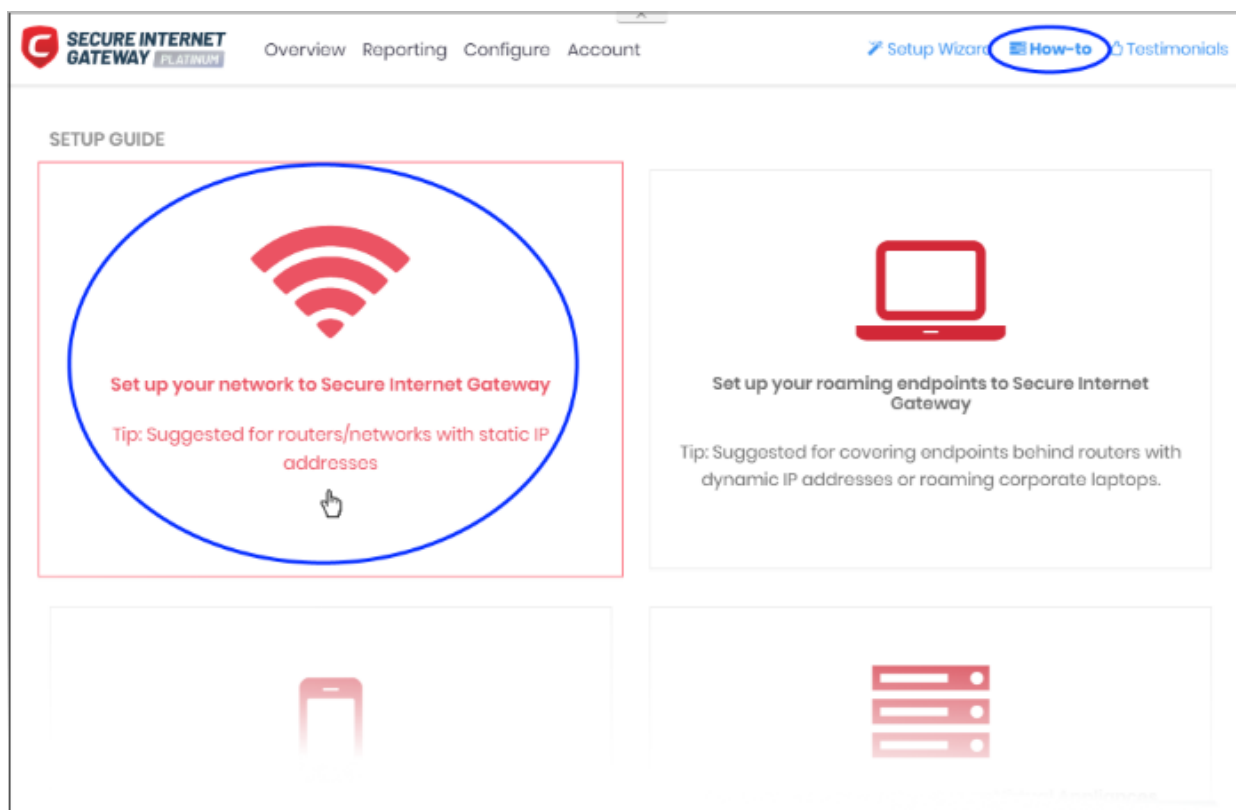
3. Install local resolvers

- You install a local resolver (LR) as a virtual appliance on the network
- Once deployed, your networks will be automatically imported to Secure Internet Gateway
- The resolver will forward public DNS queries from your endpoints to CSIG DNS servers
- The resolver method offers some key advantages over the 'direct' methods
- [Click here](#) for help to setup the local resolvers

1.3.1 Tutorial to Add Networks to Secure Internet Gateway

- Login to Secure Internet Gateway

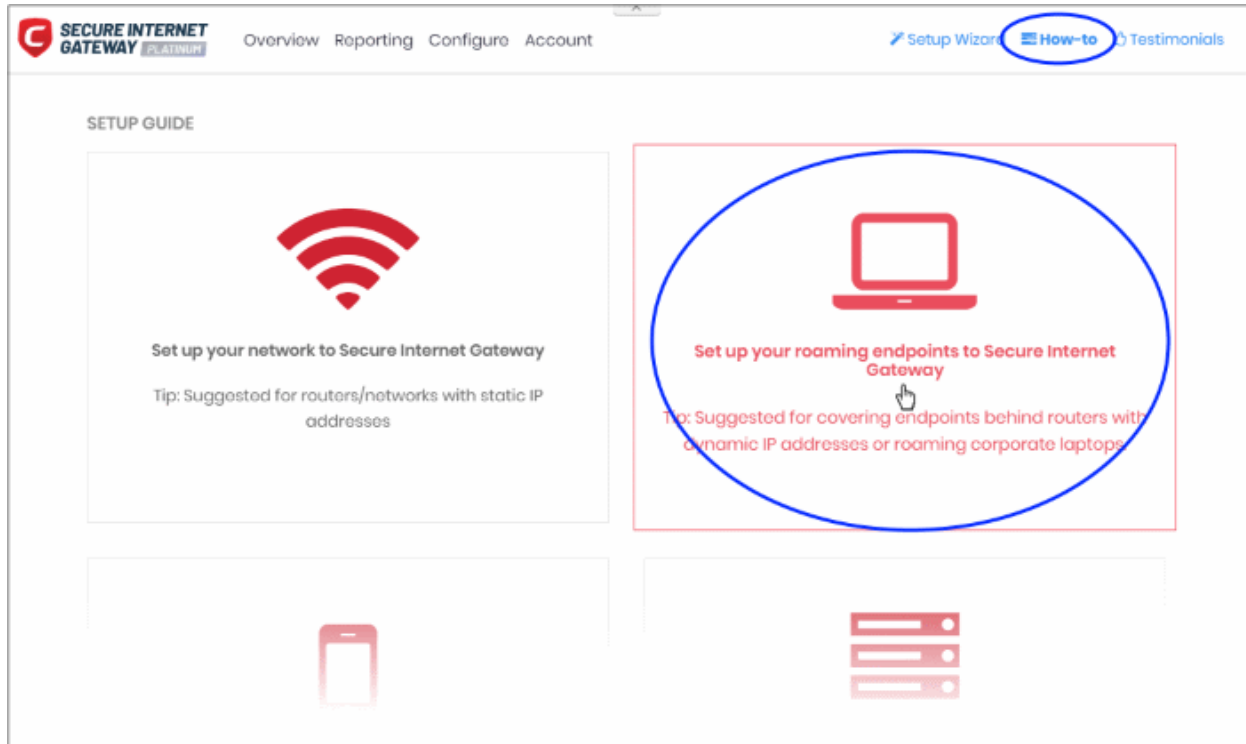
- Click 'How-to' at the top-right to open the tutorial menu:



- Click the network icon on the left to open the network setup guide:

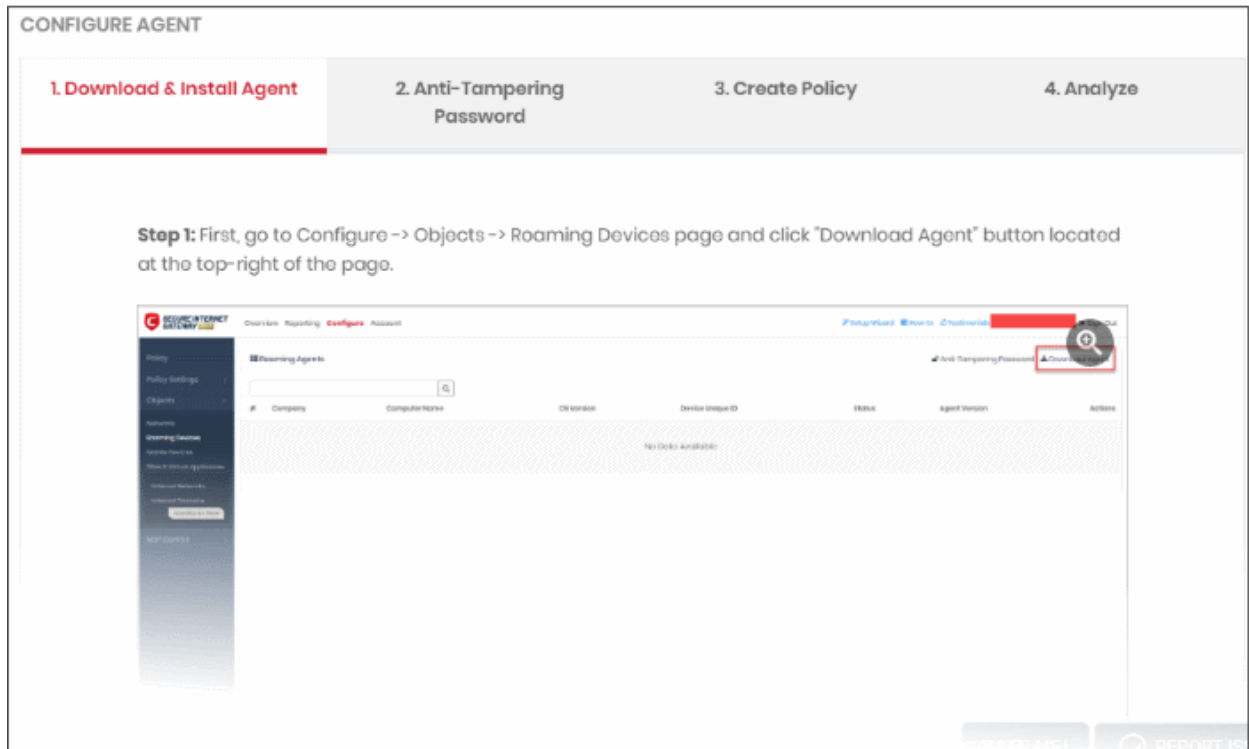
1.3.2 Tutorial to Add Roaming Endpoints to Secure Internet Gateway

- Login to Secure Internet Gateway
- Click 'How-to' at the top-right to open the tutorial menu:
- Click 'Setup your roaming endpoints...':



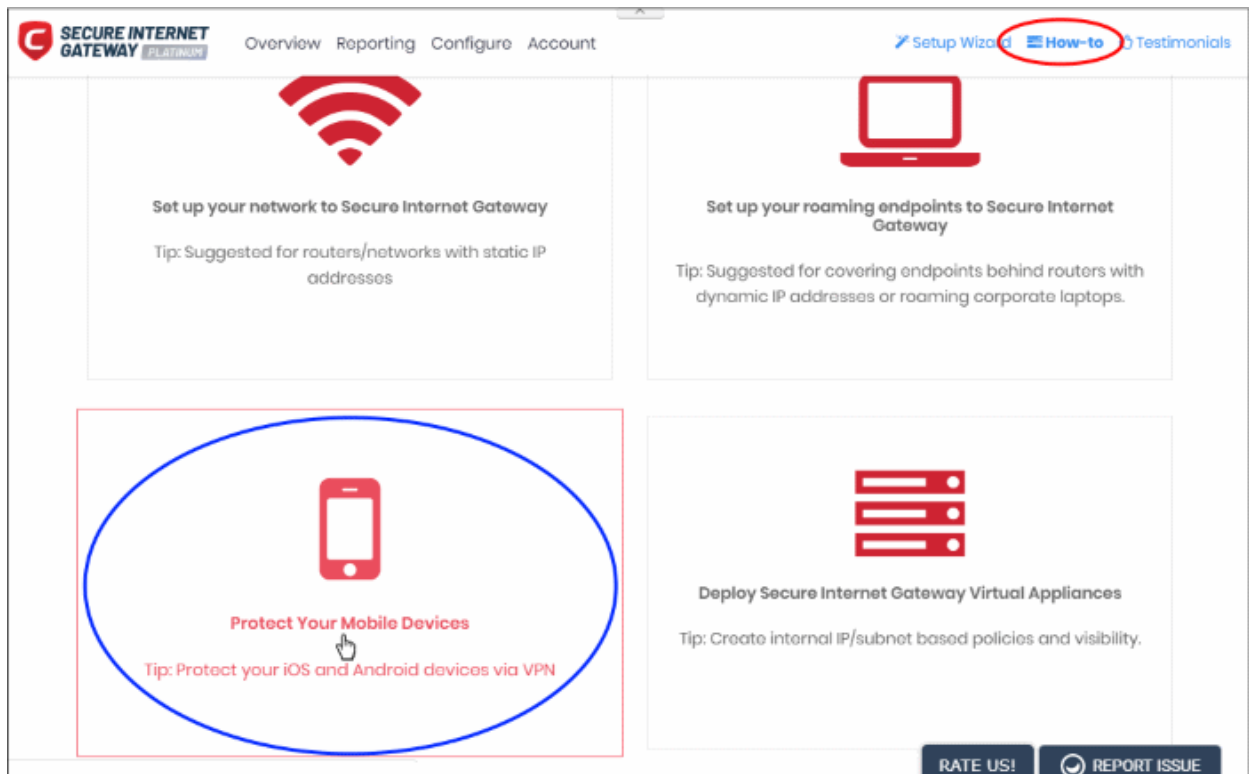
There are four steps in the tutorial:

- **Download & Install Agent** - Enroll roaming devices
- **Anti-Tampering Password** - Prevent unauthorized removal of the SIG agent from roaming devices
- **Create Policy** - Add content filtering rules and domain black/whitelists for enrolled devices.
- **Analyze** - View traffic trends on enrolled devices.



1.3.3 Tutorial to Add Mobile Devices

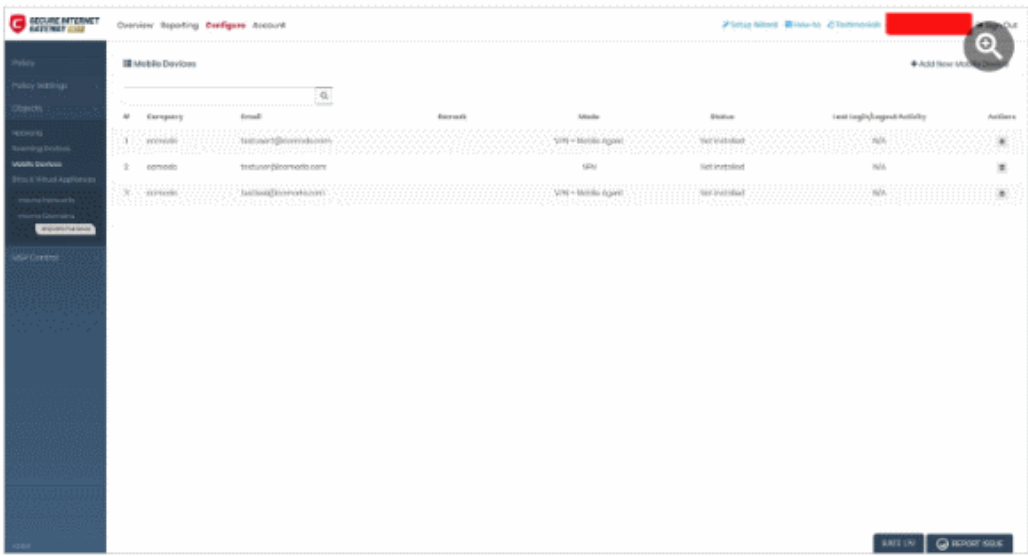
- Login to Secure Internet Gateway
- Click 'How-to' at top-right then 'Protect your mobile devices':



- The tutorial explains how to add mobile devices to CSIG.
- See '**Add Mobile Devices**' if you need help to complete the wizard.


PROTECT YOUR MOBILE DEVICES

Step 1) Go to Configure page and select "Mobile Devices"...



ID	Category	Email	Network	Mode	Status	Last Login/Logout Activity	Actions
1	android	testuser@comodo.com		VPN - Mobile Agent	Not Installed	N/A	[X]
2	android	testuser@comodo.com		VPN	Not Installed	N/A	[X]
3	android	testuser@comodo.com		VPN - Mobile Agent	Not Installed	N/A	[X]

Step 2) Click "Add New Mobile Device" button located at the top-right.



1.3.4 Tutorial to Deploy CSIG Virtual Appliances

- Login to Secure Internet Gateway
- Click 'How-to' at the top-right
- Click 'Deploy Secure Internet Gateway Virtual Appliances':

SECURE INTERNET GATEWAY PLATINUM Overview Reporting Configure Account Setup Wizard **How-to** Testimonials

SETUP GUIDE

Set up your network to Secure Internet Gateway
Tip: Suggested for routers/networks with static IP addresses

Set up your roaming endpoints to Secure Internet Gateway
Tip: Suggested for covering endpoints behind routers with dynamic IP addresses or roaming corporate laptops.

Protect Your Mobile Devices
Tip: Protect your iOS and Android devices via VPN

Deploy Secure Internet Gateway Virtual Appliances
Tip: Create internal IP/subnet based policies and visibility

[RATE US!](#) [REPORT ISSUE!](#)

<https://shield.dome.comodo.com/how-to/setup-local-resolver>

- See '[Setup Local Resolver Virtual Machines and Import Sites](#)' if you need help with the wizard.

HOW TO DEPLOY SECURE INTERNET GATEWAY VIRTUAL APPLIANCES

A. Introduction

- [What Are Secure Internet Gateway Local Resolver Virtual Appliances & How Do They Work?](#)
- [Why Should I Use Comodo Secure Internet Gateway Local Resolvers?](#)

B. Prerequisites

- Prerequisites

C. Deployment Guidelines

- Intro
- Redundancy
- Multiple DNS Egress - Single DNS Egress

D. Deploy Secure Internet Gateway Local Resolvers

- Before Deployment
- SETUP with VMWARE
- SETUP with VIRTUAL BOX

E. Setup with HYPER-V

What Are Secure Internet Gateway Local Resolver Virtual Appliances & How Do They Work?

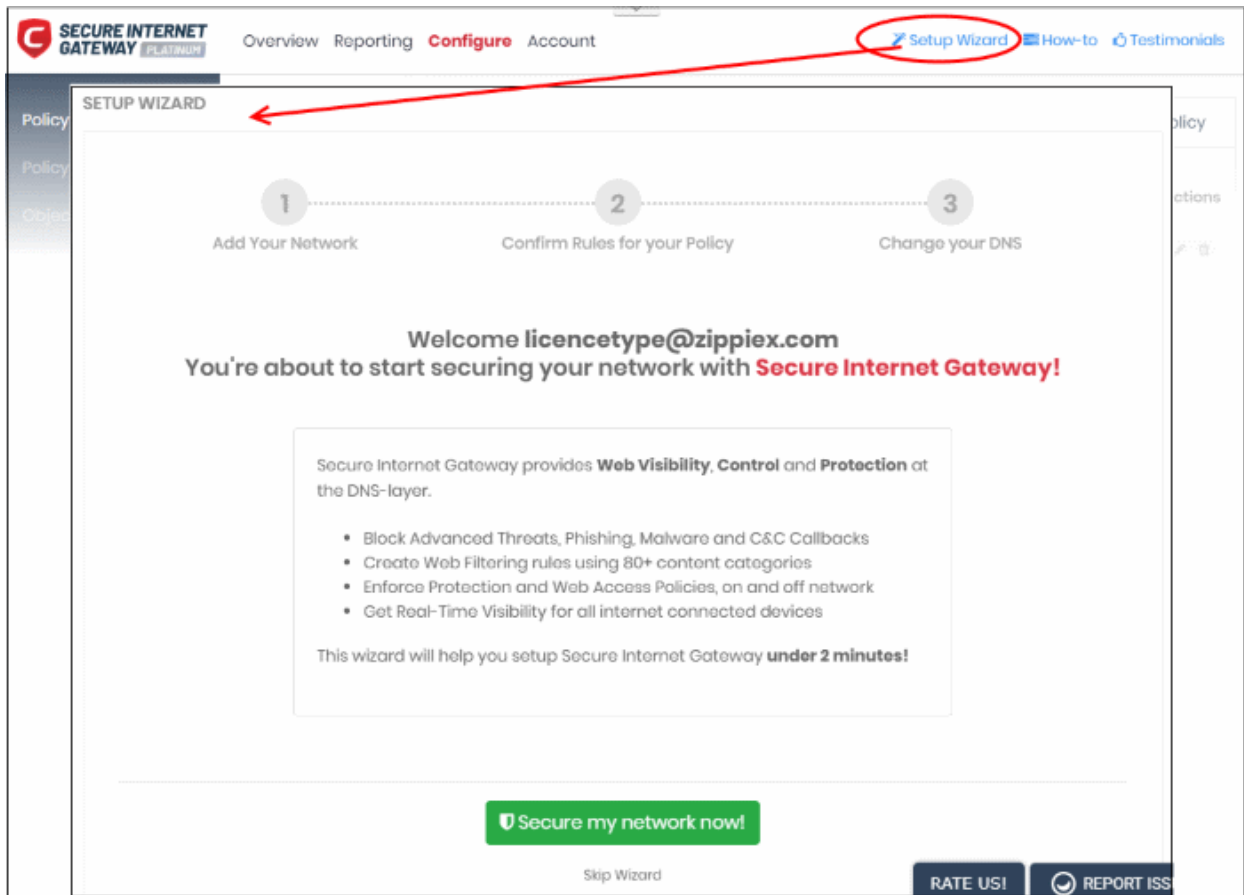
Comodo Secure Internet Gateway Local Resolver Virtual Appliances (Secure Internet Gateway LRs) are virtual machines that are compatible with VirtualBox, VMware ESXi and Windows Hyper-V hypervisors. Acting as conditional DNS forwarders, Comodo Secure Internet Gateway Local Resolver Virtual Appliances forward public DNS queries to Secure Internet Gateway's global DNS servers, while encrypting and authentication DNS data to enhance security, and recording the internal IP address of the client that DNS request is received from.

When launched as DNS forwarders on your network and registered to Secure Internet Gateway Portal, Secure Internet Gateway VAs are displayed as objects in Secure Internet Gateway Portal to be used in rules and policies for your network. Lastly, since Secure Internet Gateway VAs are able to record the internal IP info of DNS requests in your network, they provide you with the option to track down logs for each internal IP in your network.



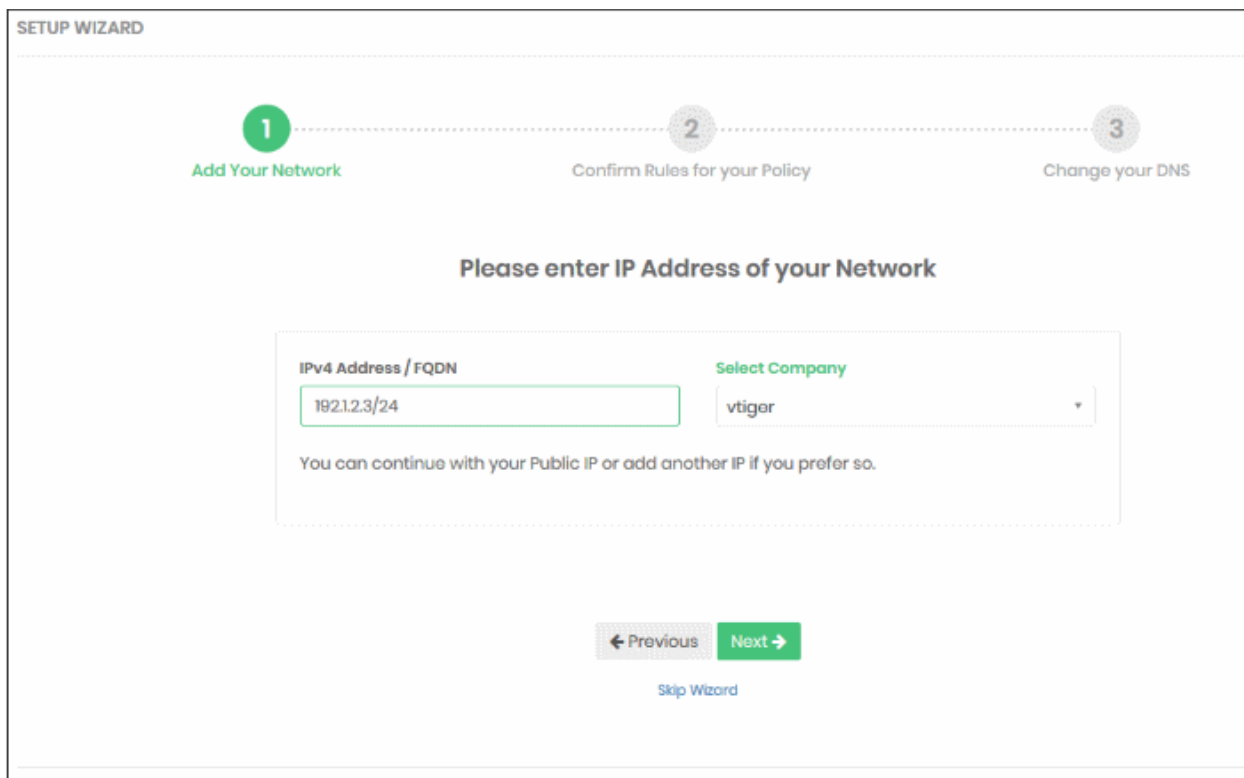
1.3.5 Setup Wizard - Add Networks

- The setup wizard lets you quickly enroll your networks to Secure Internet Gateway.
- If you haven't yet added a network then the wizard will start automatically after logging in.
- You can also start the wizard at any time by clicking 'Setup Wizard' at top-right:



- Click 'Secure my network now!'

Step 1 - Add your IP Address



IP Address / FQDN

- By default, this shows the public IP of the network from which you are connecting. This network is

automatically activated after initial enrollment.

- You can also add the IP address of a different network you want to protect. Enter the network IP address or fully qualified domain name in CIDR notation.
- Secure Internet Gateway can accept network prefixes from /24 to /32.
 - Any IP you add here will be automatically activated for protection. Make sure you are able to change the network's DNS settings to Secure Internet Gateway, as explained in step 3.
 - CSIG also supports dynamic IP addresses. You need to download the 'Windows Dynamic IP Updater' agent and install it on a network endpoint. See '[Add Networks](#)' for more information.

Select Company - MSPs only. Select the customer organization for which you want to enroll the network.

- Click 'Next' to configure rules for the default policy.

Step 2 - Configure Rules for your Policy

Configure security and website category rules for the default policy. These will be immediately applied to the network on enrollment.

- All rules are enabled by default. You can enable / disable rules here as required.
- If you are unsure, then a good rule of thumb is to just leave everything enabled. This will give you maximum protection, and you can easily modify the settings later if any issues transpire.
- You can modify the policy later by clicking 'Policy Settings' in the left-hand menu. See '[Manage Security Rules](#)' and '[Manage Category Rules](#)' if you need help with these areas.

Click 'Confirm' to apply your policy.

Step 3 - Change your DNS Settings

Change your DNS addresses to following CSIG addresses:

- Preferred DNS server - 8.26.56.10
- Alternate DNS server - 8.20.247.10

Click 'Yes, My DNS is set to CSIG' once you have done this:

SETUP WIZARD

1 Add Your Network 2 Confirm Rules for your Policy 3 Change your DNS

We are ready to secure your traffic!

Set your DNS to Secure Internet Gateway to Complete Setup!

Primary DNS	Secondary DNS
8.26.56.10	8.20.247.10

Yes, My DNS is Set to Secure Internet Gateway! ✓

Will do it later

That's it. You have now added a network to Secure Internet Gateway.

SETUP WIZARD

1 Add Your Network 2 Confirm Rules for your Policy 3 Change your DNS

CONGRATULATIONS!

Your network is now secured by **Secure Internet Gateway!**

What else can you secure and control with Secure Internet Gateway?

- Networks
- Internal IPs/Subnets and IP Blocks
- MAC and Windows Roaming Laptops
- iOS and Android Smartphones/Tablets

What else can you apply on these objects?

- Web-Filtering rules based on 80+ categories
- Blacklists and Whitelists to create exceptions
- Web-Protection Policies with 20 categories
- Custom Block Pages

[Learn More](#) [Go to Configure Page](#)

[RATE US!](#) [REPORT IS](#)

- Click 'Configure' > 'Objects' > 'Networks' in the CSIG interface to see all networks that you have added.
- Note - To support dynamic IP addresses, you need to download the 'Windows Dynamic IP Updater' agent and install it on a network endpoint. See '[Add Networks](#)' for more information.

Next, see the following items for help with specific areas:

- [Manage CSIG Rules](#)
- [Add Networks, Roaming Endpoints and Mobile Devices](#)
- [Apply Policies to Networks and Roaming / Mobile Devices](#)
- [The Dashboard](#)

1.3.6 Setup Local Resolver Virtual Machines and Import Sites

- The local resolver VM is an alternative method of importing networks to Secure Internet Gateway. The feature is only available with Platinum licenses.
- The resolver is deployed as a virtual machine on your network and will forward public DNS queries to Secure Internet Gateway DNS servers.
- The network will be automatically imported to Secure Internet Gateway after you deploy the resolver.
- The resolver method offers some key benefits over the 'direct' method of the wizards:

Benefits:

- DNS data is encrypted in transit, enhancing your network security.
- The resolver records the IP address of the client from which the DNS request originated. These addresses are included in Secure Internet Gateway logs and reports, which gives you insight into the browsing patterns of your endpoint users.
- You can apply different policies to internal IP addresses and sub-nets, giving you granular control over the network
 - See [Add Internal Networks](#) for more on defining internal address blocks for different policies
- You do not need to install agents on endpoints. You just need to change the DNS settings on the endpoint to point to the resolver's local IP address.
- Local resolver virtual machines require minimal configuration (only one CPU and 1GB of RAM) to process millions of DNS queries.

Best Practices:

- For high-availability, we recommend you deploy two local resolvers for each network you import. You can configure the resolvers in a master-slave relationship. If the master fails, the slave will continue to forward queries to Secure Internet Gateway DNS.
- Master and slave resolvers should be implemented on separate servers/hosts.
- If you have multiple DNS egress points from separate sites, you will need to deploy separate pairs for each site of the same office/environment.

Minimum System Requirements:

- A virtual machine application (VMWare, VirtualBox or Hyper-V)
- One virtual CPU
- 1024 MB of RAM
- 7 GB of disk space

Important Note: For high traffic sites, we recommend 2 virtual CPUs and 2048 MB of RAM for each VA. A high-traffic site is one that receives more than 500 DNS queries per second.

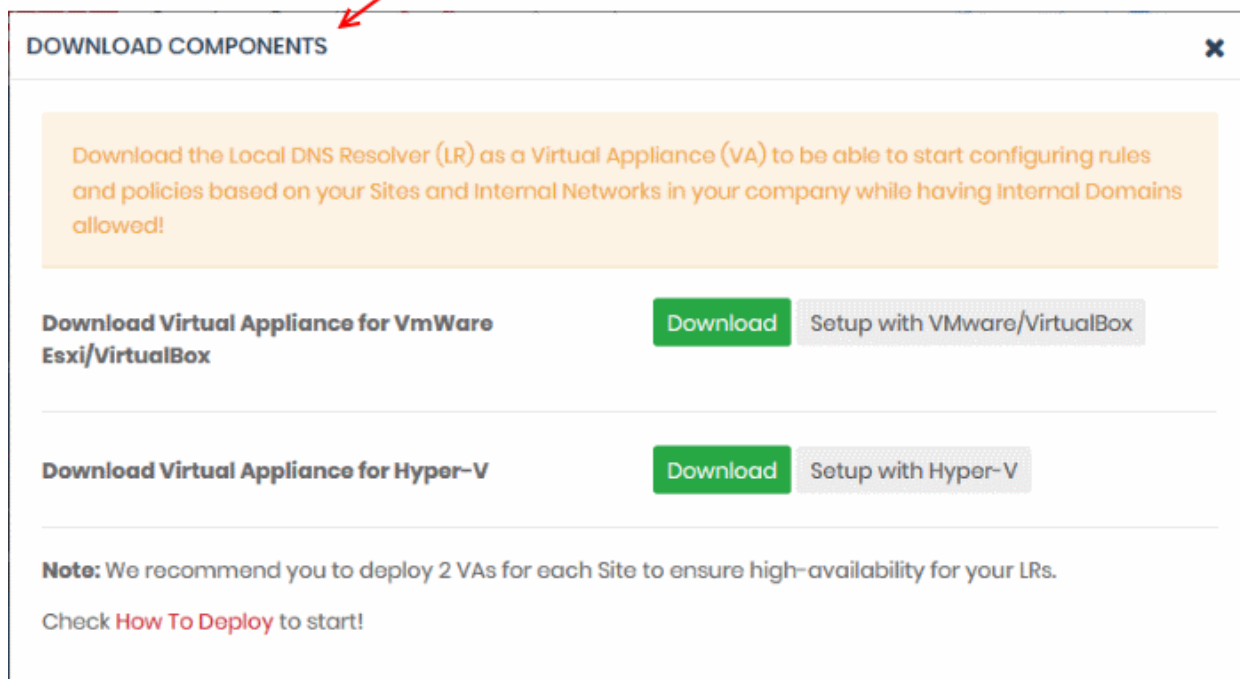
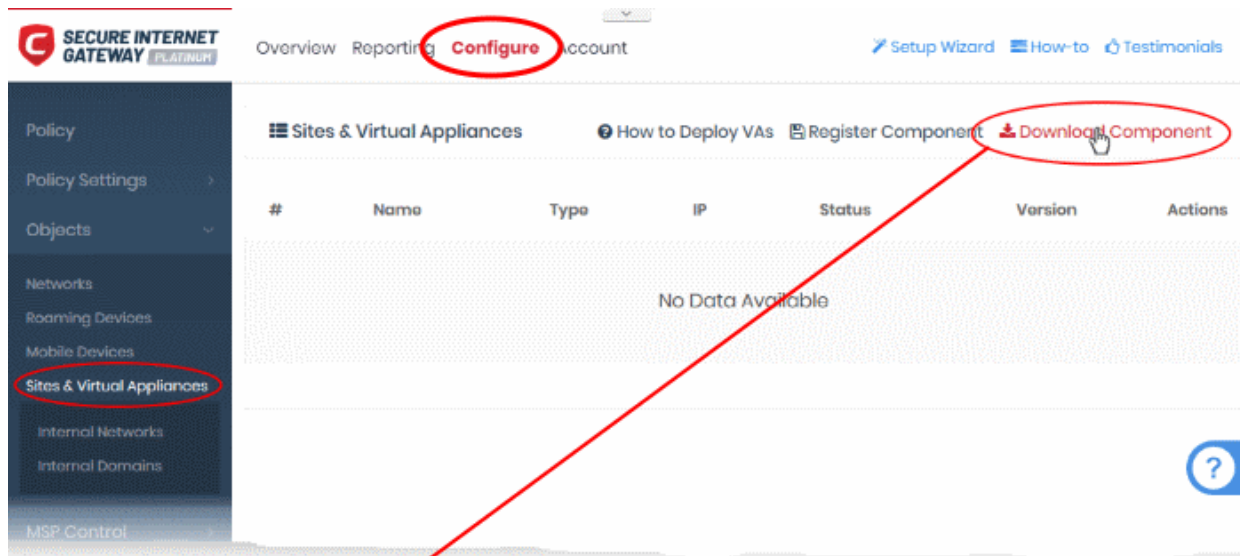
The rest of this section explains how to install the local resolver VA's

Setup the Local Resolvers

- **Step 1 - Download the Setup File**
- **Step 2 - Setup the Master Virtual appliance**
- **Step 3 - Register the Master VA**
- **Step 4 - Setup the Slave VA (Optional)**
- **Step 5 - Configure DNS Settings in the endpoints to point to the Local Resolvers**

Step 1 - Download the Setup File

- Login to Secure Internet Gateway
- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances'
- Click 'Download Component' at the top-right



The resolver VA can be setup on virtual machines like VMWare, VirtualBox and Hyper - V.

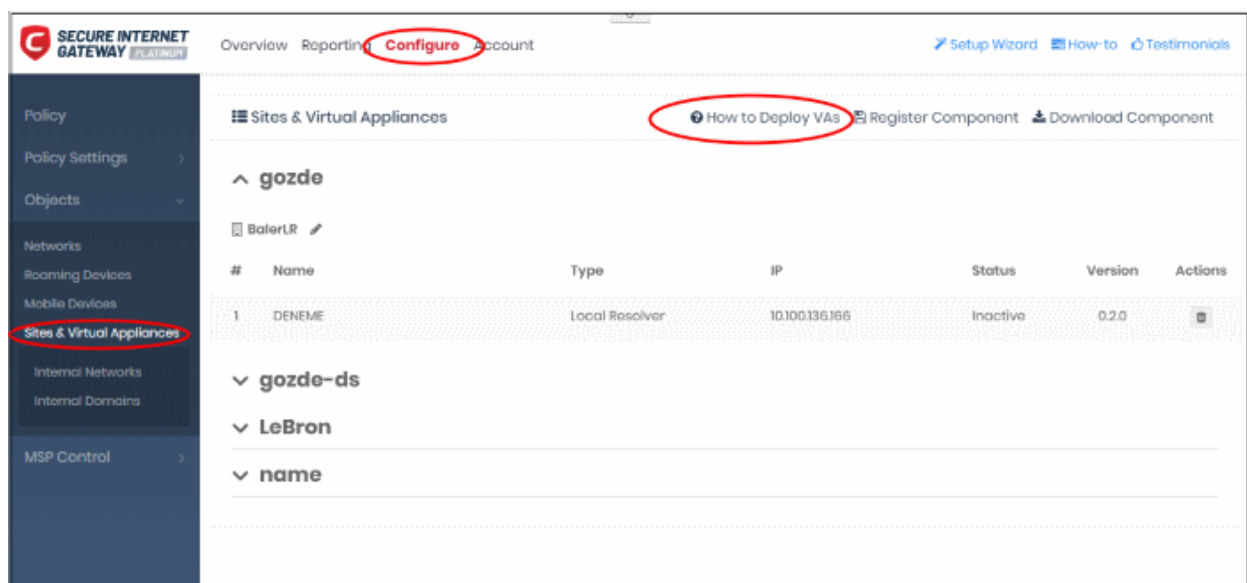
- Click the 'Download' button beside the VM application you want to use
- The setup package will download in .zip format
- The package contains an OVA or HYPER-V file depending on the VM you chose. The package also contains a text file with login credentials to access the appliance.

Step 2 - Setup the Master Virtual appliance

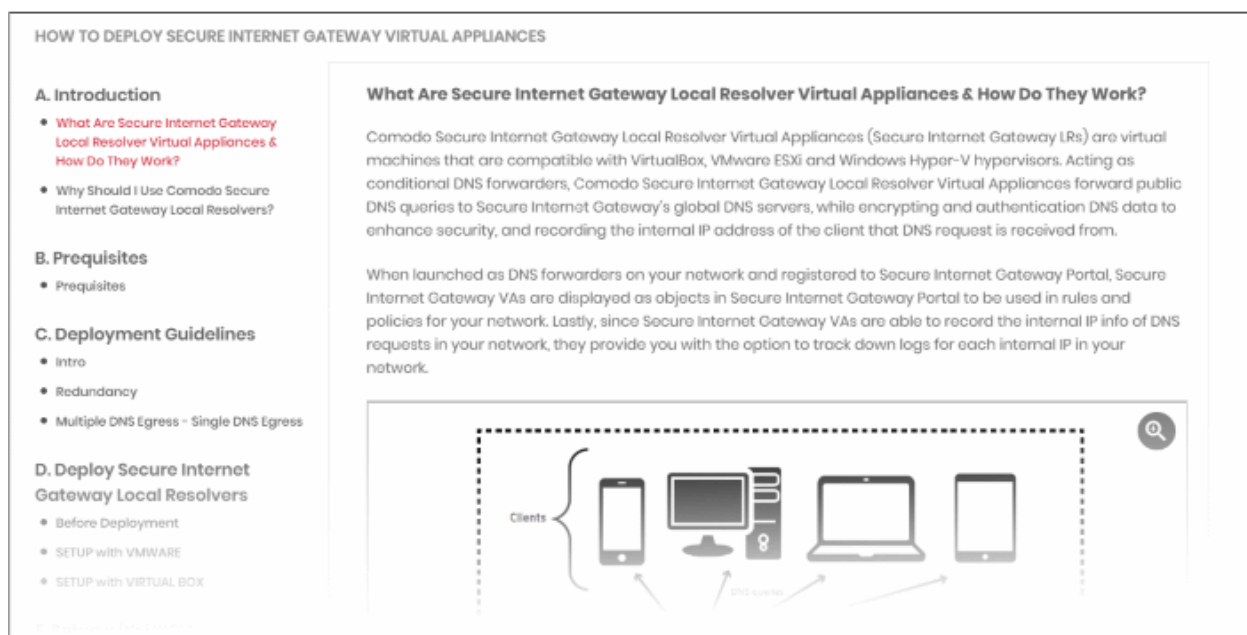
- Copy the package to the hosts on which you want to setup the appliance.
- Extract the package.
- Install the virtual appliance.

The CSIG interface contains tutorials to help you install the VA on VMWare, VirtualBox and Hyper-V.

- Click Configure > Objects > Sites & Virtual Appliances
- Click 'How to Deploy VAs'

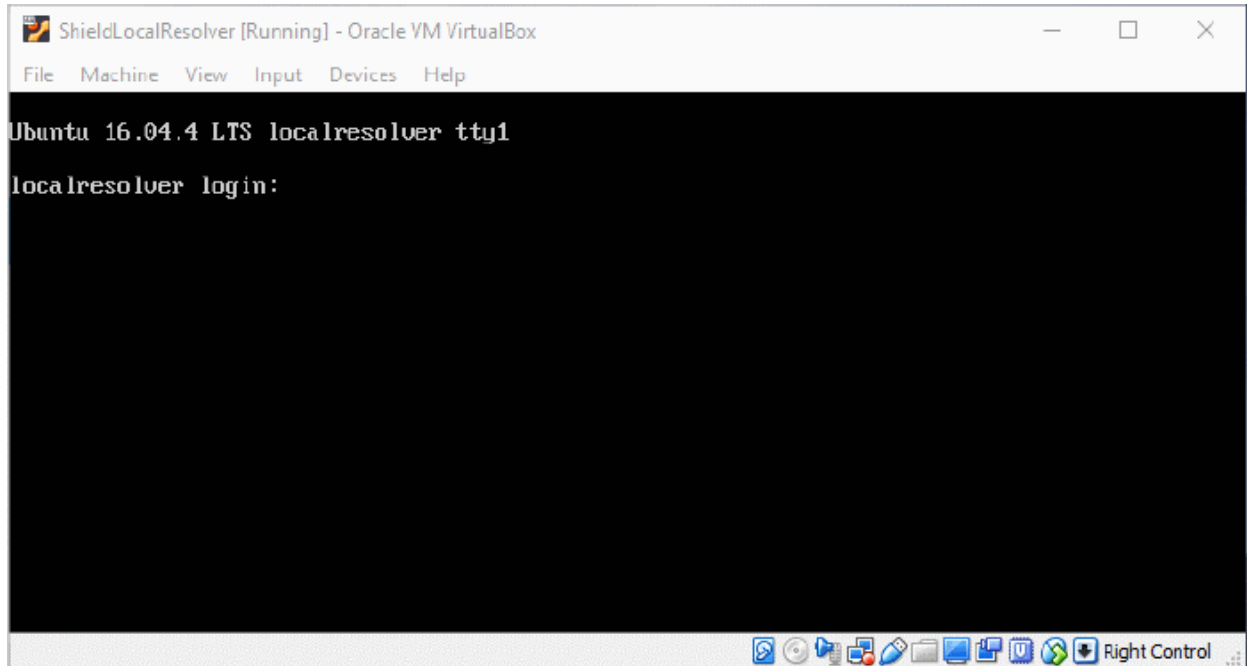


The instructions page explains how to install the VA on VMWare, VirtualBox and Hyper-V:

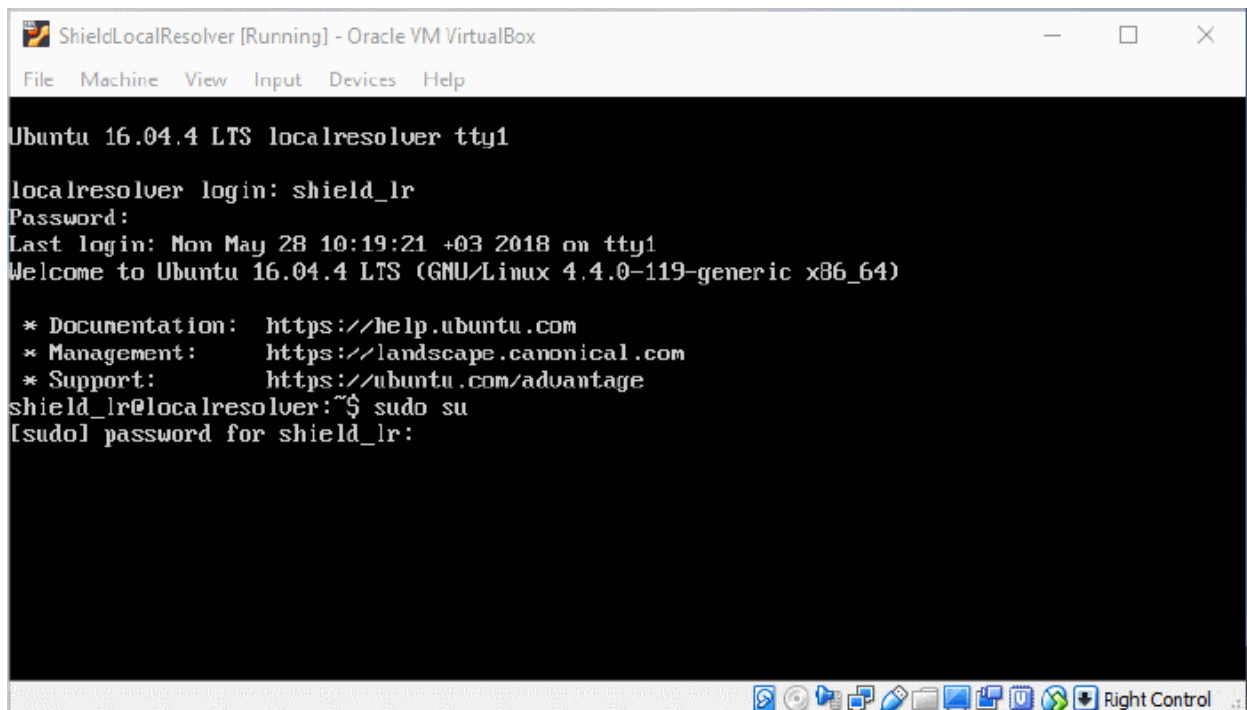


Configure the Local Resolver

- Start up the VA once installation is complete.

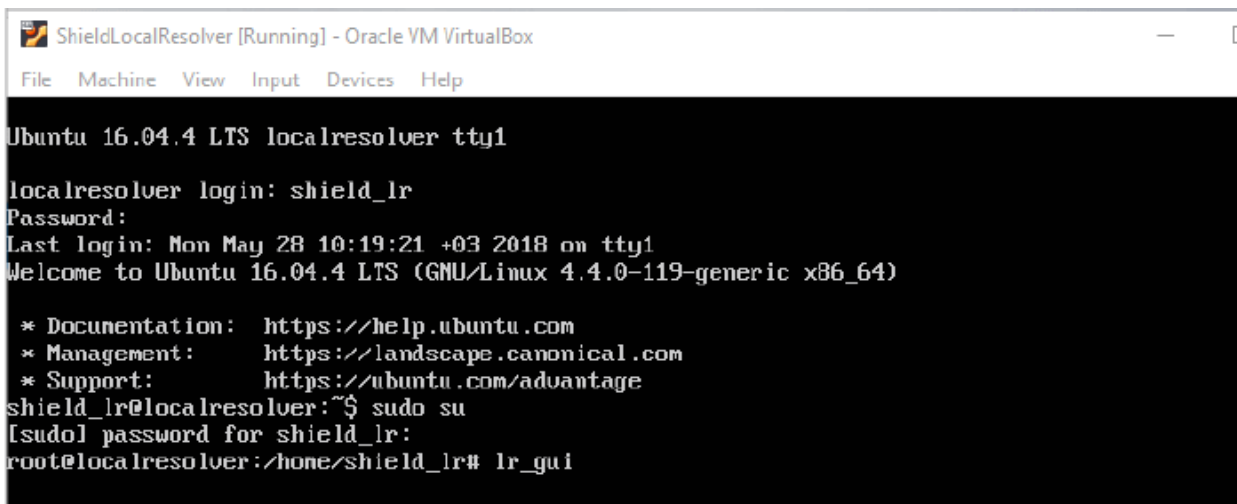


- Login to the appliance with the username and password in credentials.txt. This file is in the VA package you downloaded.

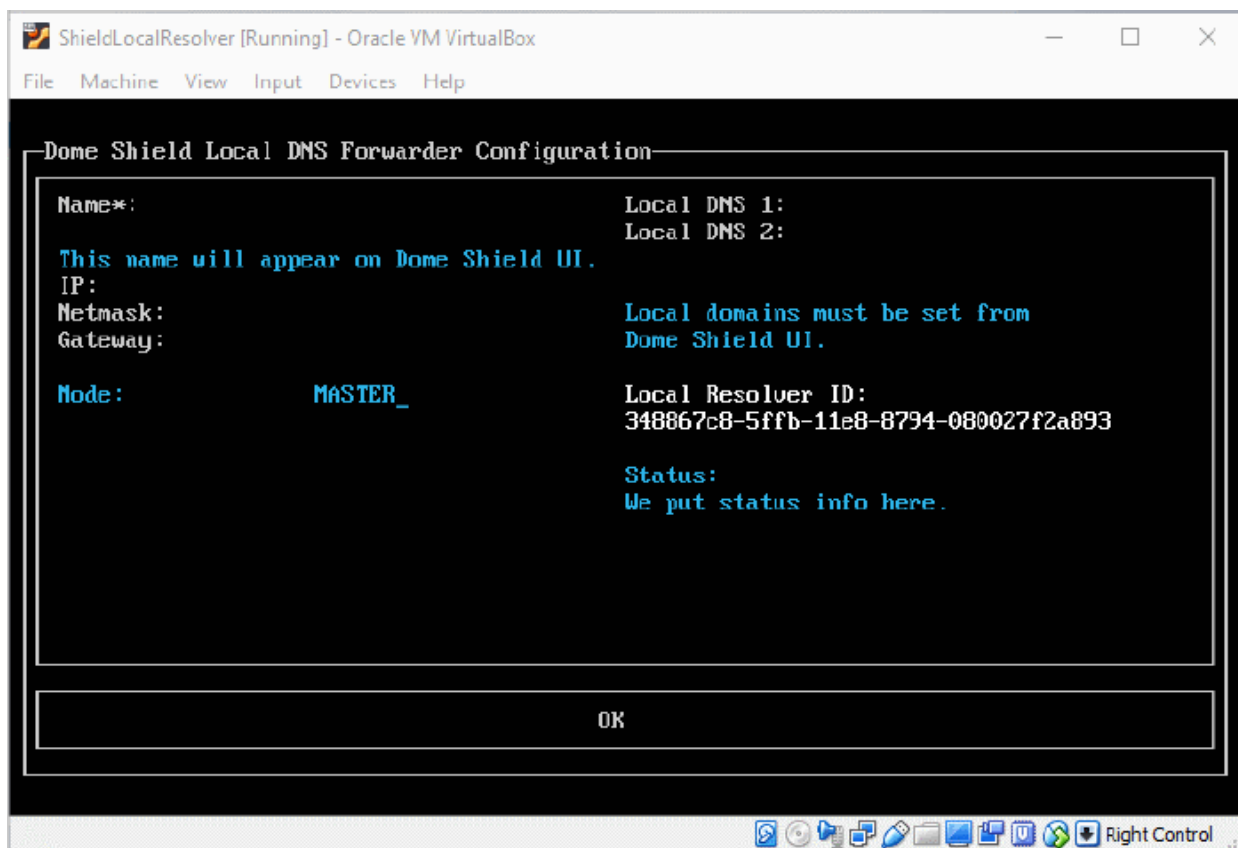


- Run the 'sudo su' command and enter the root password contained in the 'credentials.txt'. This gives you root access.

Run 'lr-gui' command as shown below to open the resolver configuration screen:



The resolver configuration screen opens.



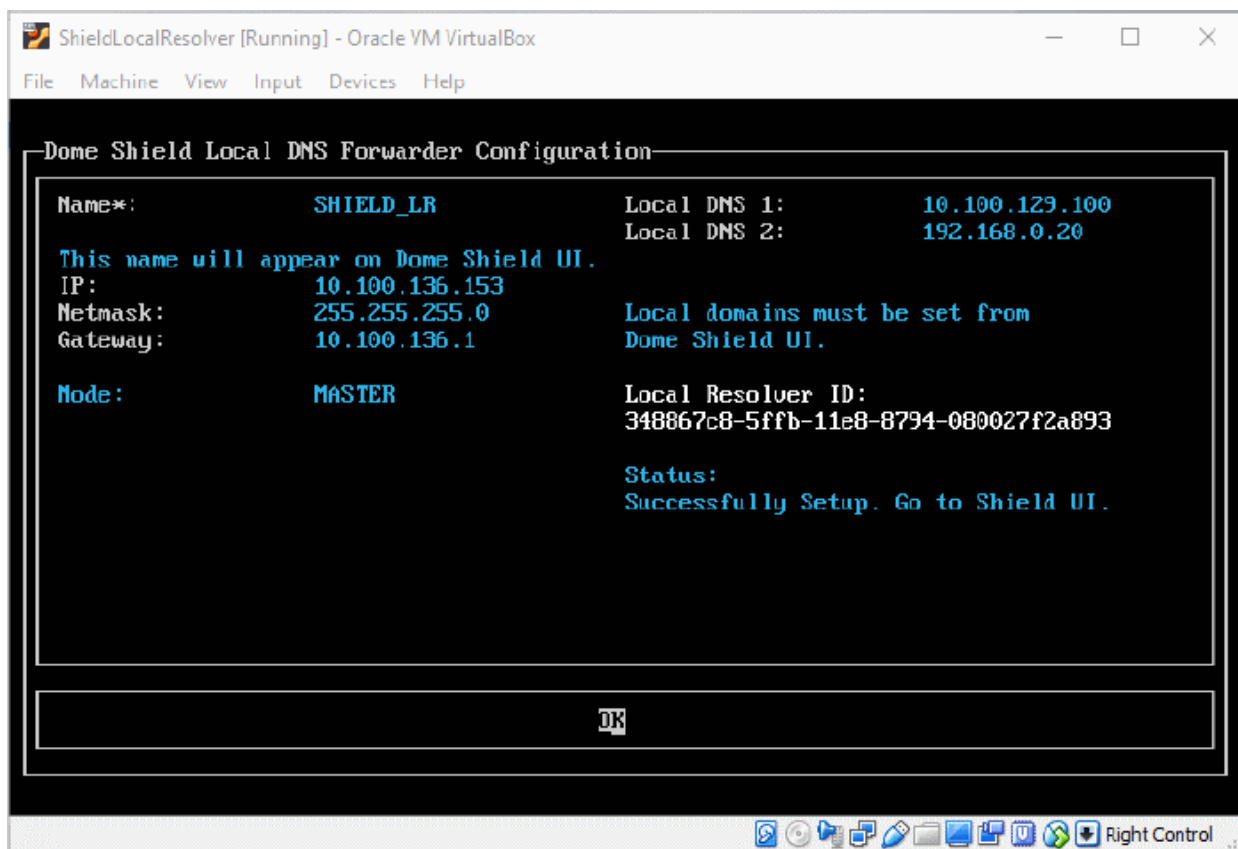
LR Configuration Screen

Form Element	Description
Name	Type a label to identify the master VA. This name will appear in the Secure Internet Gateway interface after registration.
IP	Assign an IP address to the local resolver.
Netmask	Enter the LR netmask
Gateway	Enter the IP address of the network gateway.
Mode	Select 'Master' if this is the first resolver on the network.

Local DNS 1 and Local DNS 2	Enter the IP addresses of the primary and secondary DNS servers in the network.
Local Resolver ID	Make a note of this ID string. You need this to register the resolver and import the network into Secure Internet Gateway. See Step 3 - Register the Master VA for more help.
Status	Progress of the VA setup process.

- Configure the parameters, select OK and press 'Enter'

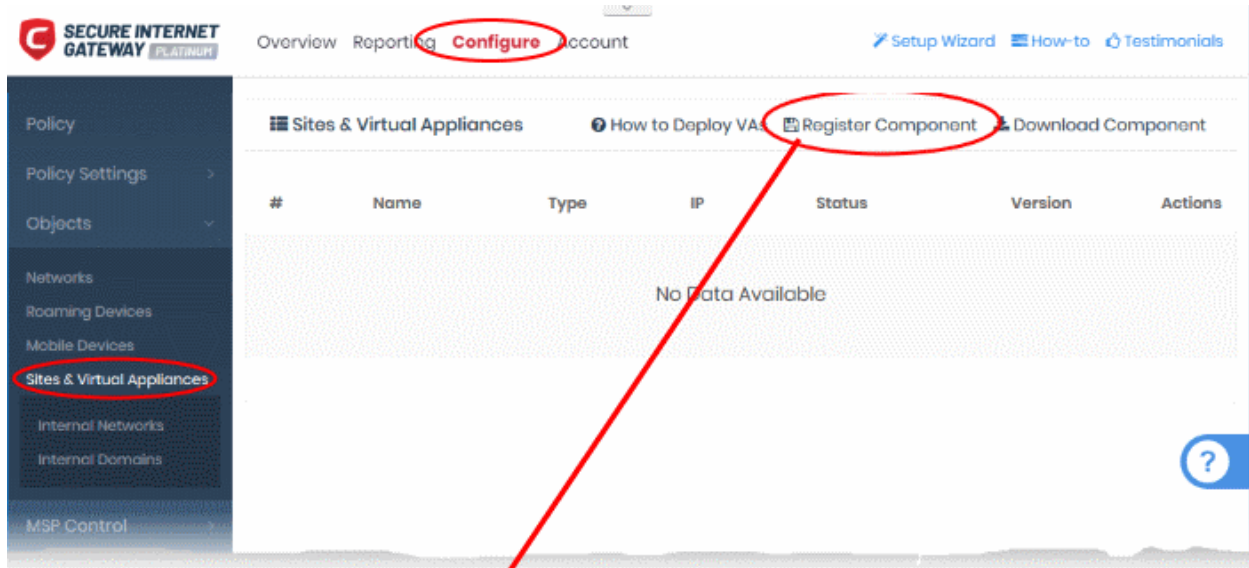
Your configuration is saved.



The next step is to register the LR with Secure Internet Gateway.

Step 3 - Register the Master VA

- Login to Secure Internet Gateway
- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances'
- Click 'Register Component'



ADD LOCAL RESOLVER ✕

Enter Registration ID of the Component

If you have installed 1 LR for your site, enter its registration ID. If you have installed more than 1 LR, you can enter Registration ID of any of them as others will automatically be retrieved into your site to provide high-availability. Read more about it [here](#).

Enter Site Name

Type a new Site name you want your LRs to be assigned.

Select Company

Select the company you want the Site and its LRs to be assigned.

Unclear? Please check [How To Deploy](#) again!

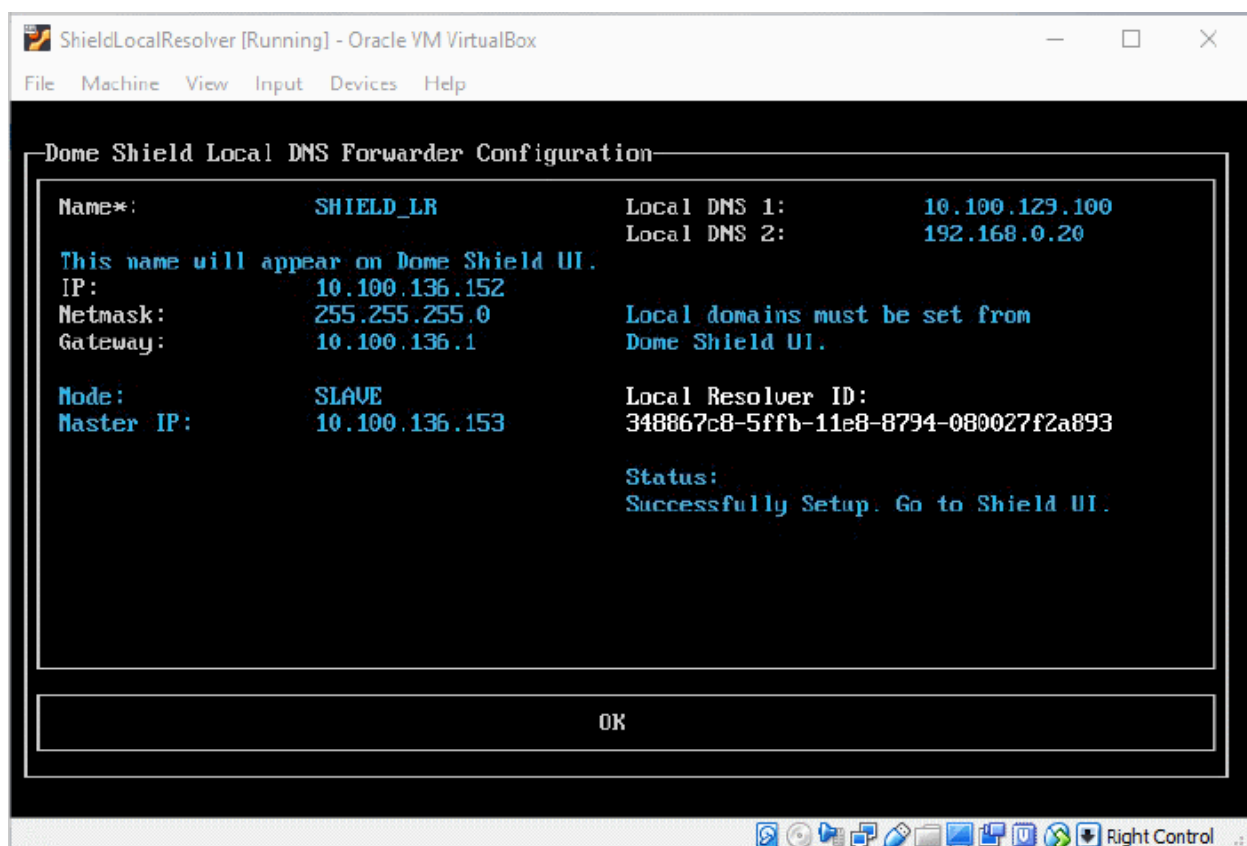
'Add Local Resolver' dialog - Table of Parameters	
Form Element	Description
Enter Registration ID of the Component	The local resolver identity string generated for the resolver during setup. See the last screen in Step 2 - Setup the Master Virtual appliance if you need help.
Enter Site Name	Type a label for the network you are about to import. The name is used to identify the network in the Secure Internet Gateway interface.
Select Company	MSPs' only. <ul style="list-style-type: none"> Choose the customer organization whose network you want to import

- Click 'Save' to register the local resolver and import the network

Click 'Sites & Virtual Appliances' to view the local resolver. You can apply policy to the whole network, or to internal network segments. See **Manage Imported Sites and Local Resolver Virtual Appliances** for more details.

Step 4 - Setup the Slave VA (Optional)

- Install a local resolver Virtual Appliance on a different server/host on the network. The process is similar to setting up the master LR.
- Start the VA and open the configuration screen as explained **above**. Setup the VA as a slave resolver:



LR Configuration Screen - Table of Parameters	
Form Element	Description
Name	Type a label to identify the slave VA.
IP	Assign an IP address to the local resolver.

LR Configuration Screen - Table of Parameters	
Form Element	Description
Netmask	Enter the LR netmask
Gateway	Enter the IP address of the network gateway.
Mode	Select 'Slave'
Master IP	Appears after choosing 'Slave' as the mode. Enter the IP address of the master local resolver.
Local DNS 1 and Local DNS 2	Enter the IP addresses of the network's primary and secondary DNS servers.
Local Resolver ID	Make a note of this ID string. You need this to register the resolver and import the network into Secure Internet Gateway. See Step 3 - Register the Master VA for more help.
Status	Progress of the VA setup process.

- Configure the parameters, select OK, then press 'Enter'

Your configuration will be saved. The resolver will be registered as 'Slave' to the 'Master'.

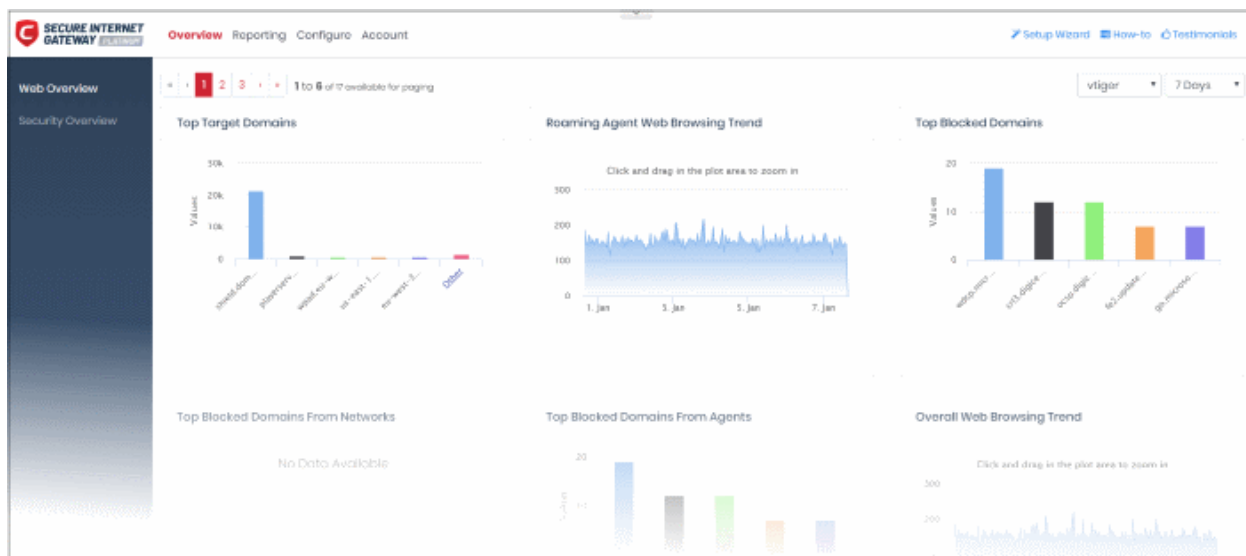
Step 5 - Configure endpoint DNS Settings to point to the local resolvers

The next step is to configure your endpoints to forward DNS queries to the local resolvers. Open the DNS configuration screen on your endpoints and use the following settings:

- Preferred DNS server - IP address assigned to the master LR VA
- Alternate DNS server - IP address assigned to the slave LR VA

2 The Admin Console

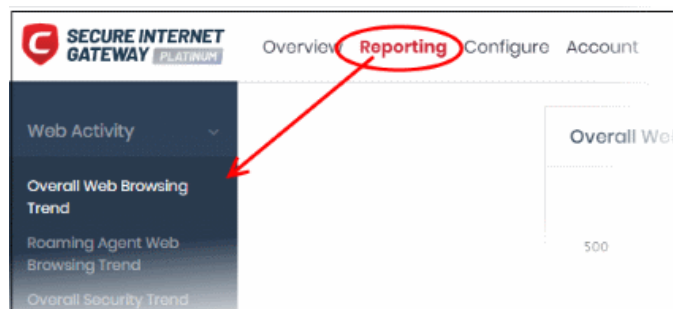
The admin console contains statistics and charts about your protected environment. From here you can add networks and devices, create security policies, analyze threat data and more.



Overview - Contains the web and security dashboards.

These are charts and graphs which show browsing trends, security trends, top URL categories and more.

See '[The Dashboard](#)' for more details.



See '[Reports](#)' for more details.

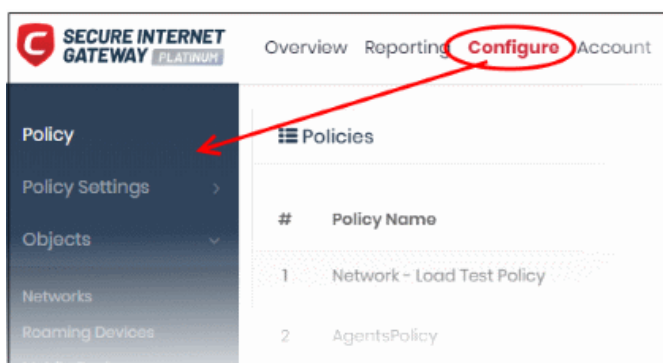
Reporting - View reports on threats detected on your assets, security trends, web browsing trends, and more.

You can choose from a range of preset reports or create a custom report.

You can schedule reports to be generated at specific intervals and sent to recipients of your choice.

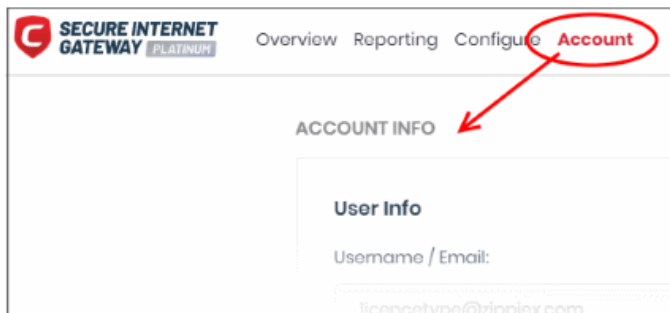
Configure - Add networks and individual endpoints to Secure Internet Gateway, and apply security policies to them.

- **Policy** - Create and deploy policies to protected networks and endpoints. Each policy is made up of security rules, category rules and/or black/white lists. See '[Apply Policies to Networks and Roaming / Mobile Devices](#)' for more details.
- **Security Rules** - Create and manage rules to block websites which host specific threat types. See '[Manage Security Rules](#)' for more details.
- **Category Rules** - Create and manage rules to block sites by content type. See '[Manage Category Rules](#)' for more details.
- **B/W Lists** - Create and manage lists to block or allow specific domains. See '[Manage Domain Blacklist and Whitelist](#)' for more details.
- **Block Pages** - Configure pages which are shown to end-users when access to a website is blocked. See '[Manage Block Pages](#)' for more details.
- **Cloud Browser** - Configure virtual browsing sessions and assign to policies. This helps users visit websites without the need to block them. See '[Configure Cloud Browser Settings](#)' for more information.
- **Networks** - Add and manage protected networks. See '[Add Networks](#)' for more details.
- **Roaming Devices** - Add and protect roaming devices outside your network. See '[Add Roaming Endpoints](#)' for more information.
- **Mobile Devices** - Add and protect Android and iOS devices. See '[Add Mobile Devices](#)' for more details.
- **Sites & Virtual Appliances** - Add networks by configuring local resolver virtual machines. See '[Import Sites to Secure Internet Gateway by Deploying Local Resolver Virtual Appliances](#)' for more details.
 - **Internal Networks** - Add internal IPs or IP ranges. See '[Add Internal Sites](#)' for more details.
 - **Internal Domains** - Add internal domains inside the imported site. The local resolvers use local DNS servers in the network to handle client requests for internal domains. This is instead of forwarding them to global DNS servers, reducing your bandwidth usage. See '[Add Internal](#)'



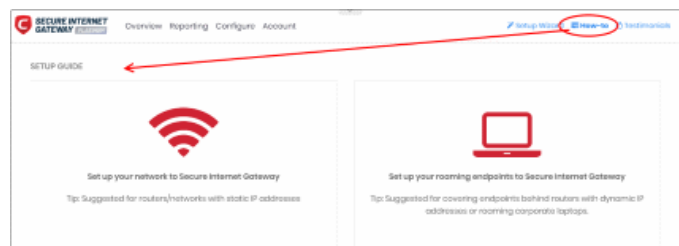
Domains for more details.

- **Customers** - View details about customer networks and roaming agents. This section is available for MSPs only. See '**View Protection Details by Customer**' for more information.

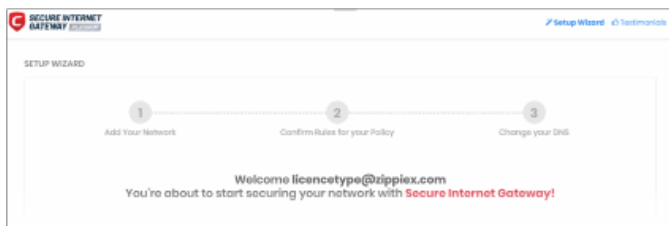


Account - View your account details and keep track of DNS requests. See '**View Account Details**' for more information.

How-to - Tutorials on how to enroll networks and endpoints, configure rules and policies, and view reports.



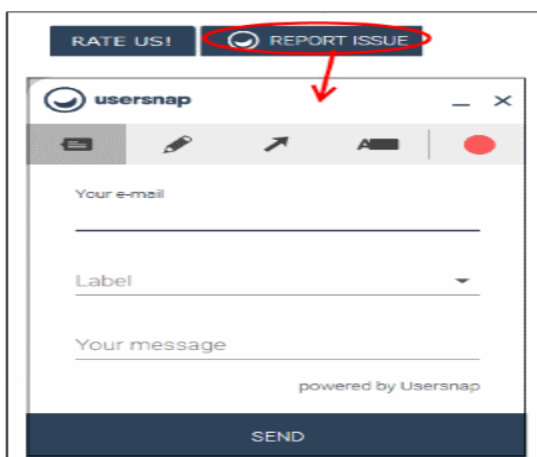
Setup Wizard - Add a network in three steps and apply policy.



Testimonials - Read reviews and comments on Secure Internet Gateway given by our valued customers.



Feedback - Send your comments, questions or report a bug.



- Click 'Report Issue' at the bottom of the interface
- Use the tools at the top of the feedback form to mark, point, highlight or comment on the CSIG interface.
- Complete the feedback form and click 'Send'
- A ticket will be created and our support team will respond to your query.

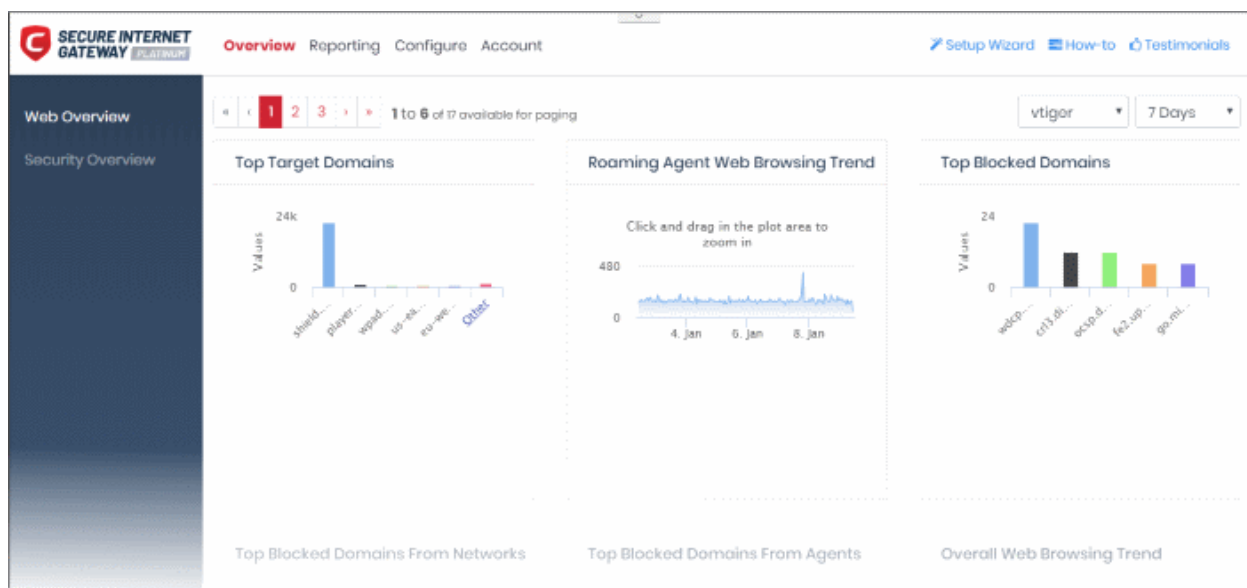
Rate Us - Click this button and select how likely are you to recommend CSIG to your friends. Also provide your valuable suggestions to improve the product.

3 The Dashboard

- Click 'Overview' in the top-menu to open the dashboards.
- The dashboard is an at-a-glance summary of your security posture under Secure Internet Gateway.
- You can use the dashboard's range of statistics and charts to view vital information about your deployment. You can also drill-down to further areas of interest.
- Charts include security trends, browsing trends, roaming devices, most frequently blocked domains, and more.

The dashboard is divided into two sections:

- **Web Overview** - Statistics about the websites visited by endpoints in your network.
- **Security Overview** - Statistics about security incidents and blocked threats on your network.



MSP customers can view statistics for particular customers. Possible data ranges are from the last 12 hours to the previous 7 days.

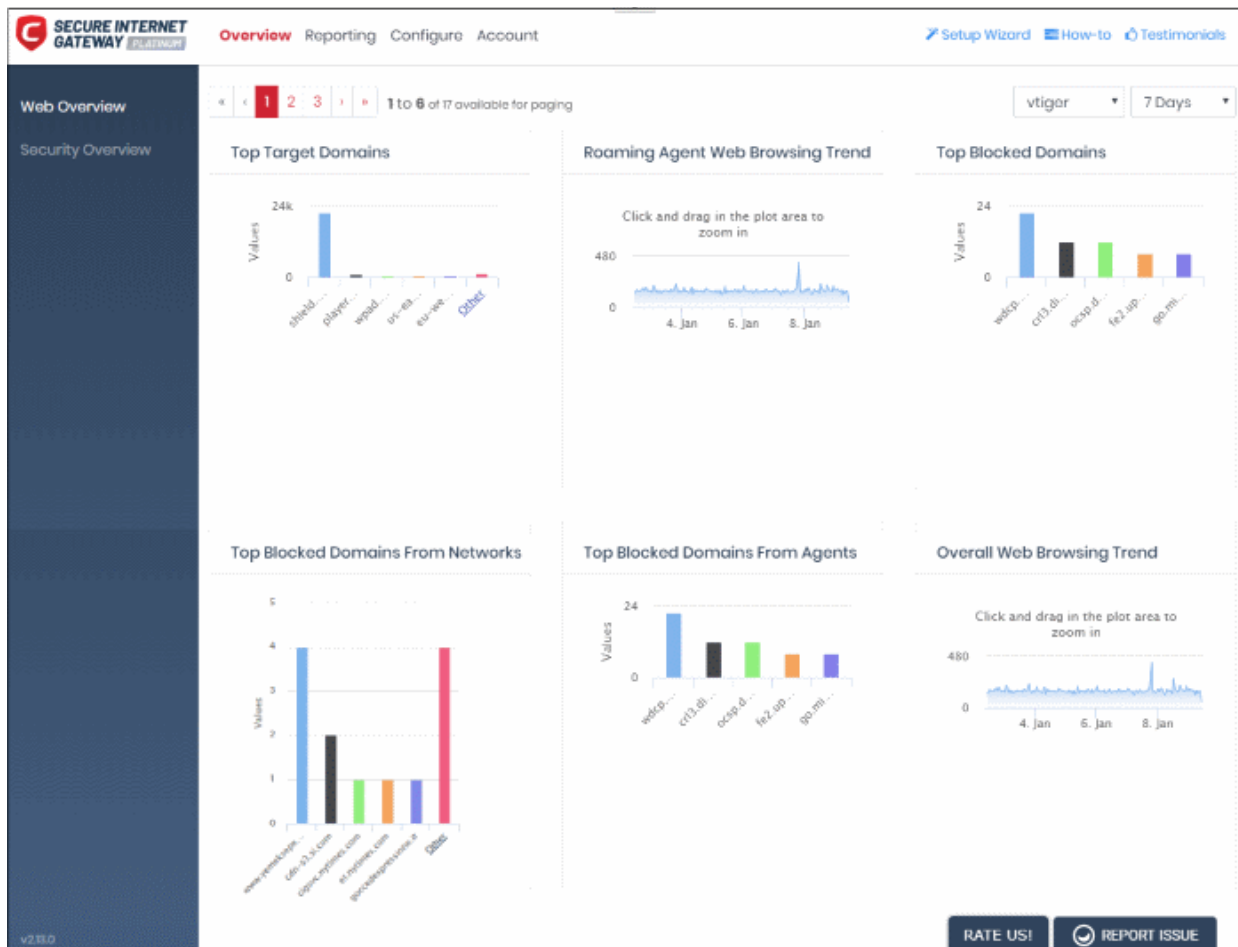
See the following sections for more information:

- **Web Overview**
- **Security Overview**
- **View Logs from the Dashboard**

3.1 Web Overview

The web overview contains data about the websites visited by your enrolled networks and devices.

- Click 'Overview' > 'Web Overview' to open the section

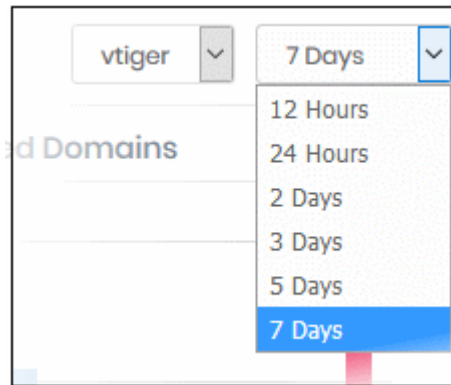


'Web Overview' contains the following tiles:

- **Top Target Domains**
- **Roaming Agent Web Browsing Trend**
- **Top Blocked Domains**
- **Top Blocked Domains from Networks**
- **Top Blocked Domains from Agents**
- **Overall Web Browsing Trend**
- **Overall Security Trend**
- **Top URL Categories**
- **Top Target Domains of Mobile Users**
- **Web Traffic of Mobile Users**
- **Top Blocked Categories of Mobile Users**
- **Sites - Top Target Domains**
- **Sites - Overall Web Browsing Trend**
- **Sites - Top Blocked Categories**
- **Top Visited Sites on CCB**
- **Top Opened Sessions on CCB**
- **File Download on CCB**

MSP customers can view statistics for particular customers. Possible data ranges are from the last 12 hours to the

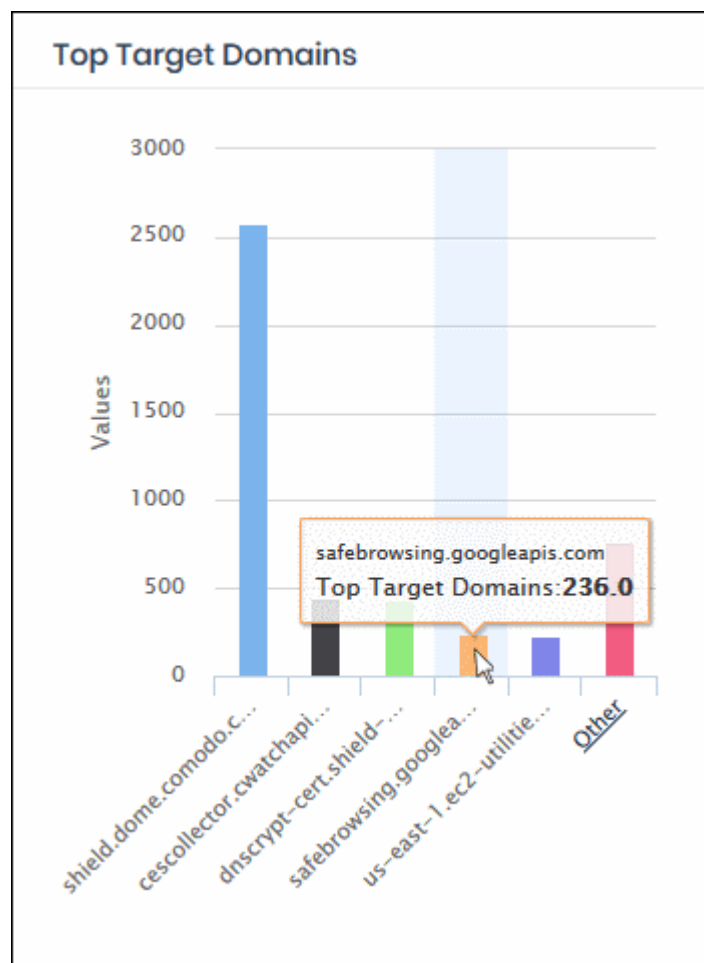
previous 7 days.



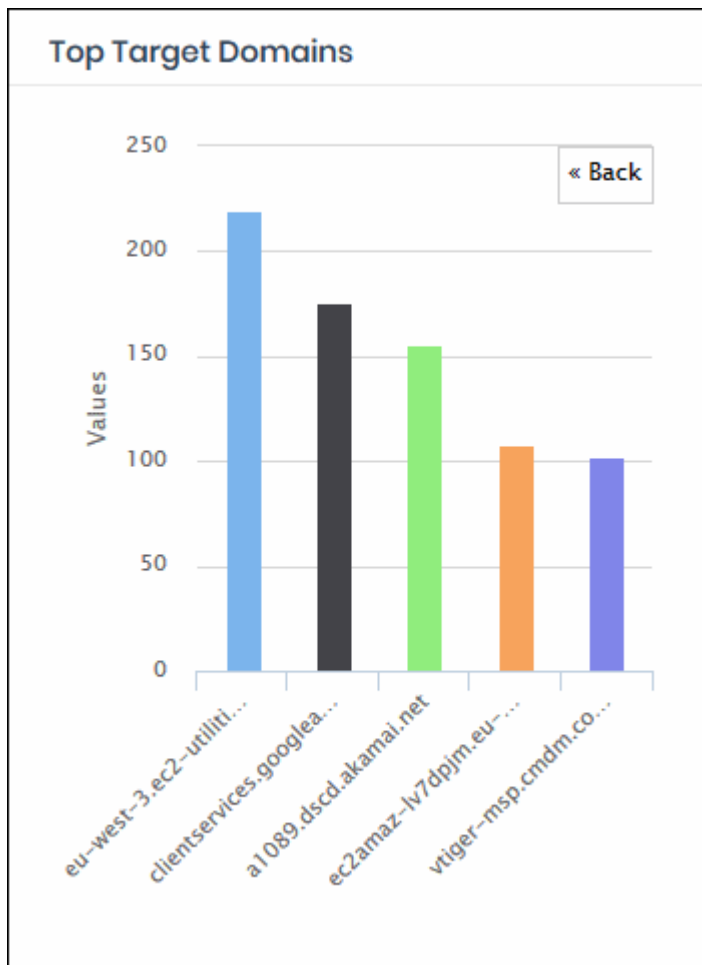
Top Target Domains

Shows the websites which were most often visited by users in your protected networks.

- The X-axis shows the name of the domain. The Y-axis shows the number of requests from endpoints in your networks or roaming devices.
- Place your mouse cursor over a bar to view further details.



- The chart shows the top five domains by default. Click 'Other' to view the next five domains.

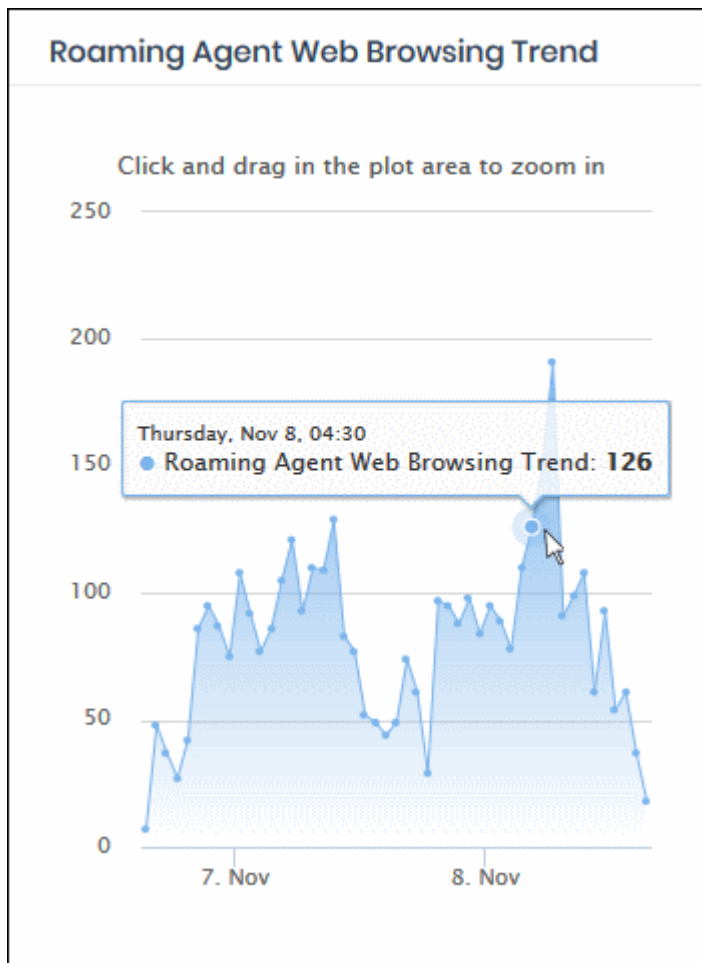


- Click 'Back' to return to the original view.
- Click a particular bar to access requests for the domain. See '**View Logs**' for more details.

Roaming Agent Web Browsing Trend

Shows the number of domain access requests by roaming devices over time.

- Results are available from the last 12 hours up to a maximum of 7 days.
- Place your mouse cursor over a point in the chart to view further details.

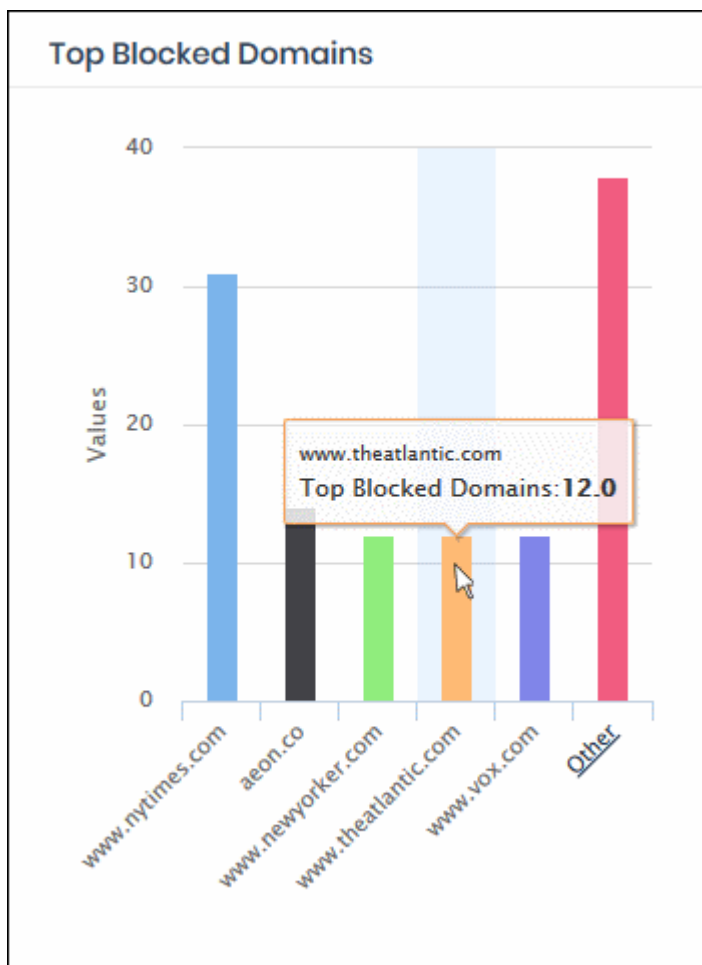


- Click and drag on the chart to zoom into a particular time period.
 - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view logs of the domain access requests. See **View Logs** for more details.

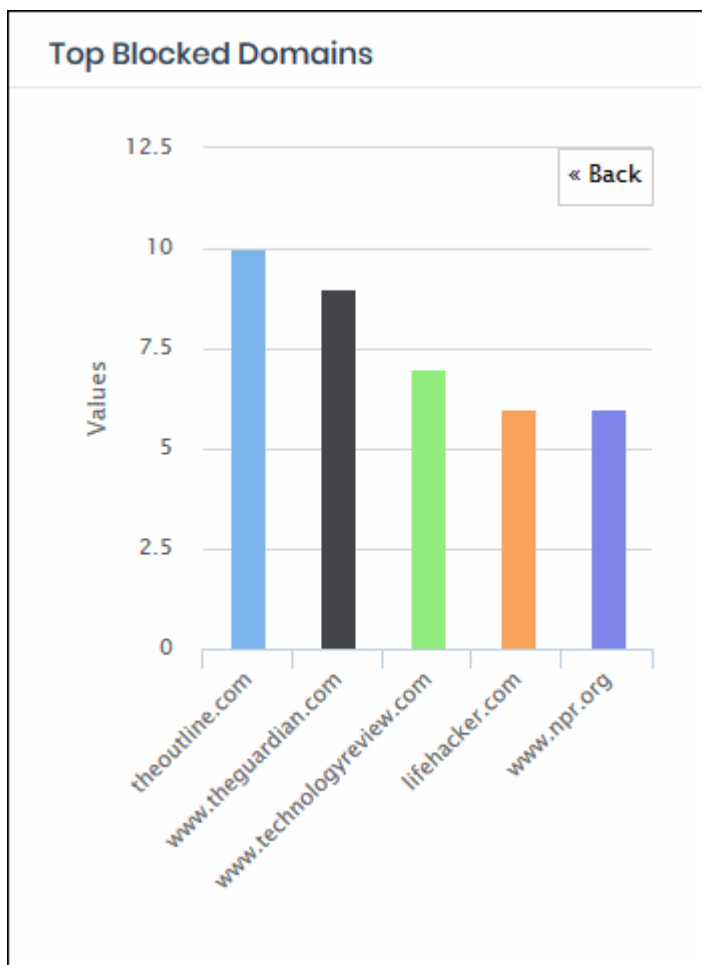
Top Blocked Domains

Shows those websites that were most often blocked by your security policies.

- The X-axis shows the name of the domain. The Y-axis shows the number of requests from endpoints in your networks or roaming devices.
- Place your mouse cursor over a bar to view further details.



- By default, the chart shows top five domains. Click 'Other' to view the next five domains.

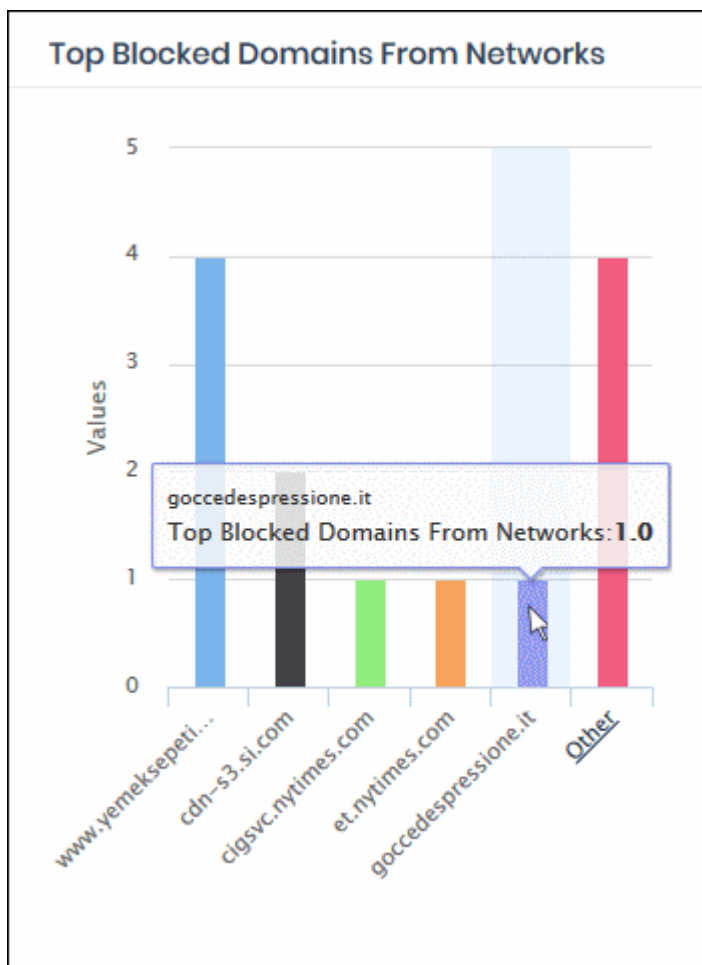


- Click 'Back' to return to the original view.
- Click a particular bar to view access requests for the domain. See '**View Logs**' for more details.

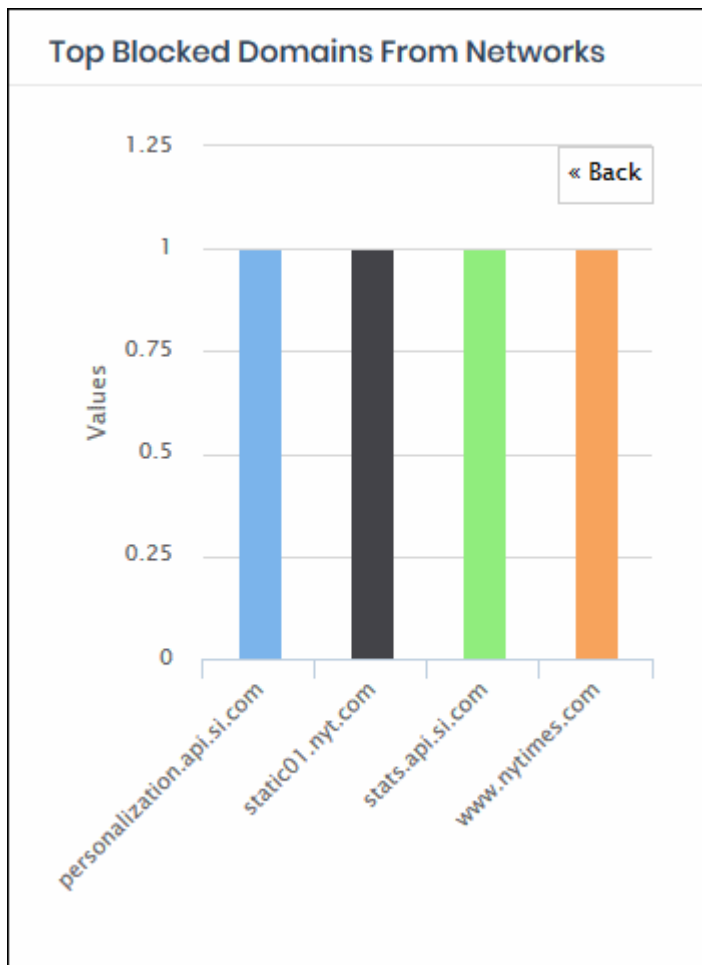
Top Blocked Domains from Networks

Shows the websites that were most often blocked on your managed endpoints.

- Place your mouse cursor over a bar to view further details.



- By default, the chart shows top five domains. Click 'Other' to view the next five domains.

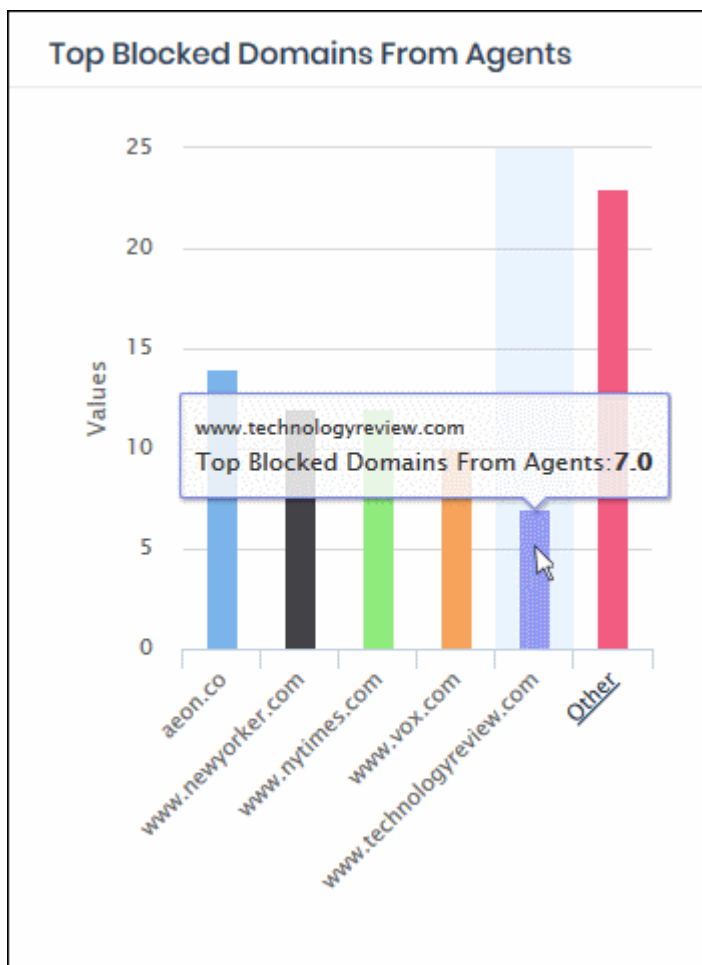


- Click 'Back' to return to the original view.
- Click a particular bar to view access requests for the domain. See '**View Logs**' for more details.

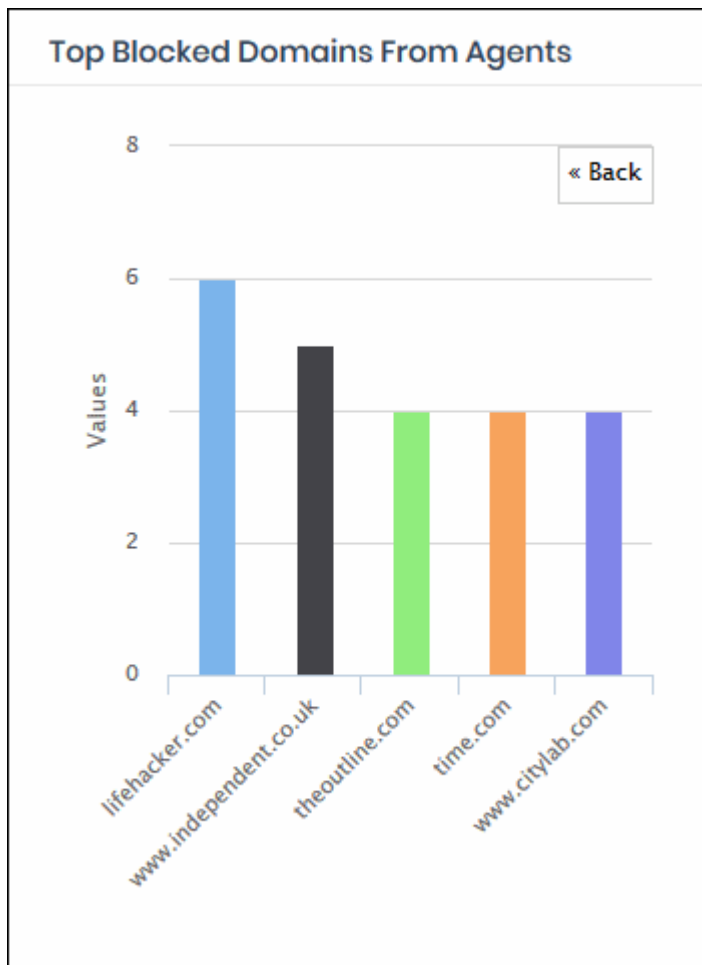
Top Blocked Domains from Agents

Shows the websites that were most often blocked on your roaming devices.

- The X-axis shows the name of the domain. The Y-axis shows the number of requests from endpoints in your networks or roaming devices.
- Place your mouse cursor over a bar to view further details.



- By default, the chart shows top five domains. Click 'Other' to view the next five domains.

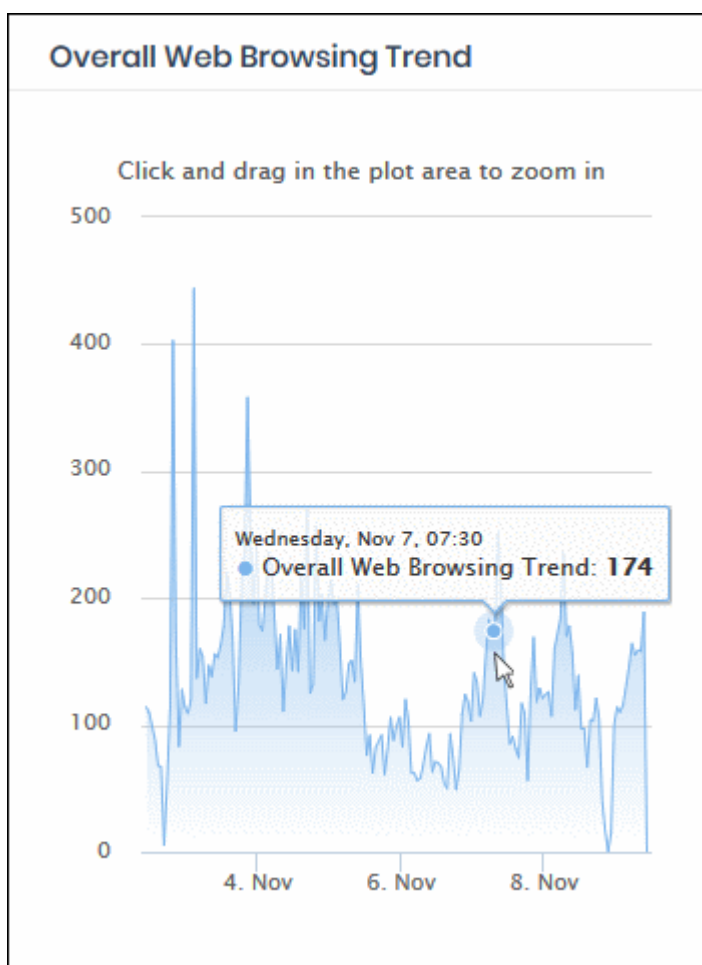


- Click 'Back' to return to the original view.
- Click a particular bar to view access requests for the domain. See '**View Logs**' for more details.

Overall Web Browsing Trend

Shows the number of domain access requests from all protected networks and endpoints over time.

- Results are available from the last 12 hours up to a maximum of 7 days.
- Place your mouse cursor over a point in the chart to view further details.

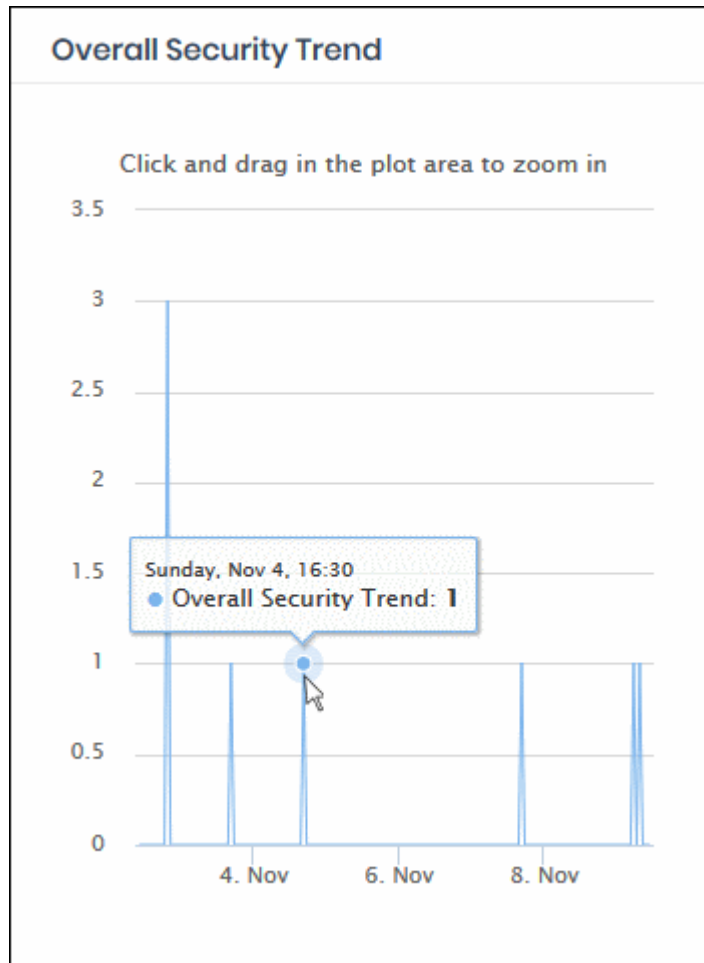


- Click and drag on the chart to zoom into a particular time period.
 - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view logs of the domain access requests. See [View Logs](#) for more details.

Overall Security Trend

Shows the number of harmful sites blocked on your networks and endpoints by your security rules.

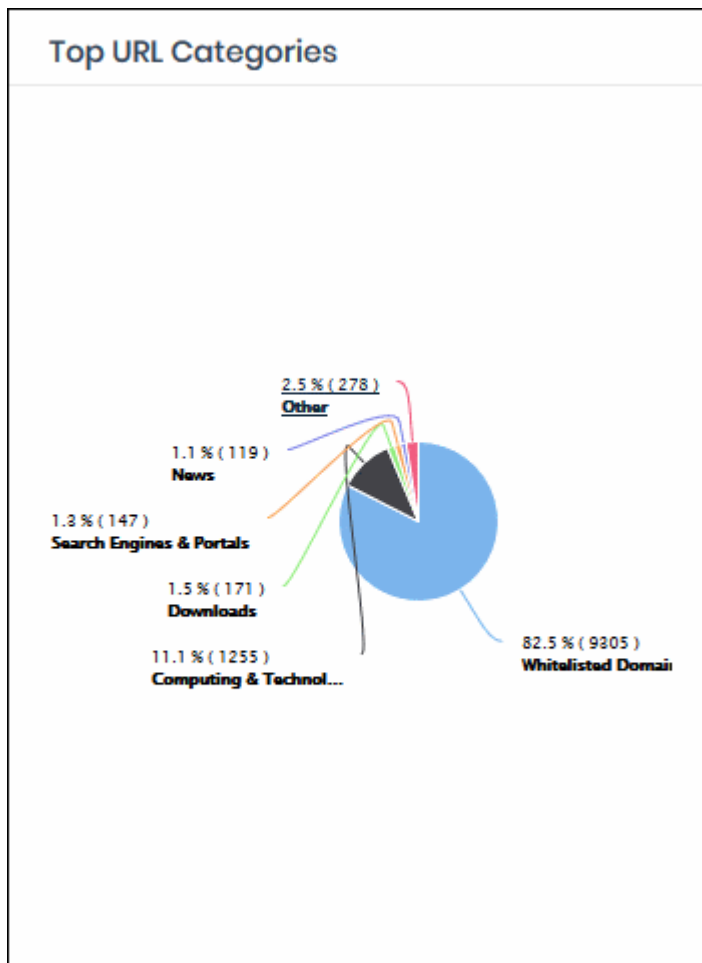
- Results are available from the last 12 hours up to a maximum of 7 days.
- Place your mouse cursor over a point in the chart to view further details.



- Click and drag on the chart to zoom into a particular time period.
 - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view logs of the domain access requests. See **'View Logs'** for more details.

Top URL Categories

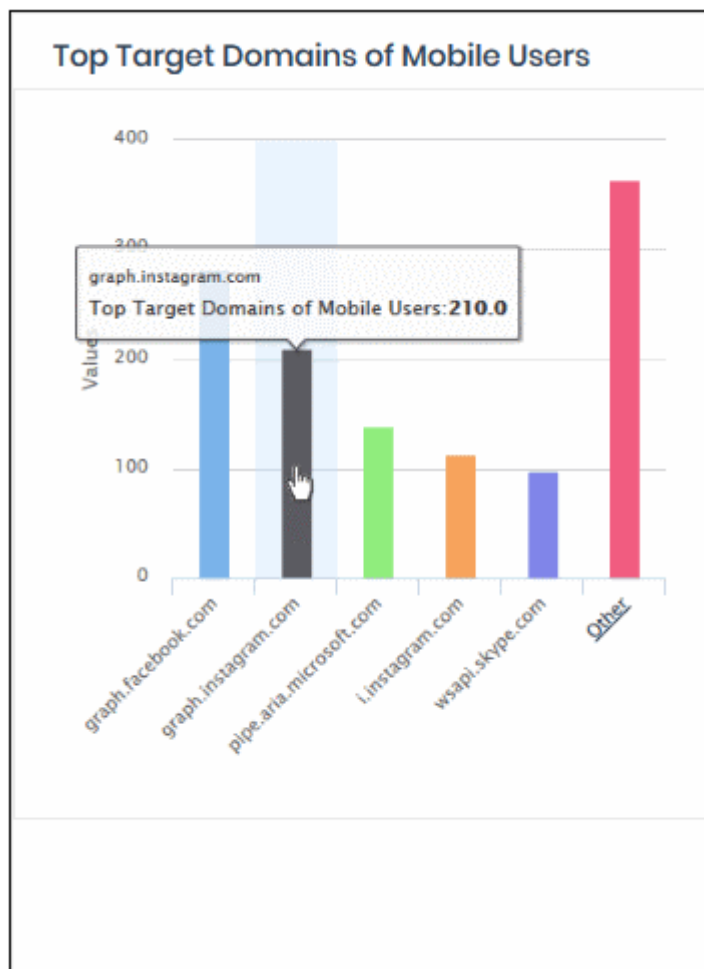
- The website categories and whitelisted domains most often visited by your users.
- Place your mouse cursor over a sector to view further details.
- Click on a sector to see a log of requested domains in that category. See **'View Logs'** for more details..



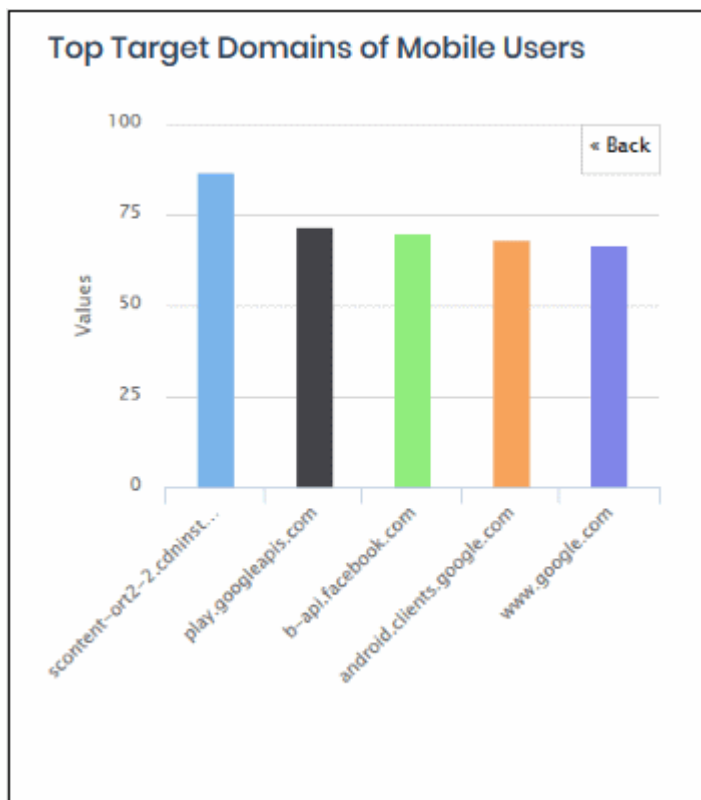
Top Target Domains of Mobile Users

Shows websites which were most often visited by mobile users in your organization.

- The X-axis shows the name of the domain. The Y-axis shows the number of requests from the mobile devices.
- Place your mouse cursor over a bar to view further details.



- By default, the chart shows the top five domains. Click 'Other' to view the next five domains.

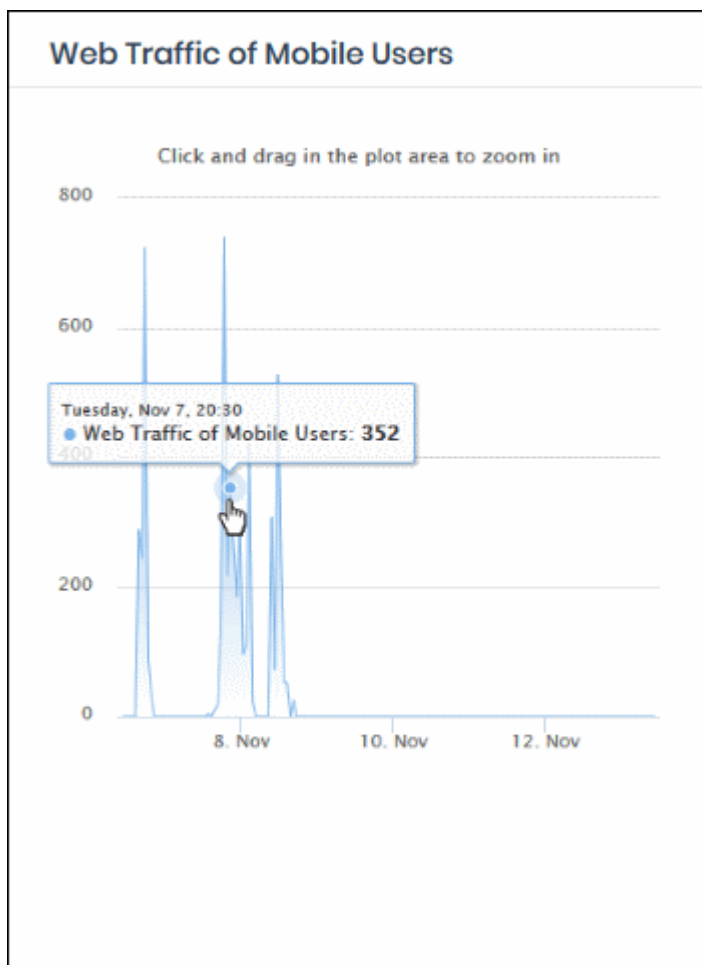


- Click 'Back' to return to the original view.
- Click a particular bar to view logs pertaining to access requests for the domain. See **'View Logs'** for more details.

Web Traffic of Mobile Users

Show the total number of domain access requests from all mobile devices over time.

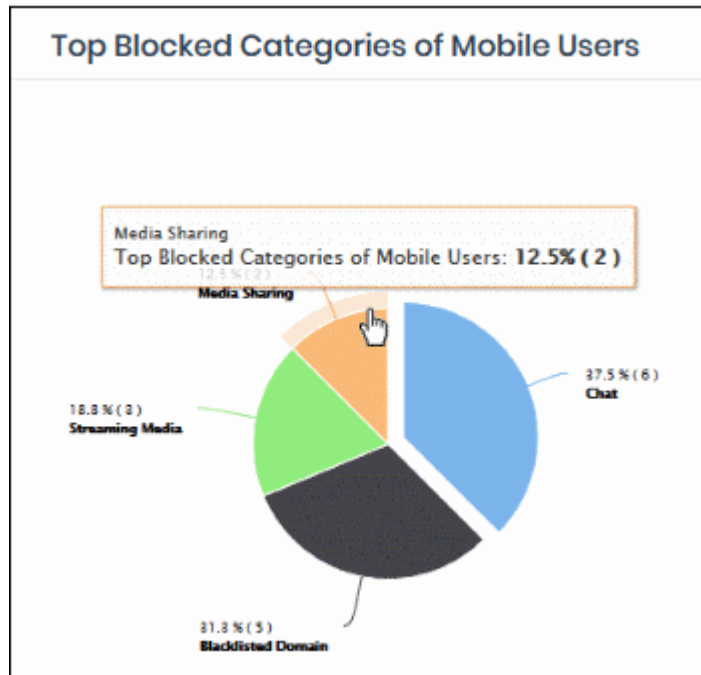
- Results are available from the last 12 hours up to a maximum of 7 days.
- Place your mouse cursor over a point in the chart to view further details.



- Click and drag on the chart to zoom into a particular time period.
 - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view logs of the domain access requests. See **View Logs** for more details.

Top Blocked Categories of Mobile Users

- The website categories and blacklisted domains that were most often blocked to mobile users by category rules in your security policies.
- Place your mouse cursor over a sector to view further details.

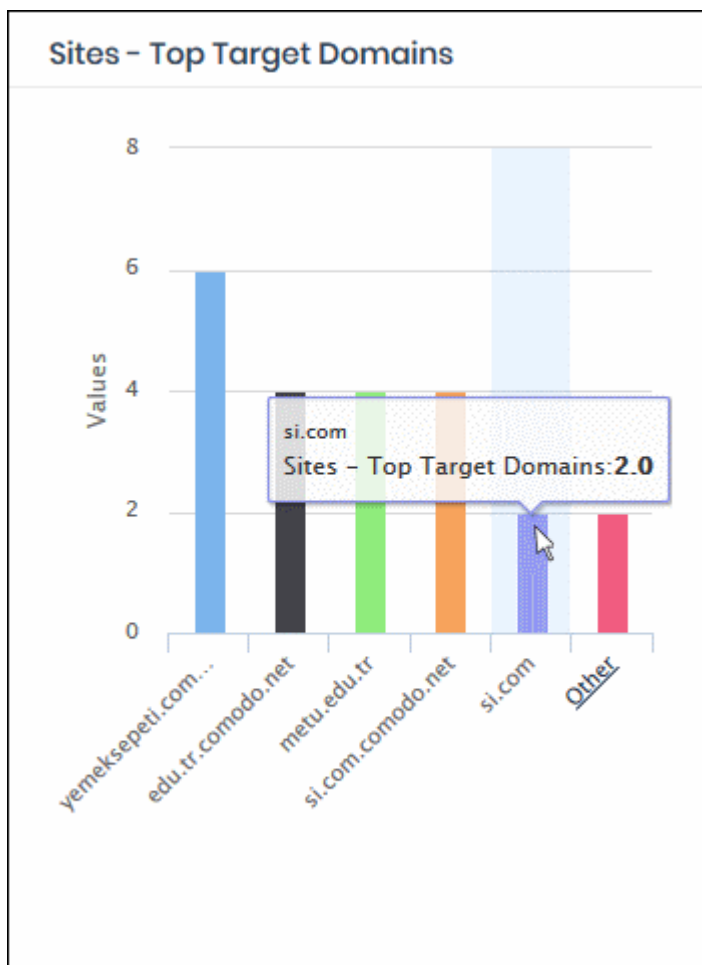


- Click on a sector to see a log of blocked categories for mobile users. See **'View Logs'** for more on this.

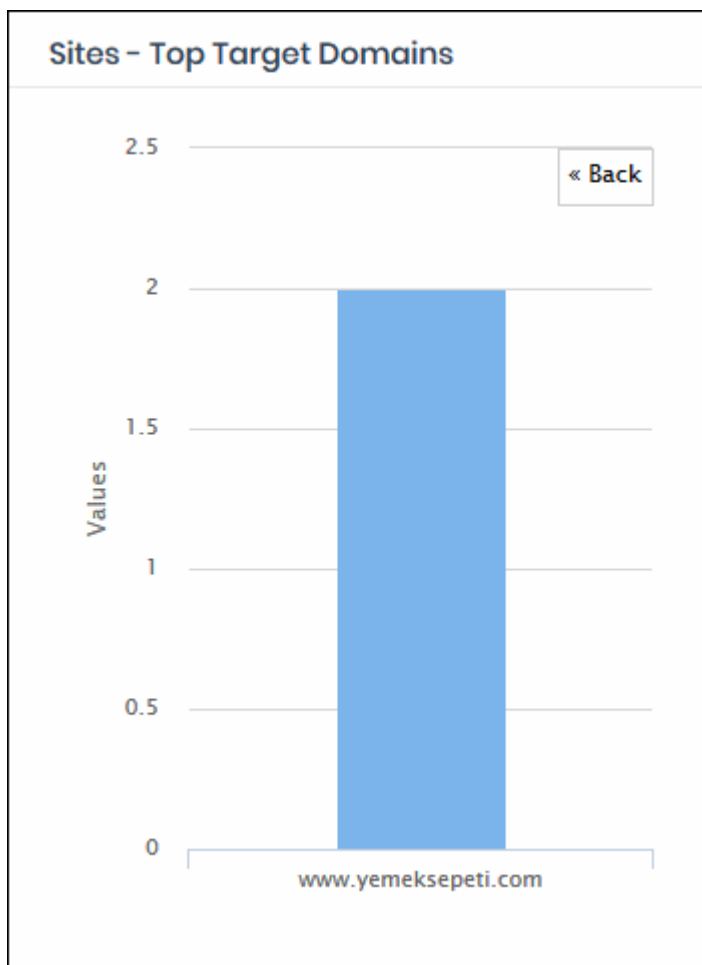
Sites - Top Target Domains

The domains most often visited by users in networks imported by local resolvers. Results are shown for the top 10 domains.

- X-axis - Name of the domain. Y-axis - Number of requests from the network.
- Place your mouse pointer over a bar to view more details.



- By default, the chart shows top five domains. Click 'Other' on the right to view the next five domains.

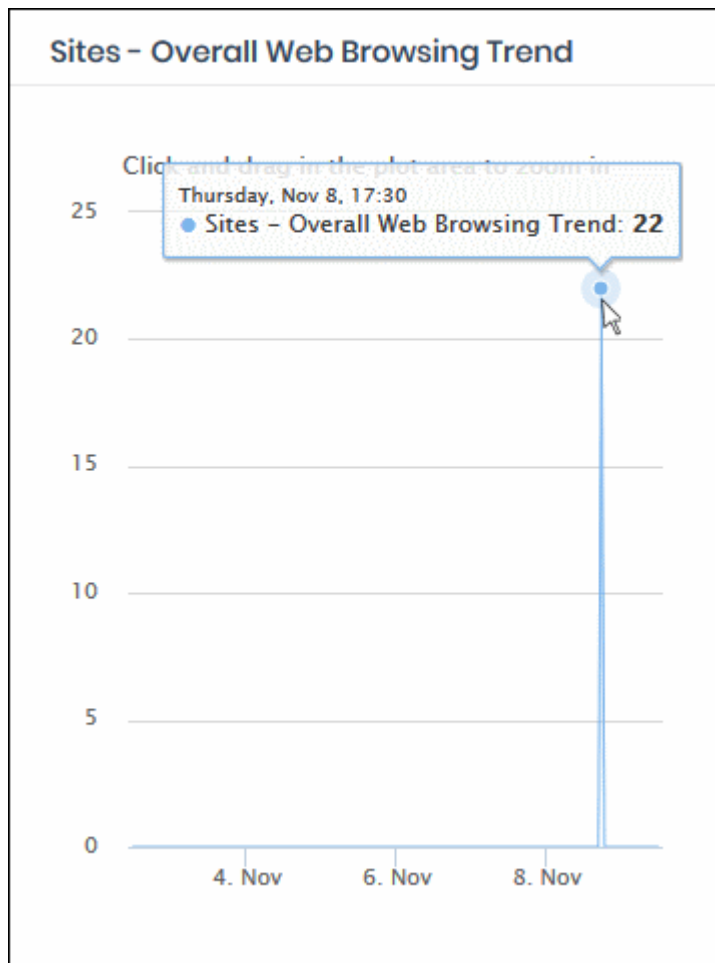


- Click 'Back' to return to the original view.
- Click on a chart bar to view domain request logs. See '**View Logs**' for more details.

Sites - Overall Web Browsing Trend

The domains most often visited by users of all endpoints imported by local resolvers.

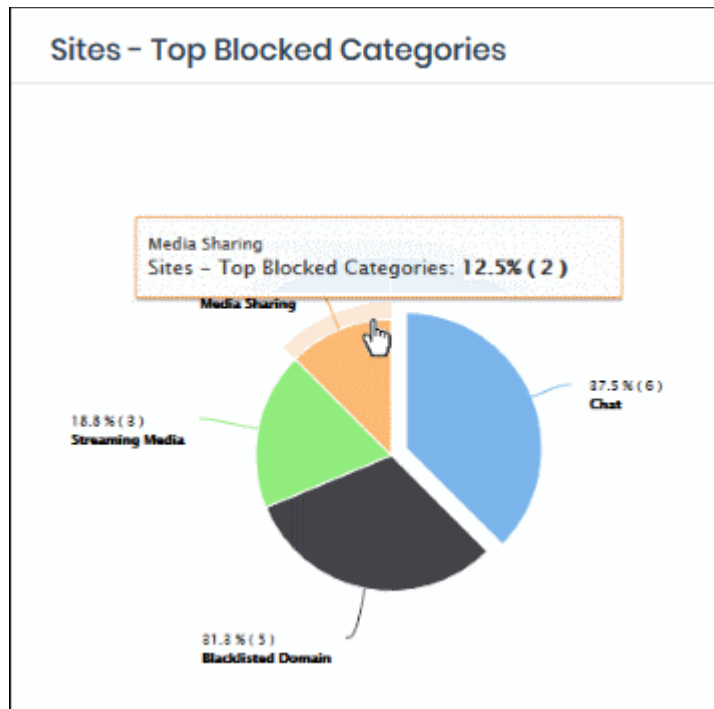
- Results are available from the last 12 hours up to a maximum of 7 days.
- Place your mouse cursor over a point in the chart to view further details.



- Click and drag on the chart to zoom into a particular time period.
 - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view domain request logs. See **'View Logs'** for more details.

Sites - Top Blocked Categories

- Website categories and domains that were most often blocked by rules.
- Place your mouse cursor over a sector to view further details.

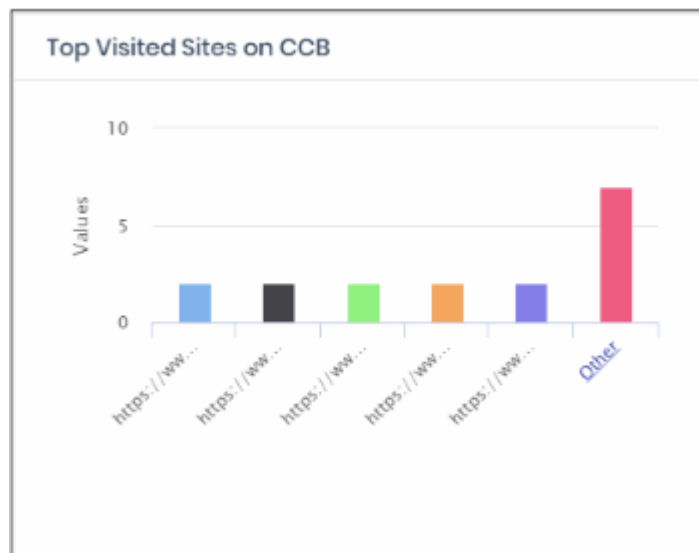


- Click on a sector to see a log of blocked categories. See **'View Logs'** for more on this.

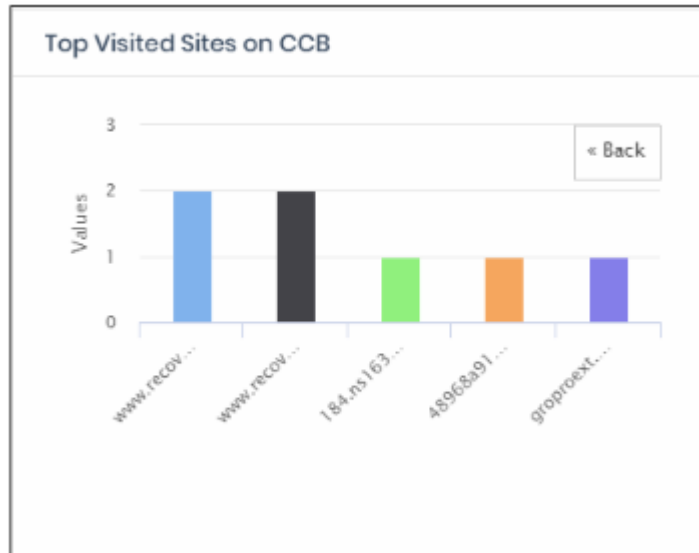
Top Visited Sites on CCB

Shows those websites that were most often visited in virtual sessions.

- The X-axis shows the name of the domain. The Y-axis shows the number of requests from endpoints in your networks or roaming devices.
- Place your mouse cursor over a bar to view further details.



- By default, the chart shows the top five domains. Click 'Other' to view the next five domains.

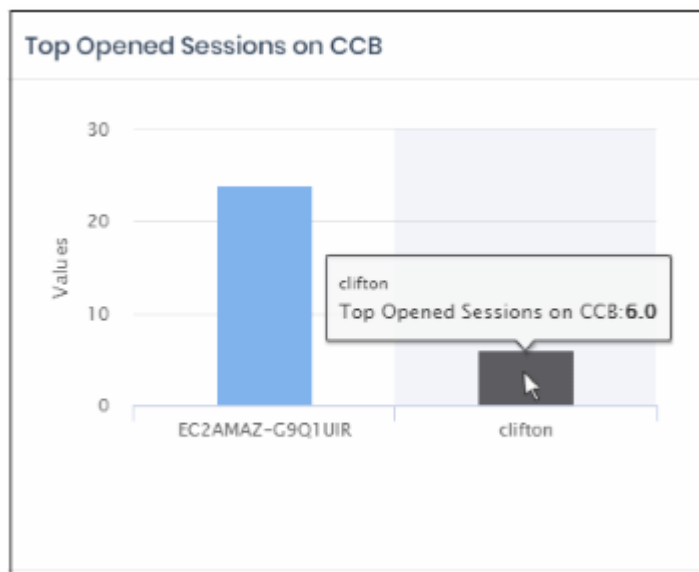


- Click 'Back' to return to the original view.
- Click a particular bar to view access requests for the domain. See '**View Logs**' for more details.

Top Opened Sessions on CCB

Shows devices that most often visited sites in virtual sessions.

- The X-axis shows the name of the device. The Y-axis shows the number requests.
- Place your mouse cursor over a bar to view further details.

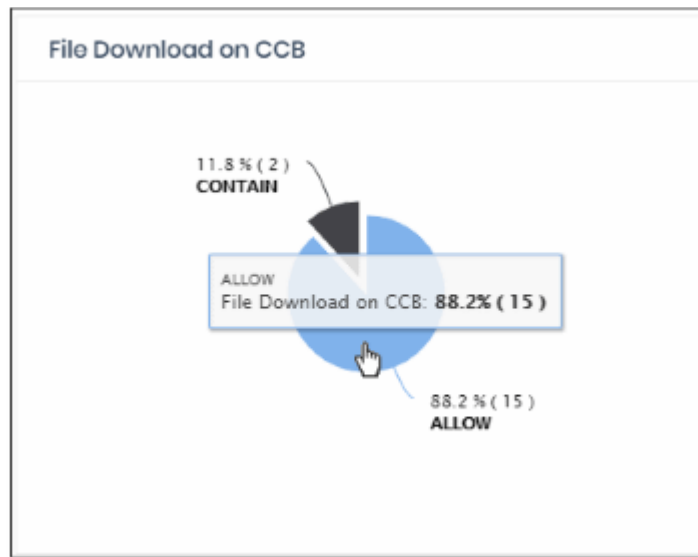


- By default, the chart shows the top five devices. Click 'Other' to view the next five devices.
 - Click 'Back' to return to the original view.
- Click a particular bar to the device virtual sessions. See '**View Logs**' for more details.

File Download on CCB

- Shows a summary of files saved from virtual sessions.
 - Allow - Files scanned and found safe
 - Contain - Unknown / malicious files that were placed in the container (sandboxed)
- Place your mouse cursor over a sector to view further details.

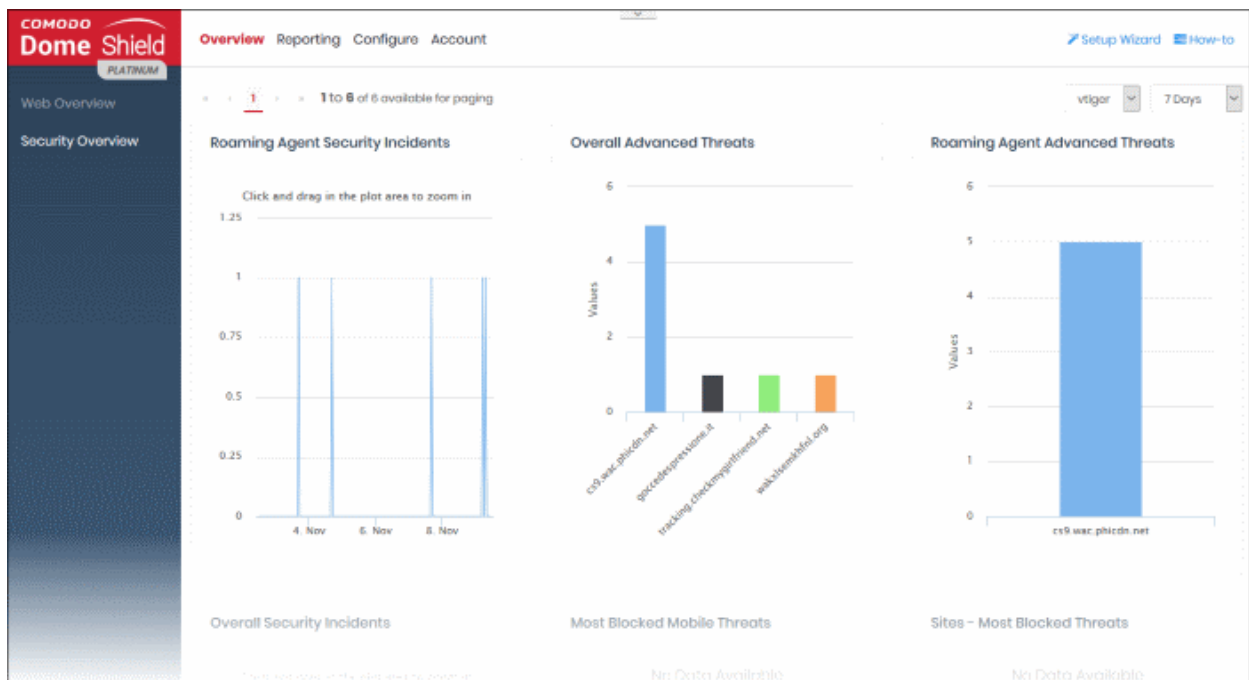
- Click on a sector to view the files downloaded in that category. See **'View Logs'** for more details..



3.2 Security Overview

The 'Security Overview' section contains data on security incidents and websites blocked by rules in your policies.

- Click 'Overview' > 'Security Overview'



The dashboard contains the following tiles:

- **Roaming Agent Security Incidents**
- **Overall Advanced Threats**
- **Roaming Agent Advanced Threats**
- **Top Threat Categories**
- **Overall Security Incidents**
- **Most Blocked Mobile Threats**

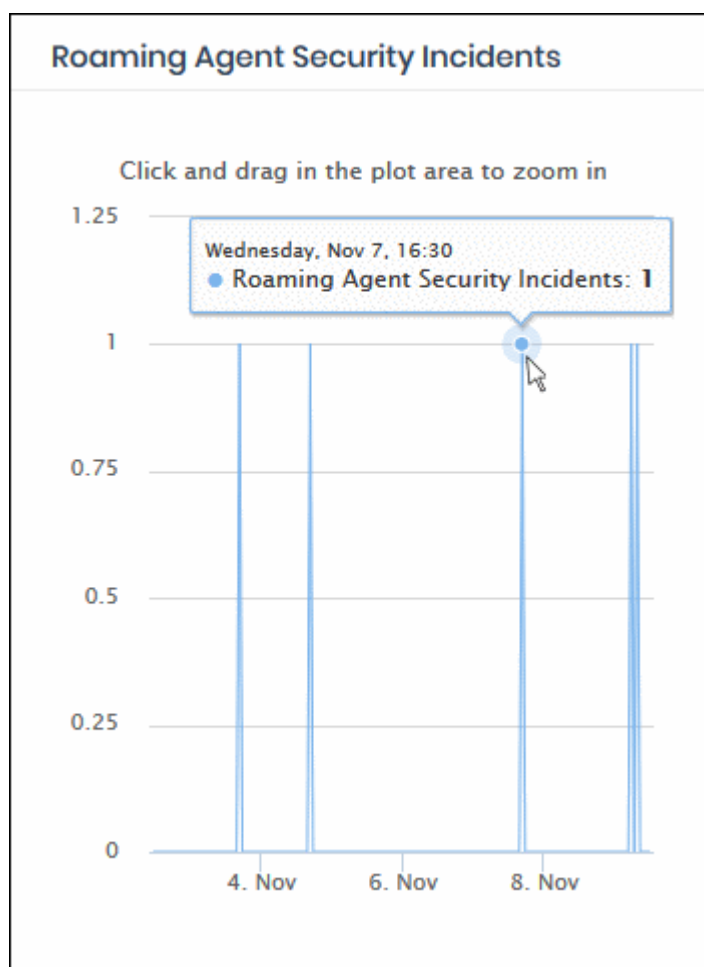
- **Sites - Most Blocked Threats**

MSP customers can view statistics for particular customers. Possible data ranges are from the last 12 hours to the previous 7 days.

Roaming Agent Security Incidents

Shows the number of incidents in which harmful sites were blocked on roaming devices over time.

- Results are available from the last 12 hours up to a maximum of 7 days.
- Place your mouse cursor over a point in the chart to view further details.

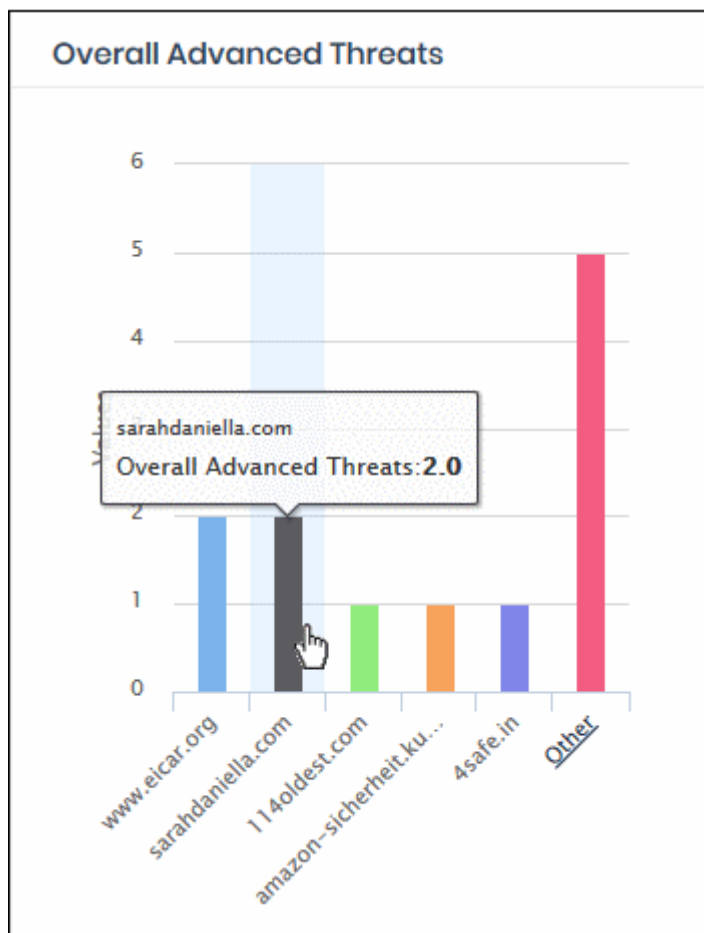


- Click and drag on the chart to zoom into a particular time period.
 - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view the domain access requests. See **'View Logs'** for more details.

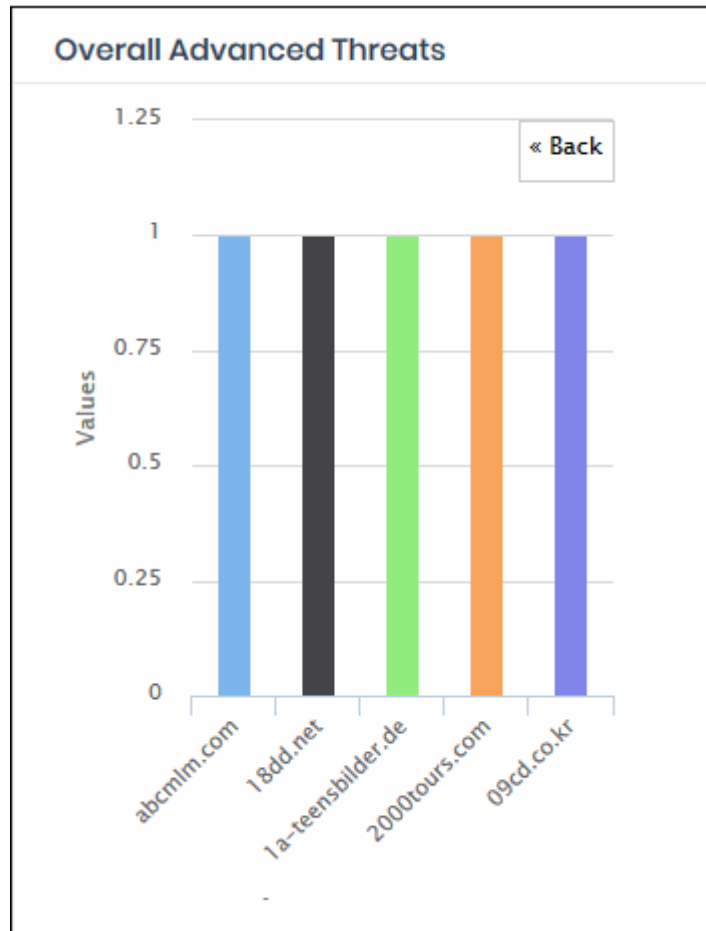
Overall Advanced Threats

Shows the websites that were most often blocked by your security rules. The results cover both enrolled networks and roaming devices.

- The X-axis shows the name of the domain. The Y-axis shows the number of requests from endpoints in your networks or roaming devices.
- Place your mouse cursor over a bar to view further details.



- By default, the chart shows top five domains. Click 'Other' to view the next five domains.

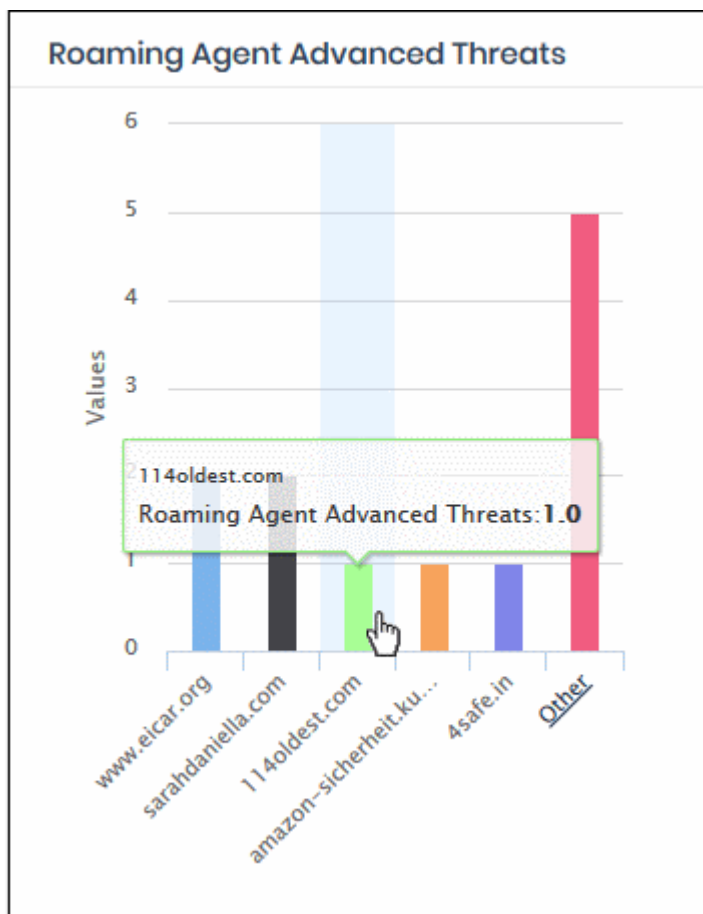


- Click 'Back' to return to the original view.
- Click a particular bar to view access requests for the domain. See '[View Logs](#)' for more details.

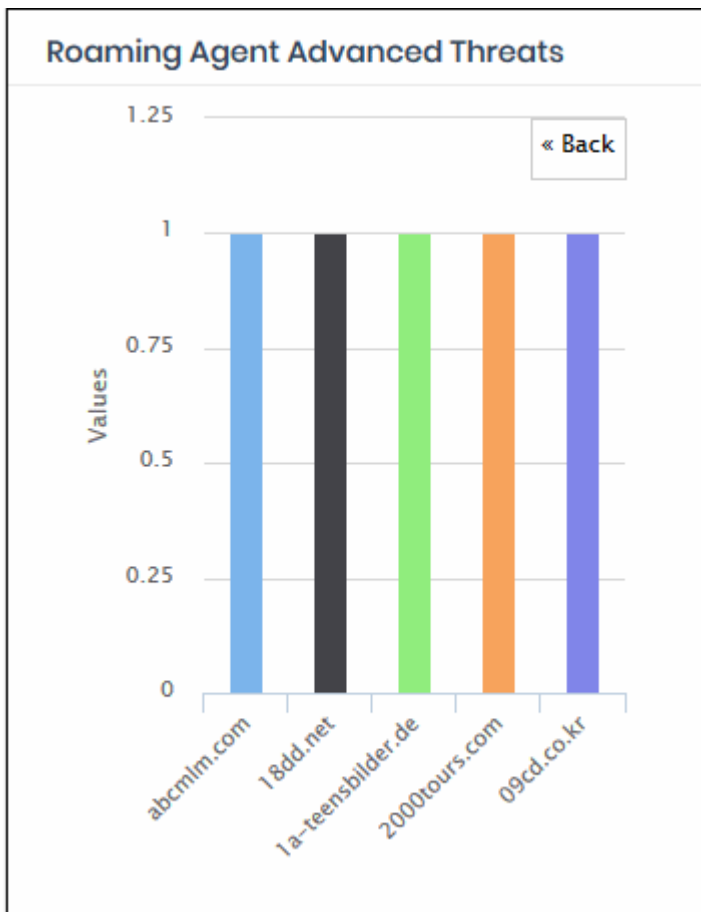
Roaming Agent Advanced Threats

Shows the sites that were most often blocked by your policies after requests from your roaming devices.

- The X-axis shows the name of the domain. The Y-axis shows the number of requests from endpoints in your networks or roaming devices.
- Place your mouse cursor over a bar to view further details.



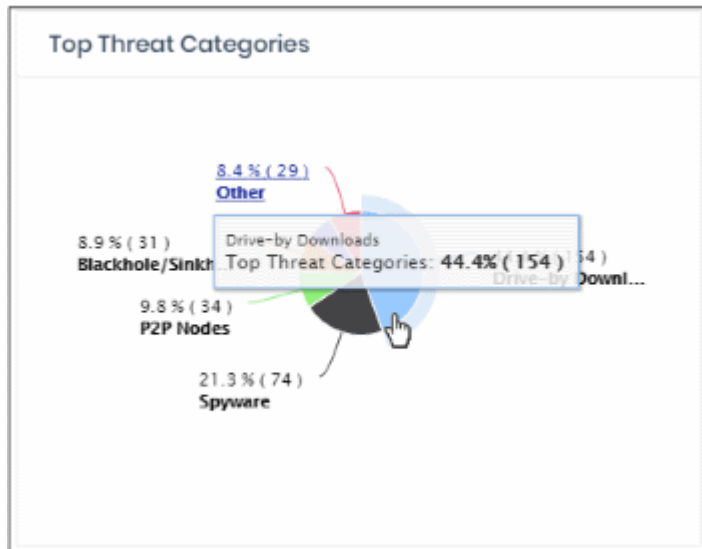
- By default, the chart shows top five domains. Click 'Other' to view the next five domains.



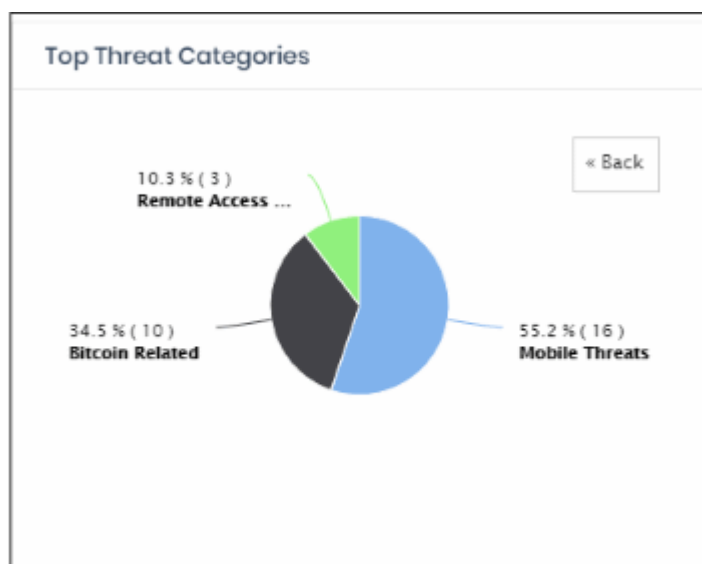
- Click 'Back' to return to the original view.
- Click a particular bar to view access requests for the domain. See '**View Logs**' for more details.

Top Threat Categories

- Shows the blocked website categories which were most often visited by your users.
- Place your mouse cursor over a sector to view further details.



- By default, the chart shows the top five threat categories. Click the 'Other' link to view the next five categories.

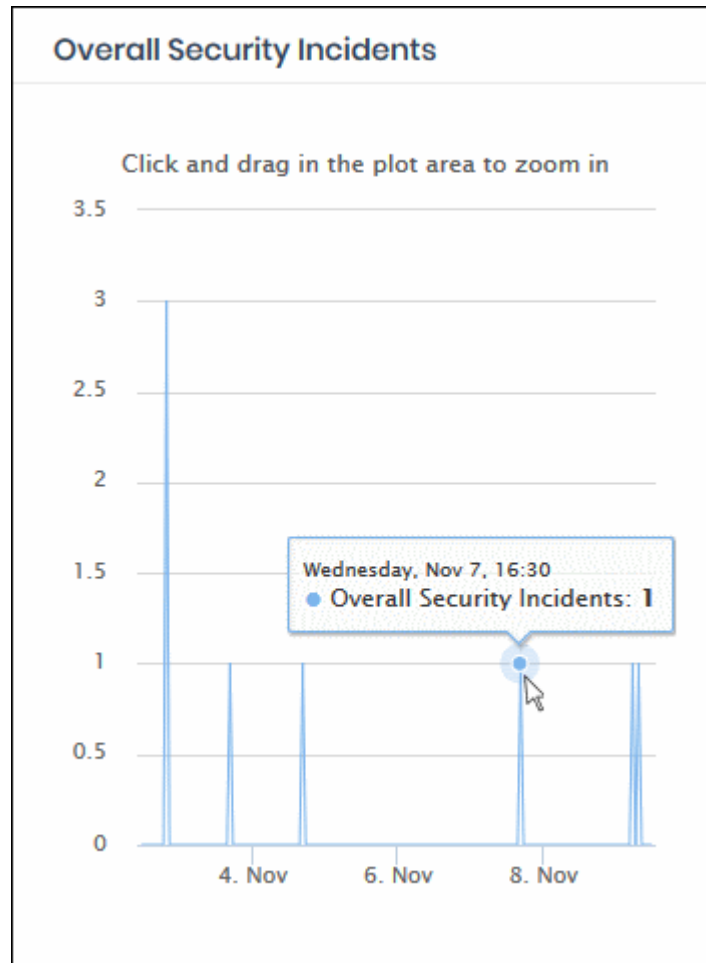


- Click 'Back' to return to the original view.
- Click a particular sector to view logs for that category. See **View Logs** for more details.

Overall Security Incidents

Shows the number of incidents in which harmful sites were blocked on your networks and roaming devices.

- Results are available from the last 12 hours up to a maximum of 7 days.
- Place your mouse cursor over a point in the chart to view further details.

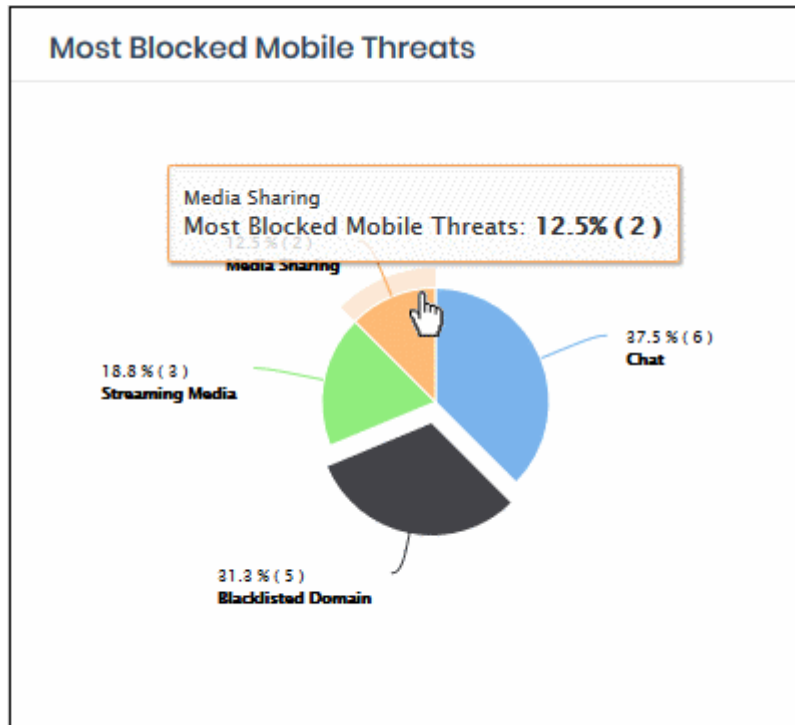


- Click and drag on the chart to zoom into a particular time period.
 - Click 'Reset Zoom' to return to the full chart.
- Click a particular point on the chart to view domain access requests. See '[View Logs](#)' for more details.

Most Blocked Mobile Threats

The web categories most often blocked to mobile users by your policies. These sites usually contain threats such as malware, phishing, spy-ware and drive-by-downloads.

- Place your mouse cursor over a sector to view further details.

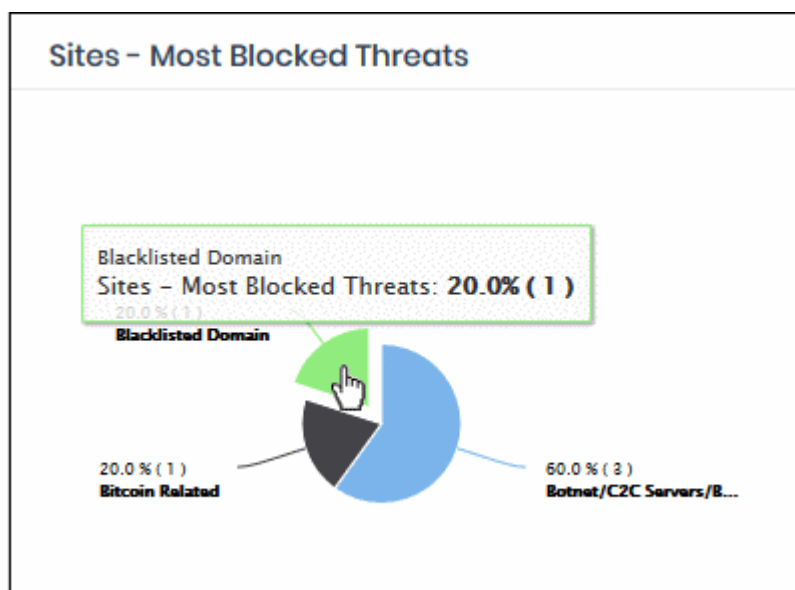


- Click on a sector to see a log of most blocked categories for mobile users. See '[View Logs](#)' for more on this.

Sites - Most Blocked Threats

The web categories most often blocked to users on imported network sites. Categories and blacklisted domains are specified in security rules in your policies. These websites usually contain threats such as malware, phishing, spyware and drive-by-downloads.

- Place your mouse cursor over a sector to view further details.



- Click on a sector to see a log of most blocked categories for mobile users. See '[View Logs](#)' for more on this.

3.3 View Logs

- You can view logs by clicking on a data item in a dashboard chart. For example, click a bar in a chart or a point on a line-graph.
- Each log shows more details about the item you clicked on. You can filter the logs by date and by various other filter types. Logs are fully searchable and can be exported to .csv.

View logs from a chart

- Click 'Overview'
- Select 'Web Overview' or 'Security Overview'
- Click on a point in the chart to view logs for that item:

Sites - Overall Web Browsing Trend

Click and drag in the plot area to zoom in

Thursday, Jun 21, 17:30
• Sites - Overall Web Browsing Trend: 24

21. Jun 22. Jun 23. Jun

View Logs - Sites - Overall Web Browsing Trend

Choose Time Interval

From: 2018-06-21 17:30 To: 2018-06-21 18:30

Filter Type: Network

#	Time	Network	Destination	Category	Action	Agent Name
1	2018-06-21 18:29:46	10.100.136.198	up.edu	Education & Reference	BLOCKED	LR_TEST
2	2018-06-21 18:29:46	10.100.136.200	up.edu	Education & Reference	BLOCKED	LR_TEST
3	2018-06-21 18:27:05	10.100.136.218	up.edu	Education & Reference	BLOCKED	LR_TEST
4	2018-06-21 18:27:05	10.100.136.216	up.edu	Education & Reference	BLOCKED	LR_TEST
5	2018-06-21 18:24:31	10.100.136.208	up.edu	Education & Reference	BLOCKED	LR_TEST
6	2018-06-21 18:24:31	10.100.136.208	up.edu	Education & Reference	BLOCKED	LR_TEST
7	2018-06-21 18:22:01	10.100.136.208	up.edu	Education & Reference	BLOCKED	LR_TEST
8	2018-06-21 18:22:01	10.100.136.208	up.edu	Education & Reference	BLOCKED	LR_TEST
9	2018-06-21 18:22:01	10.100.136.208	up.edu	Education & Reference	BLOCKED	LR_TEST
10	2018-06-21 18:22:01	10.100.136.208	up.edu	Education & Reference	BLOCKED	LR_TEST

24 Total Items, Page 1 of 3

First Previous 1 2 3 Next Last

Close Export as CSV

- The panel on the left lets you filter by time and other parameters.

- The right of the window shows all events in the category along with other details.
- The details on the right depend on the type of chart for which you are viewing logs. The following table show all possible columns:

View Logs - Table of Column Descriptions	
Column Header	Description
Network / Location	The IP address of the network from which the traffic originated. Charts for networks imported by the resolver also show the IP address of the endpoint.
Destination	The name of the website the user attempted to visit.
Category	The genre of website to which the site belongs. You can view website categories in the 'Settings' area of a category rule. Click 'Configure' > 'Policy Settings' > 'Category Rules' > 'Create Category Rule' > 'Settings'.
Action	Action taken by Secure Internet Gateway. Can be 'Allowed', 'Blocked' or 'Contain'
Reason	The reason for the action taken. For example, a website connection was 'Allowed' because the site is in an allowed category.
Agent Name	'Roaming Device' charts - This column shows the name of the roaming device 'Imported site' charts - This column shows the name of the virtual appliance through which the network connects to Secure Internet Gateway.
Domain / Target Domain	The name of the domain that was visited / blocked
Source	The mobile device VPN ID.
Source IP	The IP of the agent / network

Select Time Interval



Logs initially show data for the time period you clicked on the graph. You can change the date and time from the 'Choose Time Interval' section:

- To change the period, click the calendar icon and select the 'From' and 'To' dates or enter the period directly in the fields.
- To change the time, enter the 'From' and 'To' time in the respective fields beside the date.


Filter Types

Filter types allow you to refine the events shown as required. You can filter by multiple parameters.

Choose Time Interval


From  **To** 




Filter Type



- Select a filter parameter from the drop-down. The options available depend on the type of chart
- Enter a relevant search term
- Click the check-mark to add the filter
- Repeat the process to add more filters if required
- Click 'Search':

Filter Type



Network	10.108.51.160	
Destination	18xn.com	
Category	Malware	

The following types of log are available:

Chart Type	Logs Displayed
<p>Web Overview</p> <ul style="list-style-type: none"> Top Target Domains Top Blocked Domains Top Blocked Domains From Networks Top Blocked Domains From Agents Top Target Domains of Mobile Users Sites - Top Target Domains <p>Security Overview</p> <ul style="list-style-type: none"> Roaming Agent Security Incidents Overall Security Incidents 	<ul style="list-style-type: none"> • Click on a bar to view the logs of access requests made for the that domain <p>The log viewer shows details of the time, network/endpoint from which the domain access request originated, the category of the domain, whether the access was allowed or denied and the reason for the action taken.</p>

<p>Web Overview Roaming Agent Web Browsing Trend Overall Security Trend Web Traffic of Mobile Users Sites - Overall Web Browsing Trend</p> <p>Security Overview Overall Advanced Threats Roaming Agent Advanced Threats Most Blocked Mobile Threats Sites - Most Blocked Threats</p>	<ul style="list-style-type: none"> Click on a point the graph to view the logs of web browsing activities in that period of time <p>The log viewer shows details of the visited domains, network/endpoint from which the domain access request originated, the category of the domains, whether the access request was allowed or denied, and the reason for the action taken.</p>
<p>Web Overview Top URL Categories Top Blocked Categories of Mobile Users Sites - Top Blocked Categories</p>	<ul style="list-style-type: none"> Click on a sector to view logs of access history of domains in that category <p>The log viewer shows details of the visited domains, network/endpoint from which the domain access request originated, the category of the domains, whether the access request was allowed or denied, and the reason for the action taken.</p>

4 Add Networks, Roaming Endpoints and Mobile Devices

- Click 'Configure' in the Secure Internet Gateway top-menu:

The screenshot shows the 'Configure' menu in the top navigation bar, which is circled in red. A red arrow points from this menu to the 'Networks' option in the left-hand sidebar, which is also highlighted with a red box. The main content area displays a table of configured networks.

#	Company	Name	Type	IP / FQDN
1	123bom	MyNetwork_2020-01-08	Static	192.22.2/28
2	123bom	MyNetwork_2020-01-08	Static	192.23.4/32
3	gozde	clifton	Static	107.20.98.84
4	gozde	Oregon -> Seattle2	Static	172.31.59.142
5	gozde	vpn-test	Static	66.111.62.218
6	gozde-ds	gözde_IP	Static	10.100.136.31
7	gozde-ds	gozdeIP_215	Static	10.100.136.31

- **Objects** - Manually add networks, roaming and mobile devices to Secure Internet Gateway.
 - Alternatively, you can automatically import networks by deploying local resolvers. Click 'Sites and Virtual Appliances' to get started with this method.
 - Note. The public IP of the network from which you are connecting is automatically added. This network becomes active immediately.
- **Policy Settings** - Configure and apply web protection policies to your networks/endpoints.

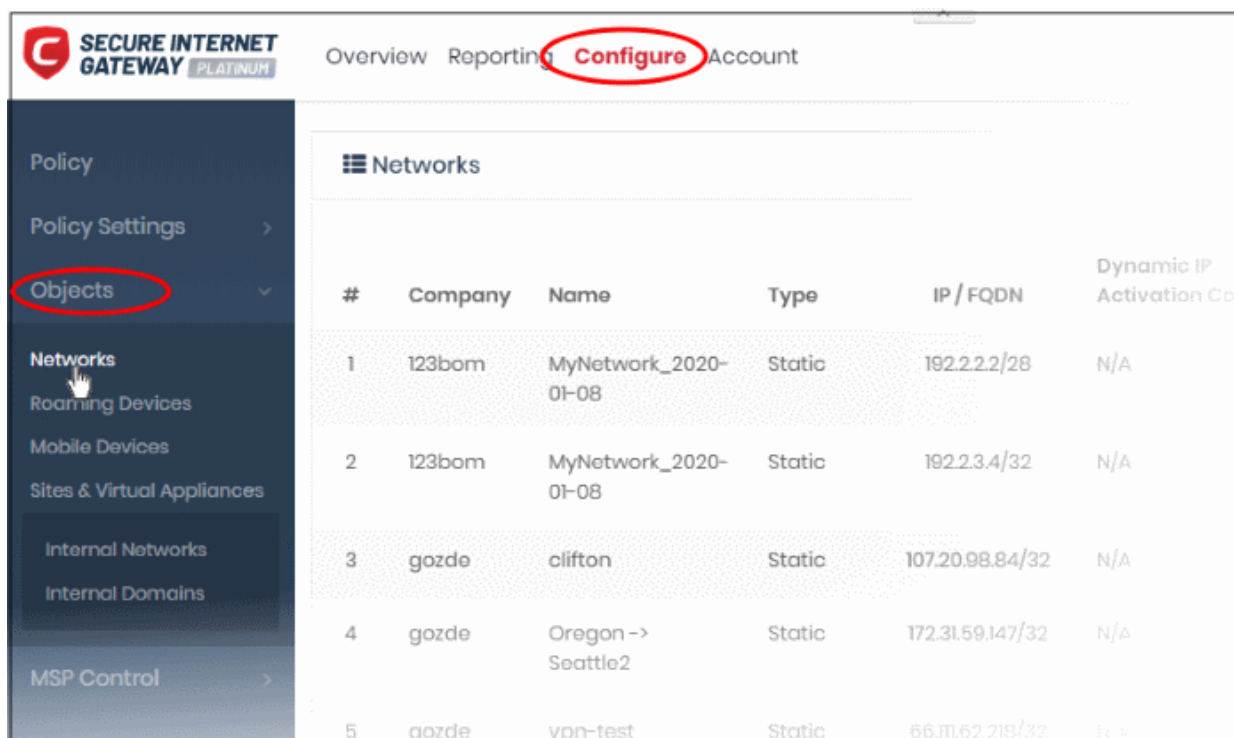
See **Setup Options Explained** for an overview of choices to add networks.

See the following sections for help to add networks:

- **Add Networks**
- **Add Roaming Endpoints**
- **Add Mobile Devices**
- **Manage Imported Sites and Local Resolver Virtual Appliances**

4.1 Add Networks

- Click 'Configure' > 'Objects' > 'Networks' to add, edit and manage protected networks.
- The IP of the network from which you are connecting was automatically added at enrollment. This network is already active.
- Any additional IPs you add will have a status of 'Pending' until they are approved by Comodo. Please contact your Comodo account manager or domesupport@comodo.com if you have questions on pending networks.
- You can add IP addresses in CIDR notation with network prefixes from /32 to /24. You can add any combination of CIDR ranges and/or individual IP addresses.
- Dynamic IP addresses. We provide an agent which auto-updates your Secure Internet Gateway policies with any address changes in your network. The agent should be installed on an endpoint in your target network. After you add a network which uses dynamic IPs, Secure Internet Gateway will create an activation code for the agent (click 'Configure' > 'Objects' > 'Networks' to view the code). Enter the code in the agent to enroll the network.
- Please also make sure endpoints in protected networks are configured to use CSIG DNS (Preferred DNS server - 8.26.56.10. Alternate DNS server - 8.20.247.10)



Networks - Table of Column Descriptions

Column Header	Description
Company	Applies to MSPs only. Name of the organization to which the network belongs.
Name	The label of the network.
Type	Indicates whether the network uses static or dynamic IP addresses.
IP / FQDN	The public IP address or Fully Qualified Domain Name (FQDN) of the network.
Dynamic IP Activation Code	(Only networks with dynamic IP addresses). The token string used to connect the network to Secure Internet Gateway. See Add Networks with Dynamic IP addresses for more details.
Agents Behavior	Shows whether the roaming agent is active or not when the device is inside the network.
Status	Can be 'Active' or 'Pending'. Active networks are available for CSIG protection. 'Pending' means the IP address/FQDN is awaiting approval by Comodo.
Remark	Description of the network.
Actions	Update or delete a network.

The interface allows you to:

- **Add new networks**
- **Edit network details**
- **Delete a network**

Add New Networks

You can add networks with static IP addresses and dynamic addresses.

- **Add Networks with Static IP Addresses** - Specify an IP address/range in CIDR notation, or a fully

qualified domain name. See [Add Networks with Static IP addresses](#) for more details

- **Add Networks with Dynamic IP Addresses** - Download the IP Updater agent from the network setup wizard and install it on a network endpoint. The software will keep Secure Internet Gateway and your policies updated with any address changes. An activation code is generated for each agent which is needed to connect the network to Secure Internet Gateway. See [Add Networks with Dynamic IP addresses](#) for more details.

Add Networks with Static IP Addresses

- Click 'Configure' > 'Objects' > 'Networks'
- Click 'Add New Network':

Add Network
✕

Name

If you create a Location with an IP address different than the one that you're currently connecting to Dome Shield, your network will be on "pending" state. Network needs to be approved after verification by Comodo Dome Shield support. If you want to do so please send a mail to domesupport@comodo.com

IPv4 Address / FQDN

is Dynamic ?

Trusted Network Behaviour

Disable Roaming Agent when on this network

Please select company

Remark

Additional Settings +

Add Networks - Form Parameters	
Field	Description
Name	Enter an appropriate label for the network
IP Address / FQDN	The network address or its fully qualified domain name. <ul style="list-style-type: none"> Enter the IP address of the network in CIDR (Classless Inter-Domain Routing) notation. Secure Internet Gateway can accept network prefixes from /24 to /32.

	<p>Note: By default, this field shows the IP of the network from which you are connecting to Secure Internet Gateway. This will automatically become active after enrollment. Any new IP address that you add here will remain in pending status until approved by Comodo.</p> <p>Dynamic - Select if you are enrolling a network with dynamic IP addresses. See Add Networks with Dynamic IP addresses for more details.</p>
Trusted Network Behavior	<p>Disable Roaming Agent when on this network - Select whether policies applied to roaming agents should be active when they connect to this network.</p> <ul style="list-style-type: none"> • Enabled = The agent is disabled on roaming devices when they are inside the network. The network policy will apply to the roaming device. • Disabled - The roaming device's policy will remain active.
Please select company	<p>MSPs only</p> <ul style="list-style-type: none"> • Select the customer organization for which you want to enroll the network.
Remark	Enter any notes about the network being added.
<p>Additional Settings - These settings apply only to roaming devices which have the CSIG agent installed.</p> <ul style="list-style-type: none"> • A roaming device cannot connect to internal hosts when inside the office network. This is because CSIG DNS is an external DNS which cannot resolve internal domains. Configure the 'Host File' fields to allow devices to reach internal domains when it has an agent installed. These settings are automatically deployed to your device's host file. • See 'Add Roaming Endpoints' for more details about how to install CSIG agents onto devices and connect to Secure Internet Gateway. 	
Host File Configuration	Enter the name and IP address of your host in the respective fields. Click the '+' button to add more host entries. To remove an entry, click the corresponding trash can icon.

- Click 'Add' when done.

The network is added and shown in the list.

The next step is to configure your network's DNS to forward queries to CSIG DNS. This will ensure all the endpoints in the networks are protected. Alternatively, you can set CSIG DNS on the required endpoints (there are various ways to do this, including DHCP setting, Windows GPO and AD configuration). See <https://www.comodo.com/secure-dns/switch/computer.html> for more details.

- Change your DNS addresses to following Secure Internet Gateway addresses:
 - Preferred DNS server - 8.26.56.10
 - Alternate DNS server - 8.20.247.10

Note - no rules are applied to the new networks by default. You have to apply a policy to the network according to your requirements. See '**Apply Policies to Networks and Roaming / Mobile Devices**'.

Note: Any external IPs you add which are different to the one detected by Comodo Secure Internet Gateway will need to be approved by Comodo. To activate these networks, please contact our support at domesupport@comodo.com

Important Note:

- Admins also need to manually internal domains to the host files of endpoints inside the network. This is because CSIG DNS cannot resolve internal domains.
- For roaming endpoints with the CSIG agent, internal domains can be configured in 'Add/Update Network' > '**Additional Settings**' > 'Host File Configuration' field

- Please contact our support at domesupport@comodo.com if you face any problem regarding this.

Add Networks with Dynamic IP Addresses

- **Step 1 - Install the IP Update agent on an endpoint in the network**
- **Step 2 - Activate the agent**

Step 1 - Install the IP Update agent on an endpoint in the network

- Click 'Configure' > 'Objects' > 'Networks'
- Click 'Add New Network':

Add Network ✕

Name

If you create a Location with an IP address different than the one that you're currently connecting to Secure Internet Gateway, your network will be on "pending" state. Network needs to be approved after verification by Comodo Secure Internet Gateway support. If you want to do so please send a mail to domesupport@comodo.com

IPv4 Address / FQDN

 is Dynamic ?

Trusted Network Behaviour

Disable Roaming Agent when on this network

Secure Internet Gateway Dynamic IP Updater helps networks with Dynamic IP addresses to update Secure Internet Gateway Service with the current IP address of the network.

This provides continuous security to networks with Dynamic IP addresses. System will continuously update the latest IP of the network you want to secure and users will have uninterrupted security/web access policies applied.

Guidelines:

- Download and install the Dynamic IP Updater Agent to a stationary computer within the network.
- This computer should always be on and should not be moved out of the network you want to secure.
- After finishing installation, Activation Code shown in Networks table should be entered in to Dynamic IP Updater Agent's Activation tab. Once this step is done, Status should be shown as Active in the Networks table.
- Current IP address of the network can be seen in Networks table.

Download

[Windows Dynamic IP Updater](#)

Please select company

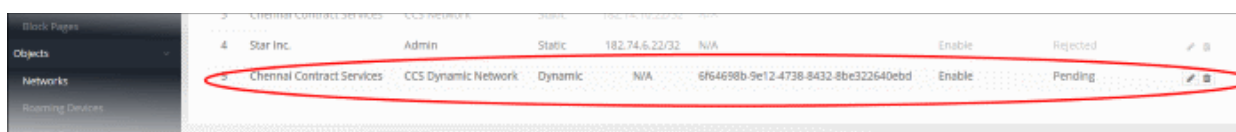
Remark

Additional Settings +

Add Networks - Form Parameters	
Field	Description
Name	Enter an appropriate label for the network
IP Address / FQDN / Dynamic	Select the 'Dynamic' checkbox to enroll a network with dynamic IP addresses. A message box will appear with help to enroll the network. <ul style="list-style-type: none"> Click the 'Windows Dynamic IP Updater' link in the message box and save the agent setup file.
Trusted Network Behavior	Disable Roaming Agent when on this network - Select whether policies applied to roaming agents should be active when they connect to this network. <ul style="list-style-type: none"> Enabled - The agent is disabled on roaming devices when they are inside the network. The network policy will apply to the roaming device. Disabled - The roaming device's policy will remain active.
Please select company	MSPs only <ul style="list-style-type: none"> Select the customer organization for which you want to enroll the network.
Remark	Enter a description for the network.
Additional Settings - These settings apply only to roaming devices which have the CSIG agent installed. <ul style="list-style-type: none"> A roaming device cannot connect to internal hosts when inside the office network. This is because CSIG DNS is an external DNS which cannot resolve internal domains. Configure the 'Host File' fields to allow devices to reach internal domains when it has an agent installed. These settings will be automatically deployed to your device's host file. See 'Add Roaming Endpoints' for more help. 	
Host File Configuration	Enter the name and IP address of your host in the respective fields. Click the '+' button to add more host entries. To remove an entry, click the corresponding trash can icon.

- Click 'Add' in the 'Add Network' dialog.

The network is added with the status 'Pending'. Also, an 'Activation code' is generated and displayed in the row of the network.



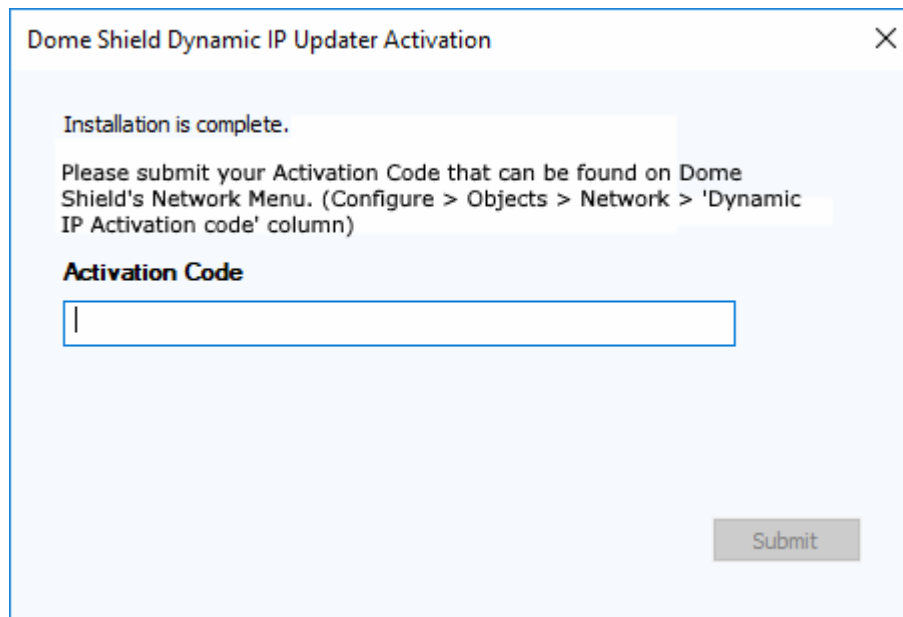
- Transfer the agent setup files to an endpoint in the target network

Note: Choose an endpoint which is always powered up and always connected to the network. This will let the agent monitor IP address changes and send updates to Secure Internet Gateway.



- Double-click on the setup file on the endpoint, or right click and select 'Install' from the context sensitive menu.

Step 2 - Activate the agent

After installing the agent, the activation dialog is displayed:



- Click 'Configure' > 'Objects' > 'Networks' in the Secure Internet Gateway interface to view the activation code:

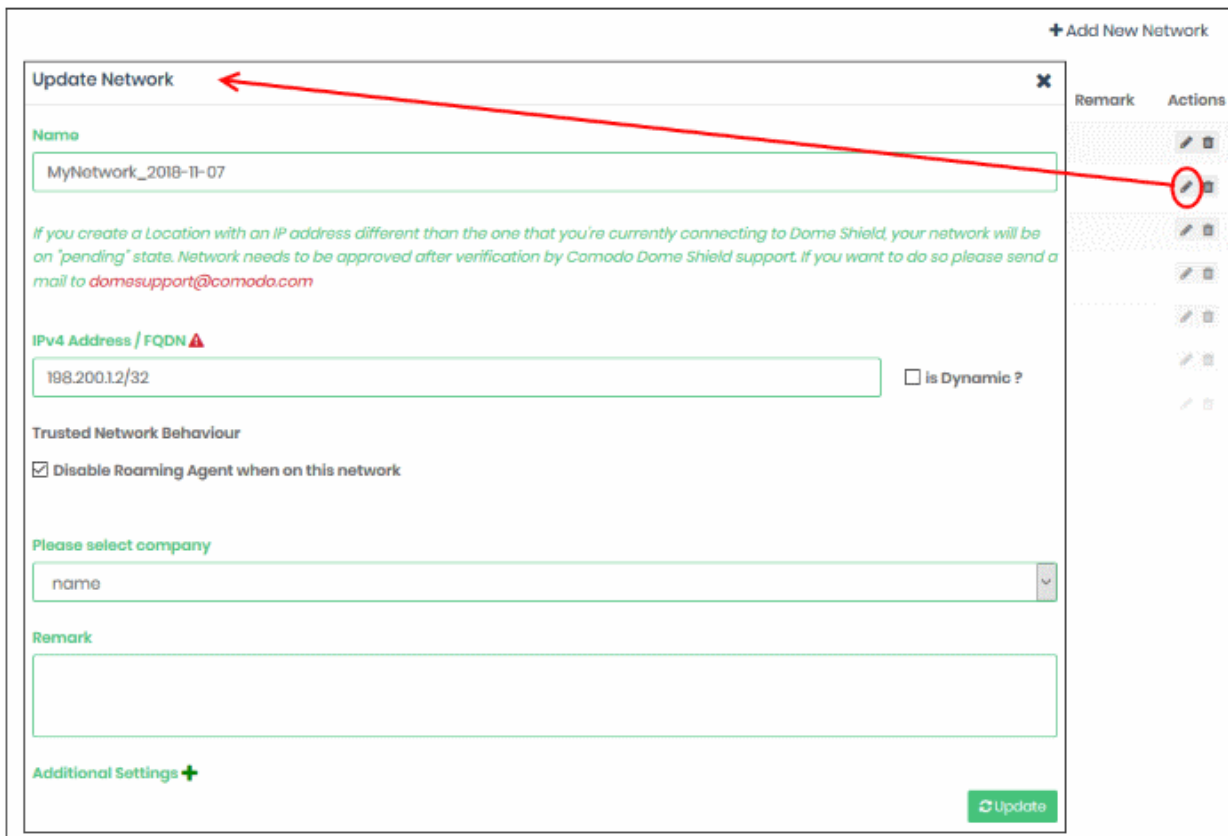
Networks										+ Add New Network
#	Company	Name	Type	IP / FQDN	Dynamic IP Activation Code	Agents Behavior	Status	Remark	Actions	
1	name	MyNetwork_2018-11-06	Static	172.12.3/32	N/A	Disable	Active		 	
2	name	MyNetwork_2018-11-07	Static	196.200.12/32	N/A	Disable	Active		 	
3	vtiger	gozdo	Static	10.100.136.208/32	N/A	Disable	Active		 	
4	vtiger	demo_ip	Dynamic	35.179.0.29/32	5c753ad0-8229-4ddb-b848-fa5c0be433a7	Enable	Active		 	
5	vtiger	MyNetwork_2018-11-02	Static	10.15.47.85/32	N/A	Disable	Active		 	
6	vtiger	London -> Manchester2	Static	172.31.21.234/32	N/A	Enable	Active		 	

- Enter code in the IP updater activation dialog.
- Click 'Submit'

After successful activation, the network is added and displayed in the list. Please note no rules are applied to the newly enrolled networks by default. You can apply network specific policy according to your requirements. See '[Apply Policies to Networks and Roaming / Mobile Devices](#)' for advice on how to deploy web protection rules to networks.

Edit the details of a network

- To update details of a network, click the edit button beside the network.



The 'Update Network' dialog will be displayed. Modify the details per your requirements. The process is similar to adding a new network **explained** above.

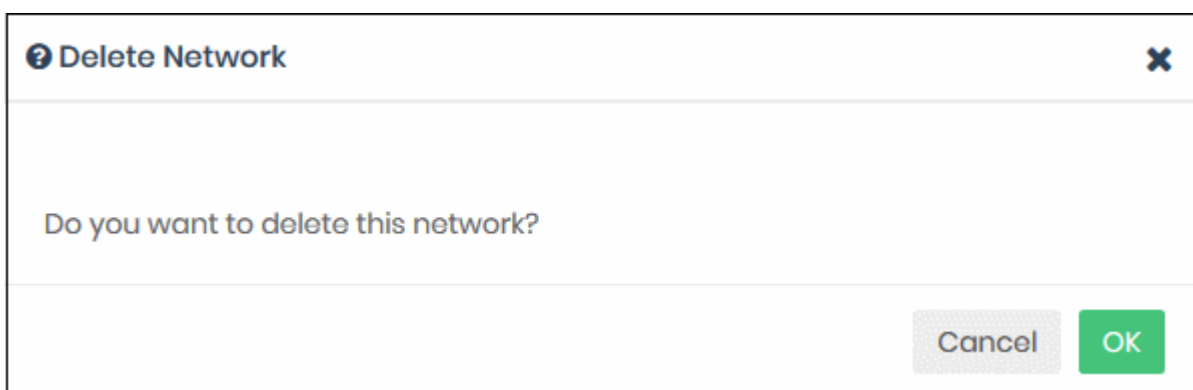
- Click the 'Update' button

Delete a network

Please note that when you delete a network, web protection policies will no longer be applied to network endpoints.

- Click the trash can icon beside a network to delete it.

A confirmation dialog is displayed.



- Click 'OK' to confirm removal of the network from the list.

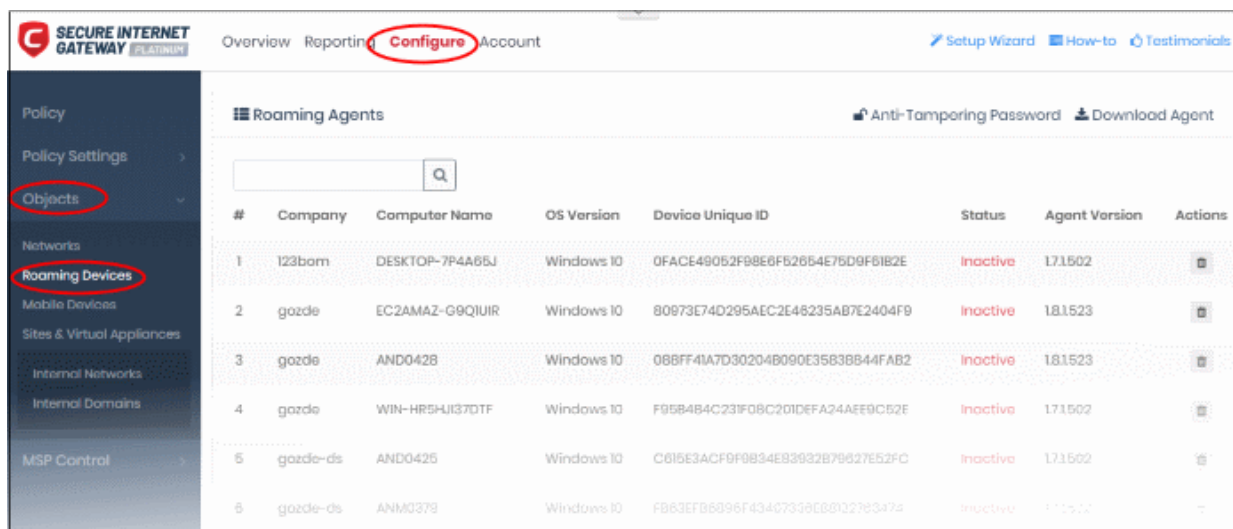
4.2 Add Roaming Endpoints

- You can protect Windows and Mac devices outside your network by installing the CSIG agent on each roaming device.
 - Click 'Configure' > 'Objects' > 'Roaming Devices' > 'Download Agent'

- You can manually install the agent on devices, or install it remotely through Endpoint Manager.
- Once installed, you can deploy policies to the devices as required.
- Roaming devices cannot connect to internal domains unless configured appropriately in the 'Network' interface.
- Set an anti-tampering password to prevent users uninstalling the agent from the device. Windows devices only.

See '**Additional Settings**' for help to configure internal DNS and host files.

- Click 'Configure' > 'Objects' > 'Roaming Devices' to view all enrolled roaming devices:



Roaming Agents - Table of Column Descriptions

Column Header	Description
Company	MSPs only. The name of the company to which the roaming device is enrolled.
Computer Name	The label of the endpoint.
OS Version	The version number of Windows or Mac operating system on the endpoint.
Device Unique ID	String generated by the agent to identify the device to Secure Internet Gateway.
Status	Shows whether the roaming device is connected to SIG or not. <ul style="list-style-type: none"> • Active - Roaming device is connected to SIG • Inactive - Roaming device is not connected to SIG. This may be because the device is powered off, there's no internet connection, or the SIG agent was removed.
Agent Version	Version number of the CSIG roaming agent deployed on the endpoint
Actions	Control for removing endpoints

The interface allows you to:

- **Add new roaming devices**
- **Configure an anti-tampering password**
- **Delete a device**

Add new roaming devices

- Click 'Configure' > 'Objects' > 'Roaming Devices' > 'Download Agent'

There are two ways you can add roaming devices:

- **Manually install the agent on endpoints** - Click 'Configure' > 'Objects' > 'Roaming Devices' > 'Download Agent'. Manually Install the agent on target devices. The devices will be automatically enrolled.
- **Import from Endpoint Manager** - You can remotely install the agent on managed Windows endpoints from the Endpoint Manager console.

Click 'Download Agent' to get the installation package.

Add new devices

- Click 'Configure' > 'Objects' > 'Roaming Devices'
- Click 'Download Agent' at the top-right:

The screenshot shows the 'Configure' section of the admin console. In the 'Roaming Agents' section, the 'Download Agent' button is circled in red. A red arrow points from this button to a 'Download Agent' dialog box. The dialog box contains the following information:

- Starting with v1.6.0**, you will be able to install Windows Agent without needing to uninstall the previous version. This will be available for v1.6.0 or higher, therefore, please uninstall your current agent for the last time and replace it with v1.6.0.
- Roaming Agent requires no additional configuration steps to activate. After download is complete, please install the Roaming Agent without changing the name of the package and it will start working immediately.
- Select Company**: A dropdown menu showing 'ACME Ammunitions'.
- Buttons for **Download for Windows** and **Download for macOS**.
- A link: [> Get Endpoint Manager Windows Link](#)

Choose your download options in the 'Download Agent' dialog:

- **Select Company** - MSPs only. Select the customer organization for which you want to enroll devices.
- **Download for Windows** - The agent installation package for Windows devices. See [Enroll Windows devices](#) for more details.
- **Download for mac OS** - The agent installation package for Mac OS devices. See [Enroll Mac OS devices](#) for more details.
- **Get Endpoint Manager Agent Windows Link** - Reveals the link you need to remotely install the agent on Windows endpoints through Endpoint Manager. See [Import Windows Devices from Endpoint Manager](#)

for more details.

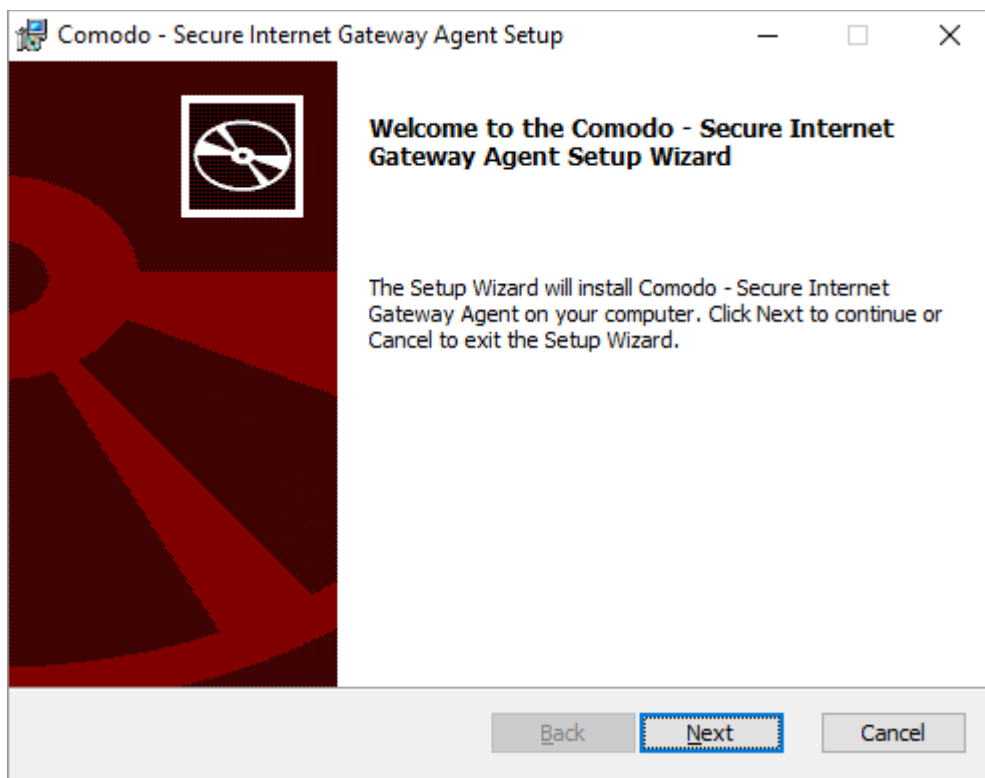
Enroll Windows devices

- Click 'Configure' > 'Objects' > 'Roaming Devices'
- Click 'Download Agent' at the top-right
- Click 'Download for Windows' in the 'Download Agent' dialog. The installation file is in .msi format.
- Transfer the setup files to the Windows devices you want to enroll.

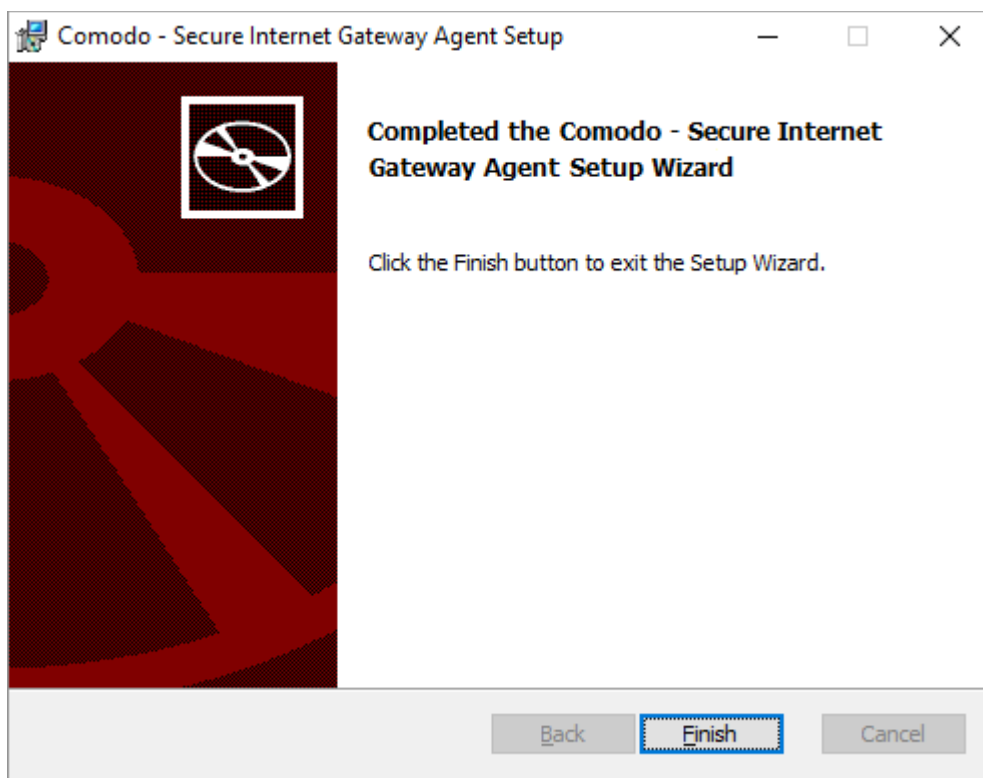
Next, install the agent on the device(s).

- Double-click the setup file  or right-click and select 'Install' from the context sensitive menu.

The installation wizard starts.



- Click 'Next' and complete the agent installation wizard.



- Click 'Finish'

That's it. The device is added and listed in the 'Configure' > 'Objects' > 'Roaming Devices' interface.

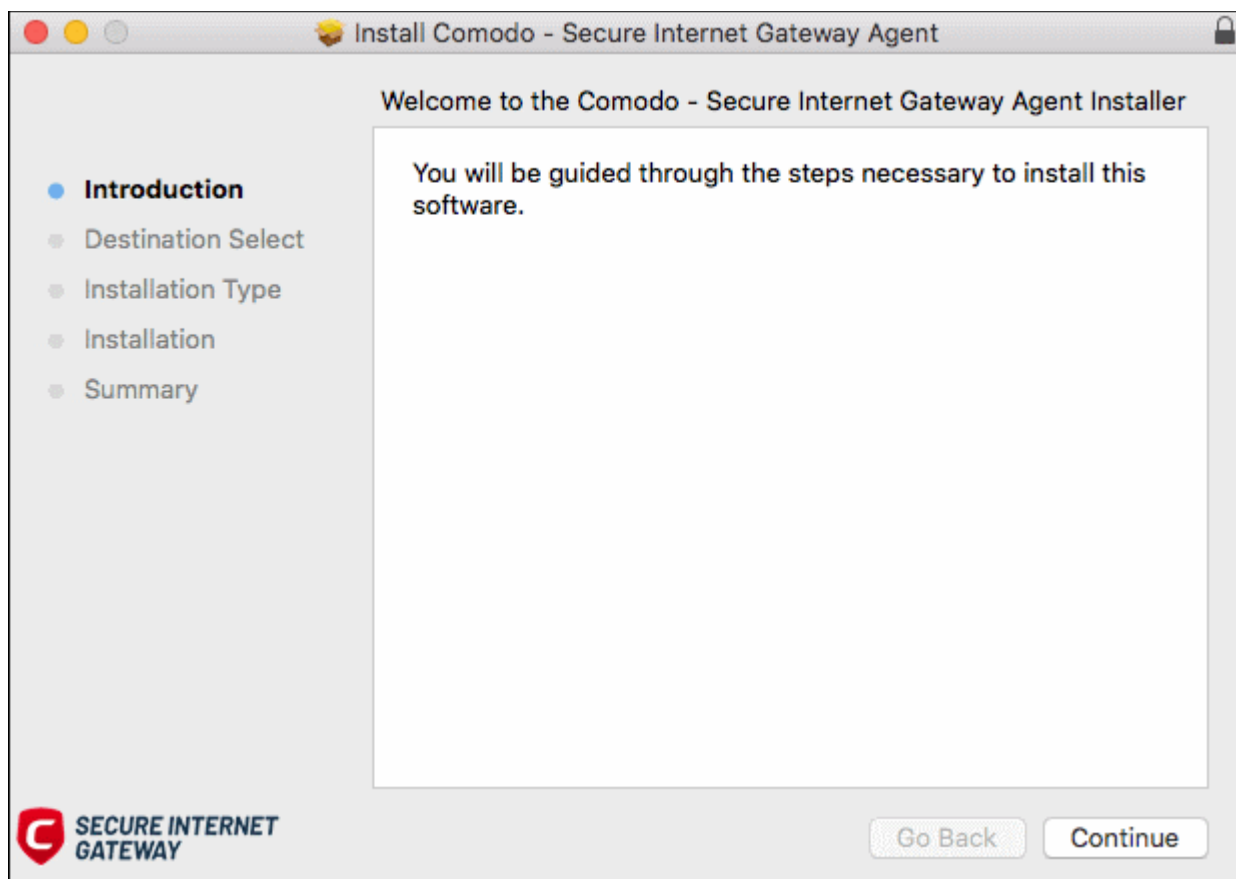
- Note - no security rules are applied to roaming device by default. You can create and apply device specific policies according to your requirements.
- See '[Apply Policies to Networks and Roaming / Mobile Devices](#)' for advice on how to configure and deploy security policies to roaming devices.

Enroll Mac OS devices

- Click 'Configure' > 'Objects' > 'Roaming Devices'
- Click 'Download Agent' at the top-right
- Click the 'Download for Mac OS' button in the 'Download Agent' dialog. The installation file is in .pkg format.
- Transfer the agent to the Mac OS devices that you want to enroll.

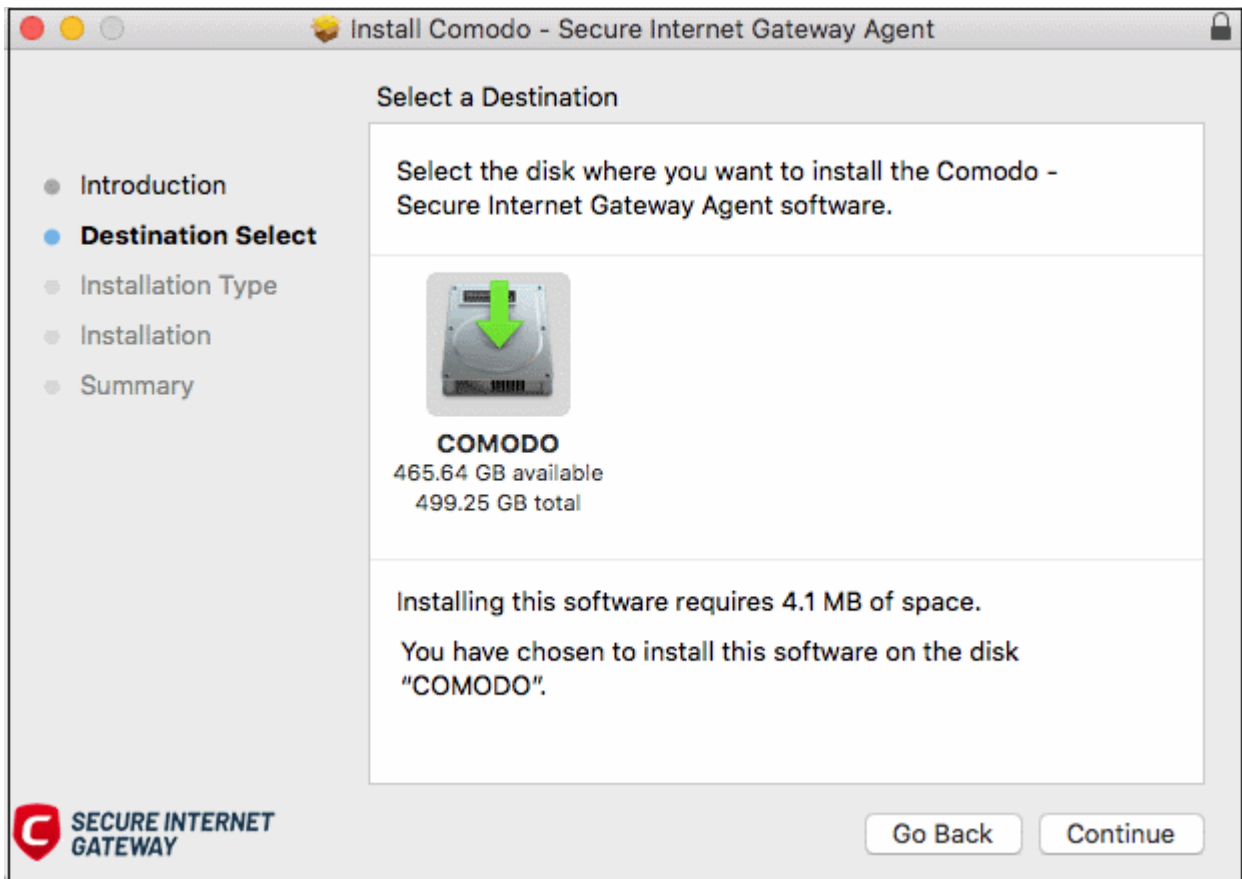
Next, install the agent on the device(s).

- Double-click the package file to start the installation wizard.



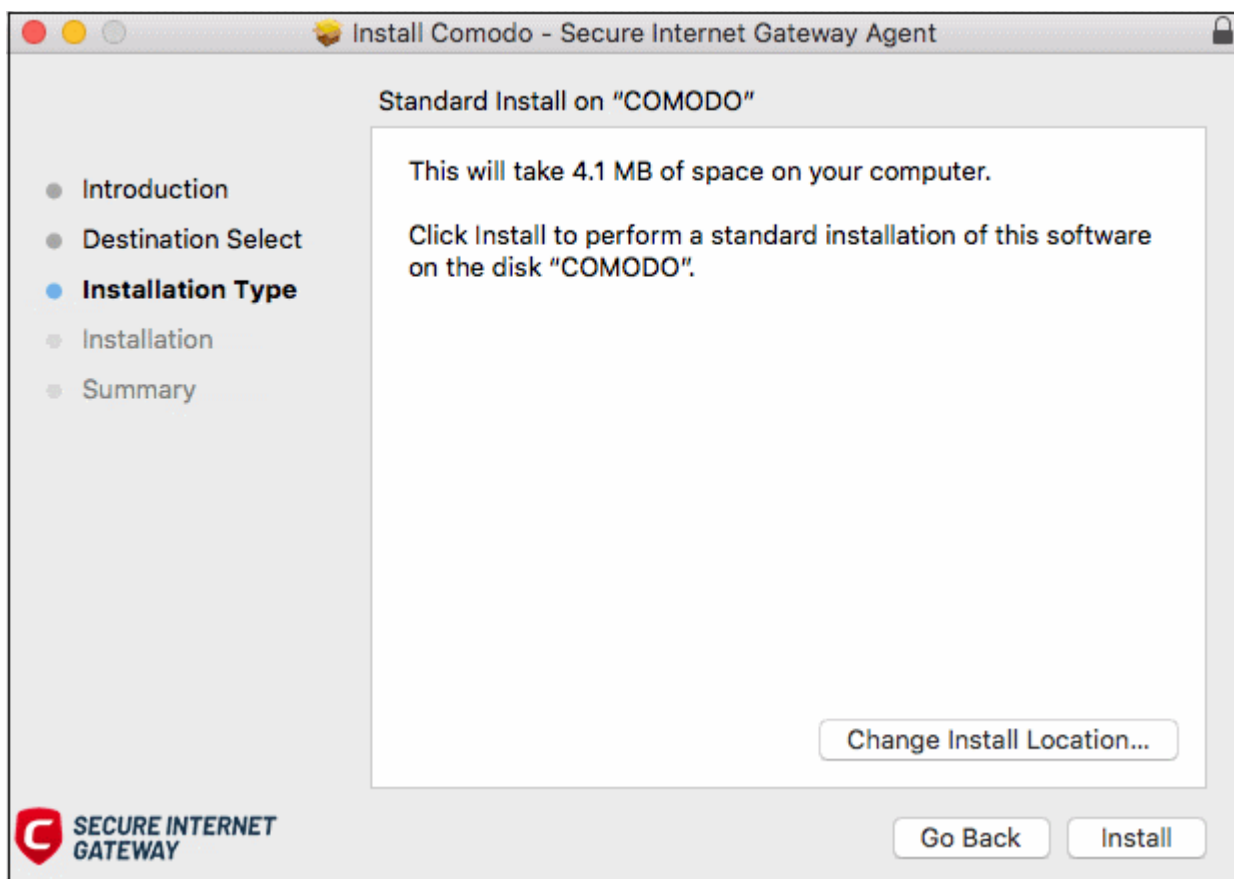
- Click 'Continue'

Choose the agent installation location in the next step:



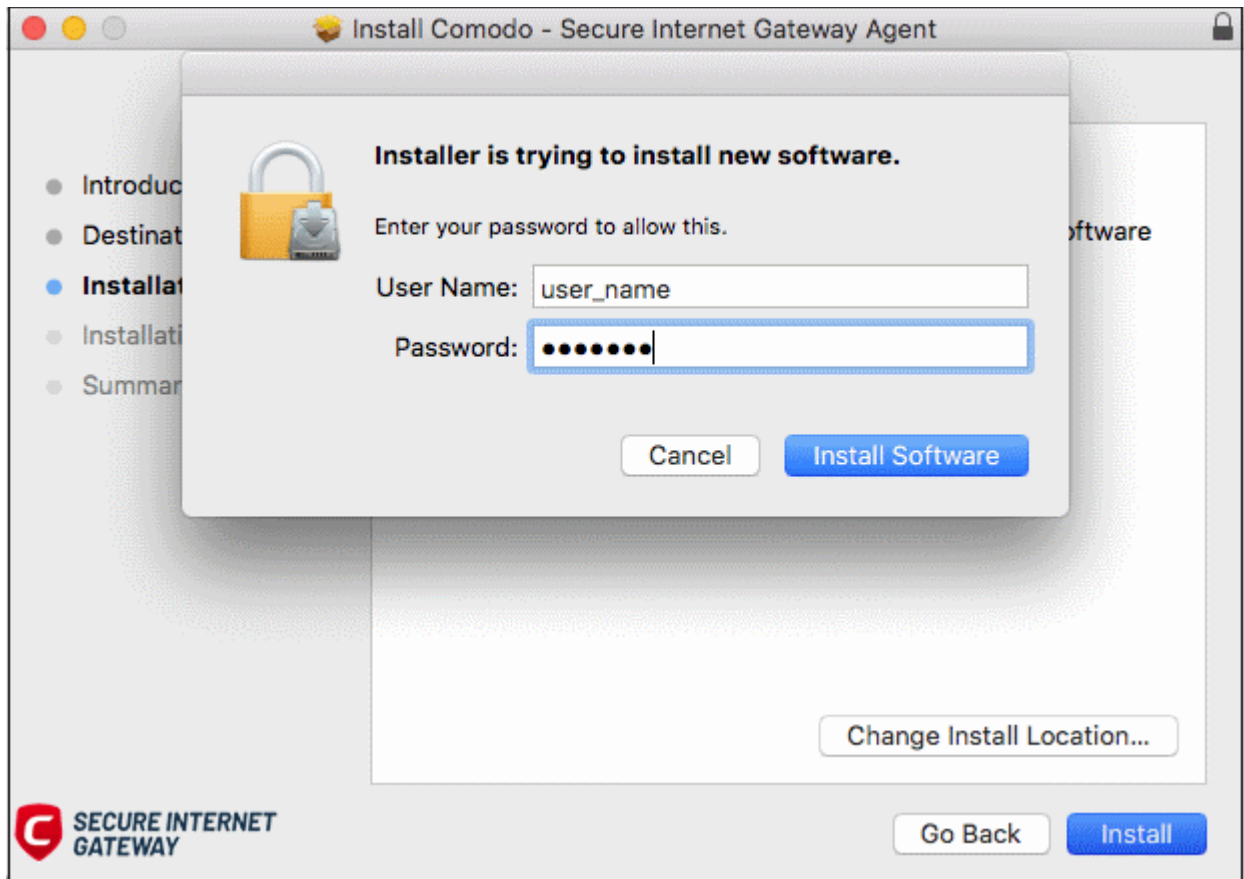
- To install the agent in the default location, click 'Continue'. To install the agent in a different location, click the disk icon, navigate to the new location and click 'Continue'.

The next step lets you to choose the installation type and start the installation.

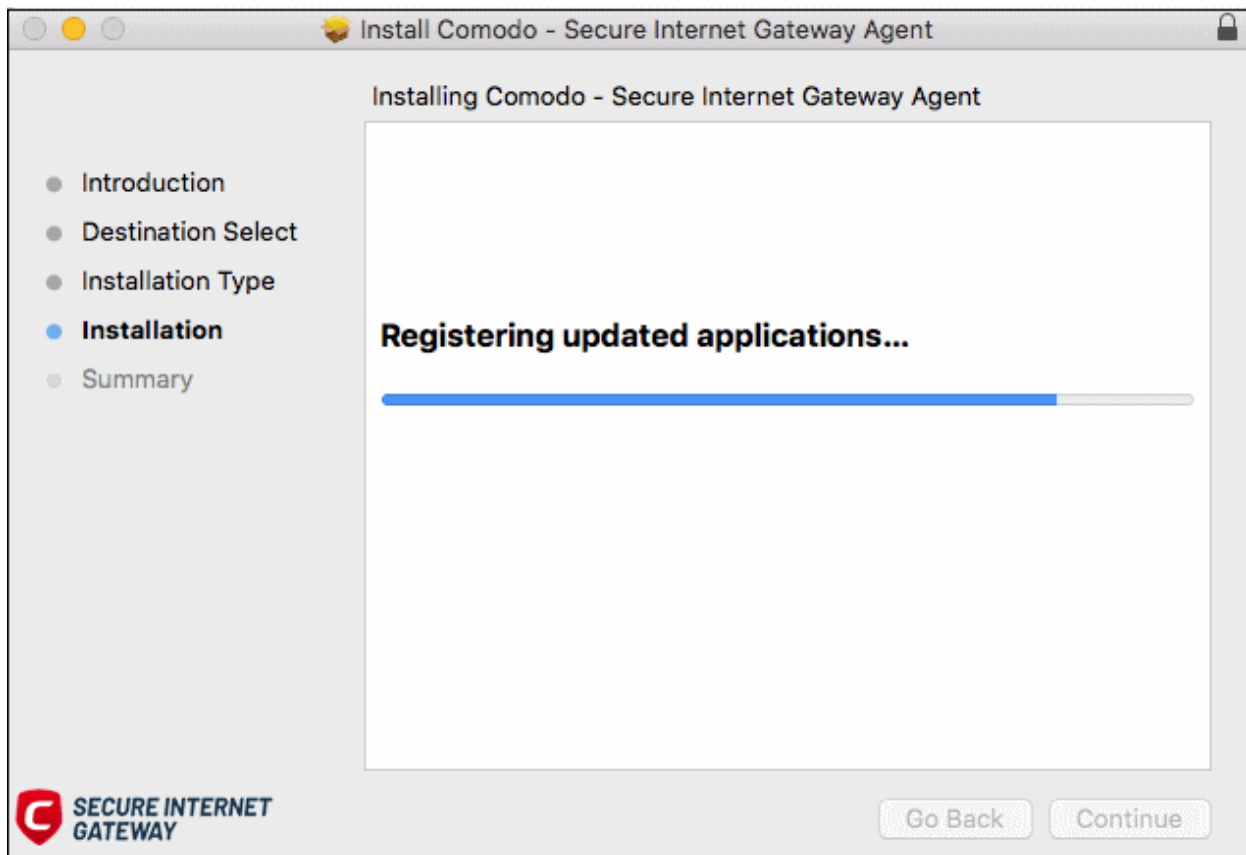


- Click 'Install'

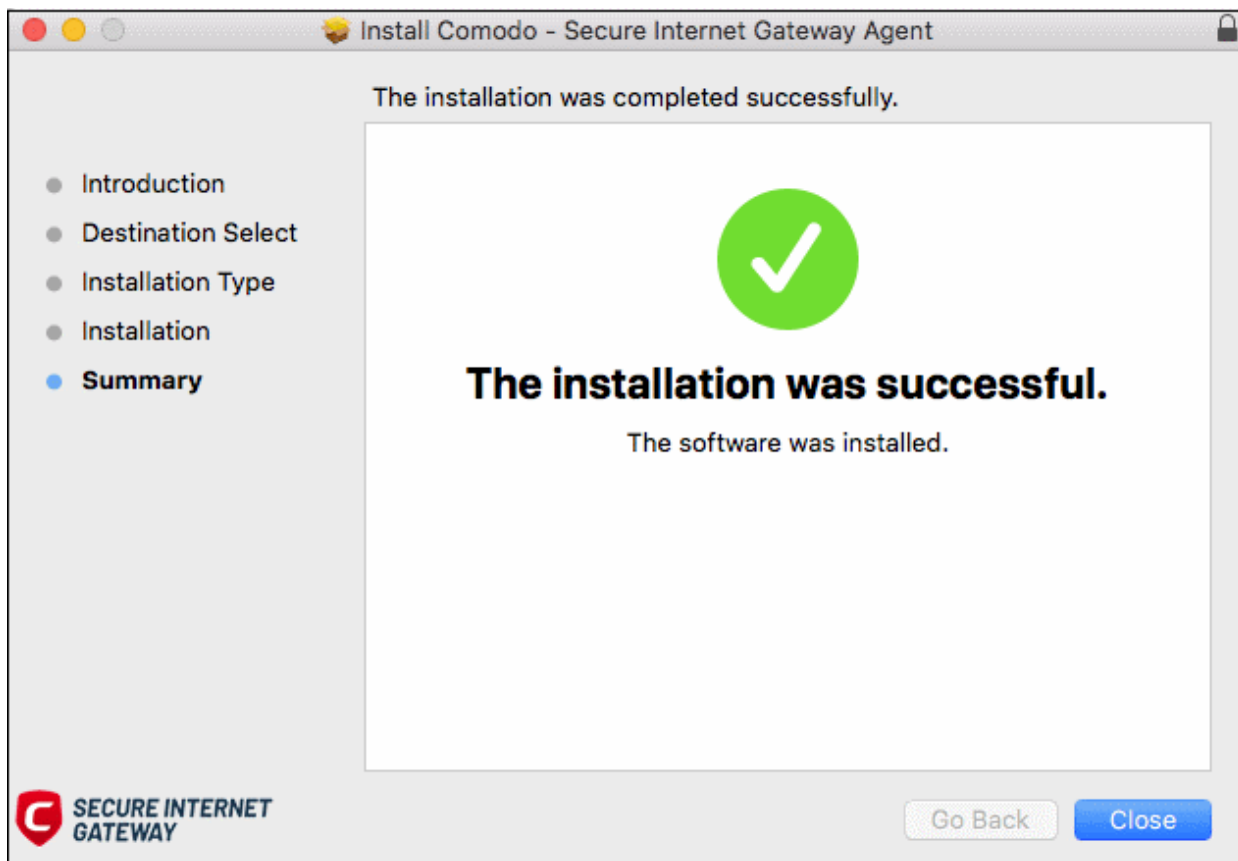
The installation requires your user account to continue.



- Enter your device user name and password in the respective fields and click 'Install Software'
- The installation starts:



- Click 'Close' to exit the wizard when installation is finished:



Once installed, the agent starts communicating with the Secure Internet Gateway server. The device is visible in 'Configure' > 'Objects' > 'Roaming Devices'.

- Note - no security rules are applied to roaming device by default. You can create and apply device specific policies according to your requirements.
- See '[Apply Policies to Networks and Roaming / Mobile Devices](#)' for advice on how to configure and deploy security policies to roaming devices.

Import Windows Devices from Endpoint Manager

- Click 'Configure' > 'Objects' > 'Roaming Devices'
- Click 'Download Agent' at the top-right
- Click 'Get Endpoint Manager Windows Link':

Download Agent ✕

Starting with **v1.6.0**, you will be able to install Windows Agent without needing to uninstall the previous version. This will be available for **v1.6.0** or higher, therefore, please uninstall your current agent for the last time and replace it with **v1.6.0**.

Roaming Agent requires no additional configuration steps to activate. After download is complete, please install the Roaming Agent without changing the name of the package and it will start working immediately.

Select Company

ACME Ammunitions

Download for Windows
Download for macOS

> [Get Endpoint Manager Windows Link](#)

Download for Windows
Download for macOS

> [Get Endpoint Manager Windows Link](#)

ITSM Agent Download link is <https://shield.dome.comodo.com/api/agent/download/B1d9onkZ7>

- Use this link as the 'Package URL' to install the agent on managed endpoints.

Process in brief:

- Login to Endpoint Manager
- Click 'Devices' > 'Device List' > 'Device Management' tab
- Select the Windows device(s) on which you want install the packages
- Click 'Install or Update Packages' and select 'Install Custom MSI/Packages'
- Paste the agent download link into the 'MSI/Package URL' field
- Configure the other remote installation options as required
- Click 'Install'
- See <https://help.comodo.com/topic-399-1-786-10139-Remotely-Install-and-Update-Packages-on-Windows-Devices.html> if you need additional help to install packages via Endpoint Manager.

Configure Anti-Tampering Password

- The anti-tampering password helps stop the agent from being uninstalled from a roaming device.
- Once set, the agent cannot be removed unless the password is provided.
- Password protection is only available for Windows devices.

Set an uninstallation password

- Click 'Configure' > 'Objects' > 'Roaming Devices'

- Click 'Anti-Tampering Password' on the top right

The screenshot shows the 'Configure' tab of the Admin Console. In the 'Roaming Agents' section, the 'Anti-Tampering Password' link is circled in red. A red arrow points from this link to a modal window titled 'Anti-Tampering Password'. The modal contains the following text:

Define an Anti-Tampering Password for your Agents to control its uninstallation from endpoints.

Note that this is valid for Agents with version 1.5.0 and later.
Agents are informed about password changes within 10 minutes.
Note: This is only for Windows Agents.

Select Company

postprodtest

Password

password

Save

- Select Company - MSPs only. Select the customer organization for which you want to set a password.
- Password - Create a unique key that is required to uninstall the agent.
- Click 'Save' for your settings to take effect
- Repeat the process to set password for other companies
- Password protection will take effect within ten minutes.

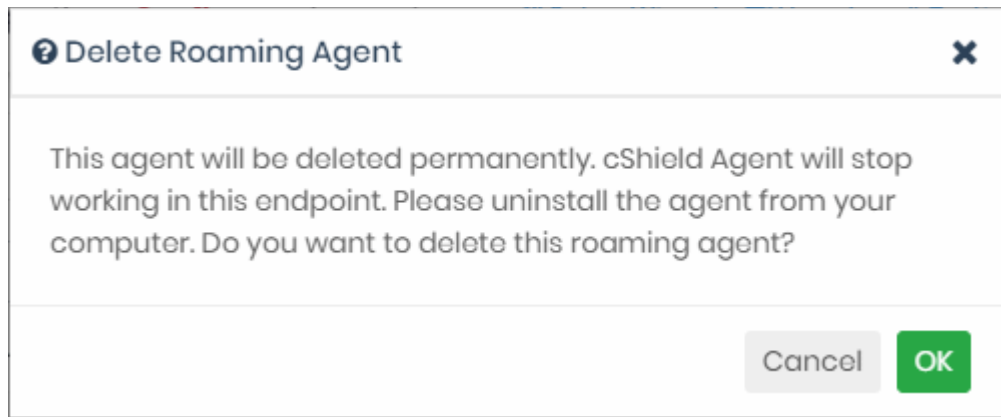
Note: The password protection applies only to the agents of version 1.5 and later.

Delete a Roaming Device

- Roaming devices that no longer need web protection can be removed from Secure Internet Gateway.
- Any security policies will also be removed from the deleted devices.
- You have to manually uninstall the agent from the device

Remove a roaming device

- Click 'Configure' > 'Objects' > 'Roaming Devices'
- Click the trash can icon beside a device to delete it.



- Click 'OK' to confirm device removal

4.3 Add Mobile Devices

Click 'Configure' > 'Objects' > 'Mobile Devices'

- You can protect iOS and Android devices by enrolling them to the VPN service.
- You need to install the CSIG mobile app or the VPN profile on each device you want to manage.
 - CSIG App - Includes a VPN client and a VPN profile.
 - VPN Profile - Contains only the profile. Android users need to install the StrongSwan VPN client.
- You should use different email addresses to download the app/profile to each device. The same email should not be used on different devices to download the app/profile.
- Supported versions: Android - 4.4 and above; iOS - 9 and above.
- Once installed, you can deploy policies to mobile devices as required.
- Click 'Configure' > 'Objects' > 'Mobile Devices' to view all enrolled mobile devices:

The screenshot shows the 'Configure' > 'Objects' > 'Mobile Devices' page in the Comodo Secure Internet Gateway Admin Console. The page title is 'Mobile Devices' with a '+ Add New Mobile Device' button. Below the title is a search bar. The main content is a table with the following columns: #, Company, Email, Remark, Mode, Status, Last Login/Logout Activity, and Actions. There are five rows of data.

#	Company	Email	Remark	Mode	Status	Last Login/Logout Activity	Actions
1	123bom	sedda1993@gmail.com		VPN + Mobile Agent	Not installed	N/A	[trash icon]
2	gazde	gzd.lkn@gmail.com		VPN + Mobile Agent	Installed, Not Active	2020-01-09 14:18:03 - Logout	[trash icon]
3	gazde	chandrasekaran@comodo.com		VPN + Mobile Agent	Not installed	N/A	[trash icon]
4	vtiger	bfdfgrghdflj@yopmail.com		VPN	Not installed	N/A	[trash icon]
5	vtiger	sdllghdtj@yopmail.com		VPN	Not installed	N/A	[trash icon]

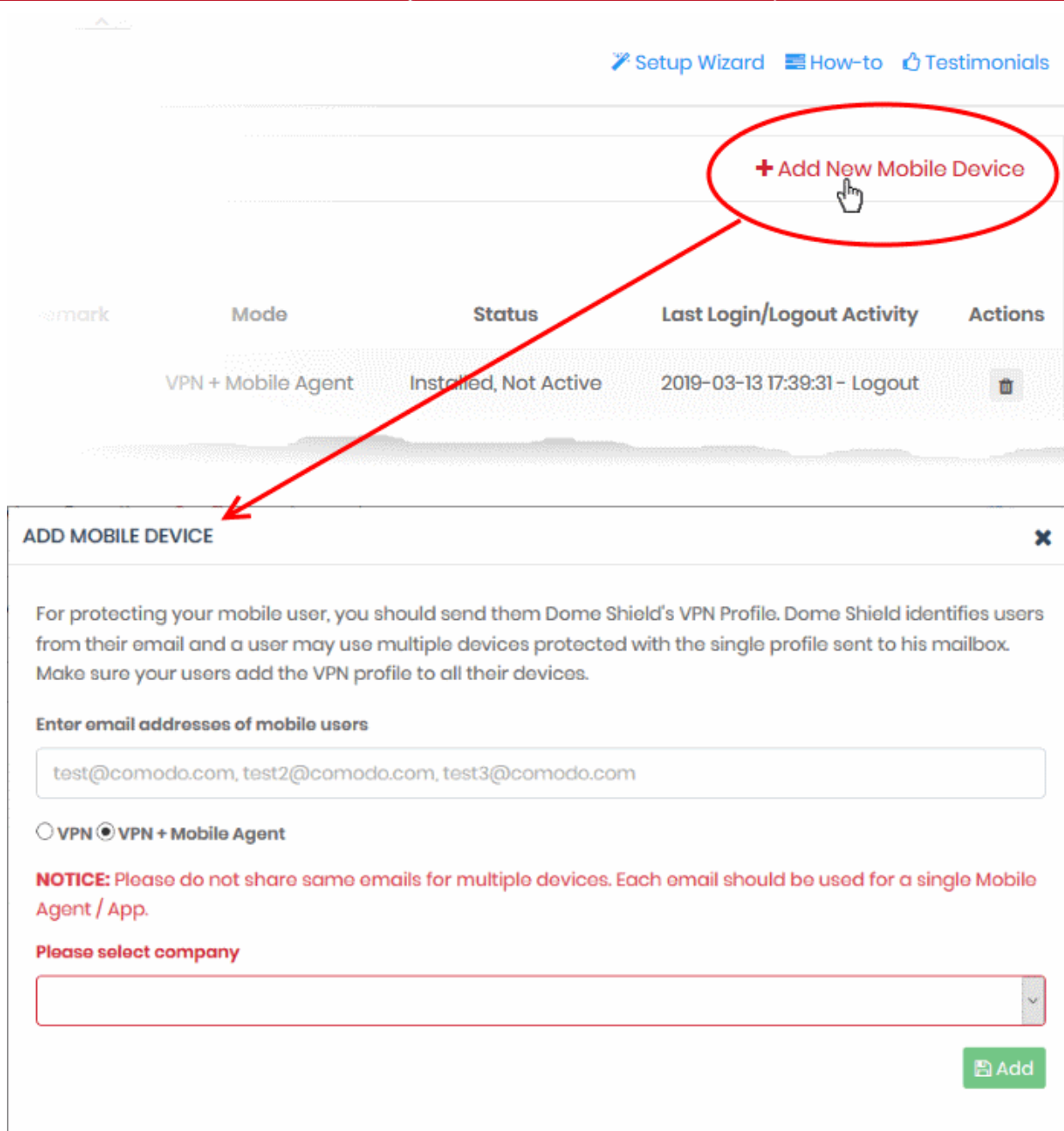
Mobile device interface - column headers

Company	MSPs'only. The customer organization to which the device is enrolled.
Email	The enrollment mail is sent to this address.
Remark	Comments about the account.

Mode	'VPN Profile' - The device has only the VPN profile installed. 'VPN + Mobile Agent' - The CSIG app is installed, which includes the VPN profile and the client.
Status	The connection state of the mobile device to Secure Internet Gateway. <ul style="list-style-type: none"> • Installed, Active - Protection is enabled, and the device is connected to Secure Internet Gateway. • Installed, Not Active - The profile is present on the device, but the device is not connected to Secure Internet Gateway. • Not installed - The enrollment mail was sent to the user, but the CSIG profile/app hasn't yet been installed.
Last Login/Logout Activity	Date and time of the device's most recent connection <ul style="list-style-type: none"> • Login - The last time the device connected to Secure Internet Gateway • Logout - The last time the device disconnected from Secure Internet Gateway
Actions	Control for removing mobile devices

Add a mobile device

- Click 'Configure' > 'Objects' > 'Mobile Devices'
- Click 'Add New Mobile Device':



- **Enter the email addresses of mobile users** - The contact addresses of the users whose devices you want to add. You can enter multiple email addresses. Please note - each device requires a unique email address. You cannot use the same email address on different devices.
- Select the type of installation you want:
 - **VPN + Mobile Agent** - This is the CSIG mobile app. If you select this, the user need not install any third party VPN client.
 - **Click here** to see instructions for this option.
 - OR
 - **VPN** - This is the profile only. If you select this, Android users must also install the StrongSwan VPN app. StrongSwan is not required for iOS devices.
 - **Click here** to see instructions for this option.
- **Please select company** - MSPs only. Choose the customer organization for which you want to enroll mobile devices

- Click 'Add'

VPN

- The user is initially added to the list with a device status of 'Not installed':
- CSIG will send device enrollment emails to all users that you added.

#	Company	Email	Remark	Mode	Status	Last Login/Logout Activity	Actions
1	vtiger	fiatliona@gmail.com		VPN	Not installed	N/A	
2	vtiger	gzd.ahn@gmail.com		VPN	Not installed	N/A	
3	vtiger	licencetype@zippix.com		VPN + Mobile Agent	Not installed	N/A	

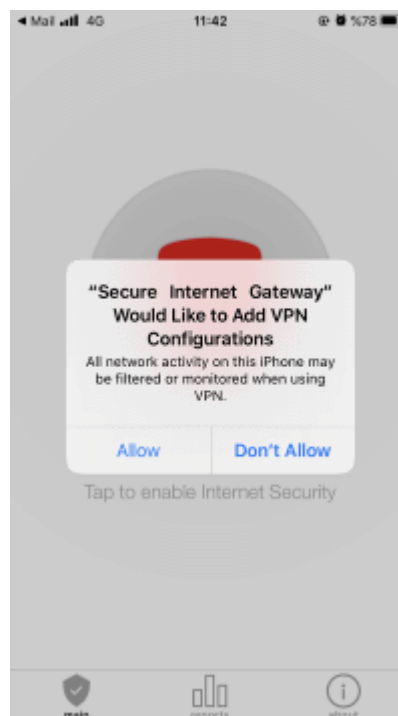
- Users should open the email on their device.
- The email contains instructions to enroll their device and three attachments:
 - iOS_VPN_Profile.mobileconfig - iOS device users should select this.
 - Android_VPN_Profile.sswan - Strongswan VPN profile for Android users
 - Android SSLCert.pem - This SSL certificate needs to be imported to Android devices to secure the VPN connection.

iOS instructions

Android instructions

Instructions for iOS

- Tap 'Activate iOS App' in the mail
- Hit 'Allow' to complete the activation:

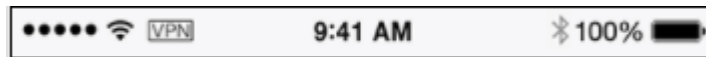


The VPN profile is now installed on the device.

- You also need to trust the SSL certificates in iOS in order to view HTTPS pages over the VPN.

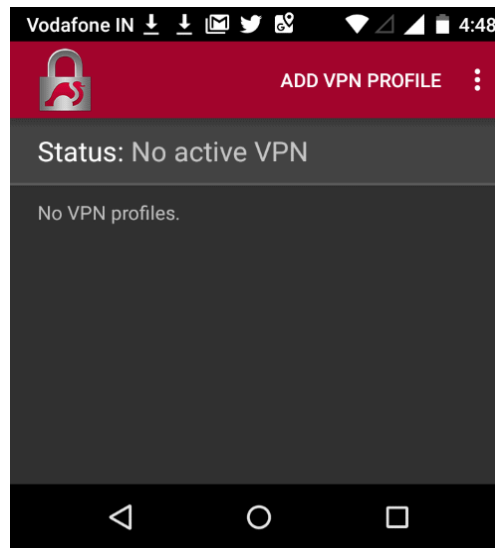
- Go to 'Settings' > 'General' > 'About' > 'Certificate Trust Settings' and enable full trust for root certificates.

Once connected, the VPN icon will appear in the navigation bar:

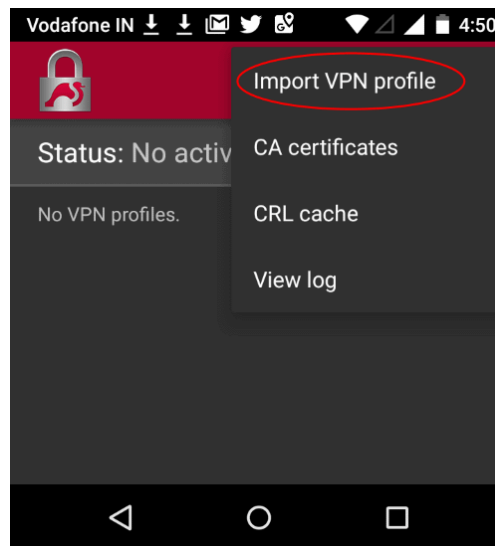


Instructions for Android

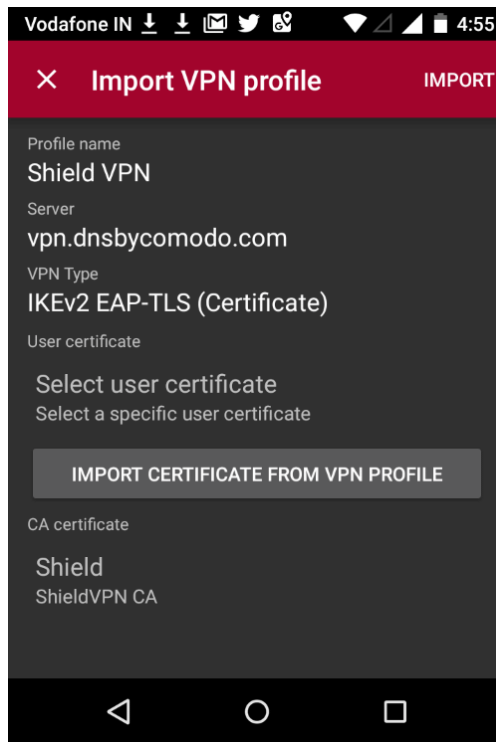
- Open the enrollment mail and select 'Android_VPN_Profile'
- Open the StrongSwan VPN app:



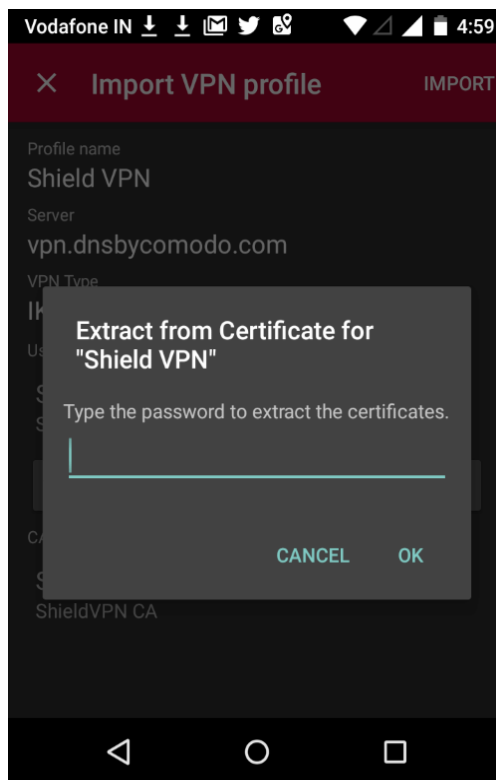
- Select 'Add VPN Profile' > 'Import VPN profile':



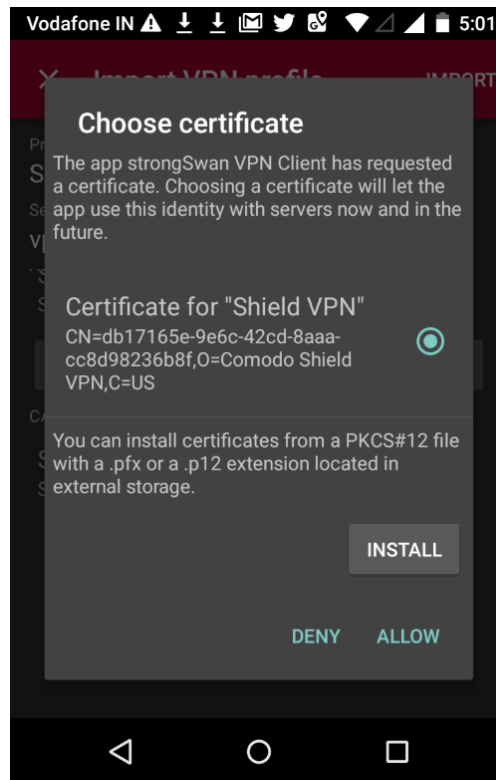
- Choose 'Android_VPN_Profile' from the downloaded location



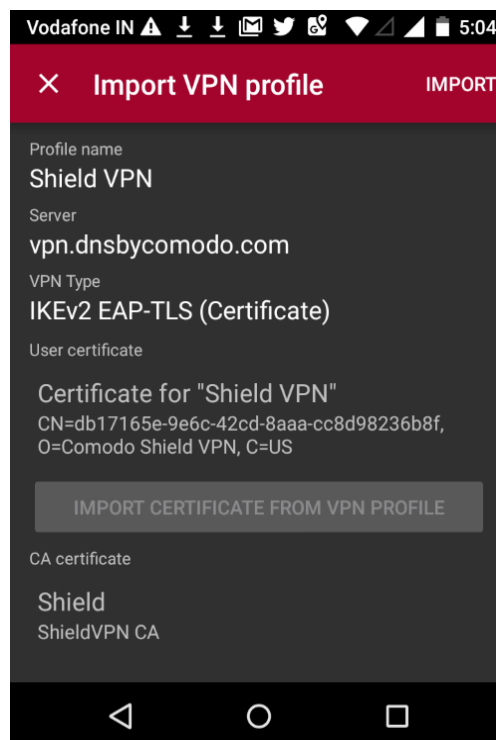
- Select 'Import Certificate from VPN Profile'



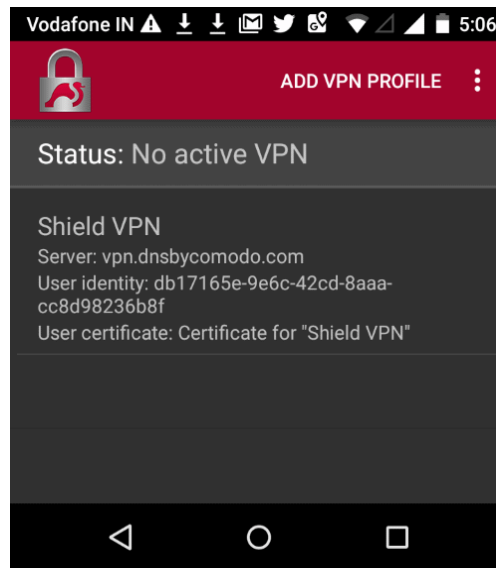
- Enter the password in the email and select 'OK'



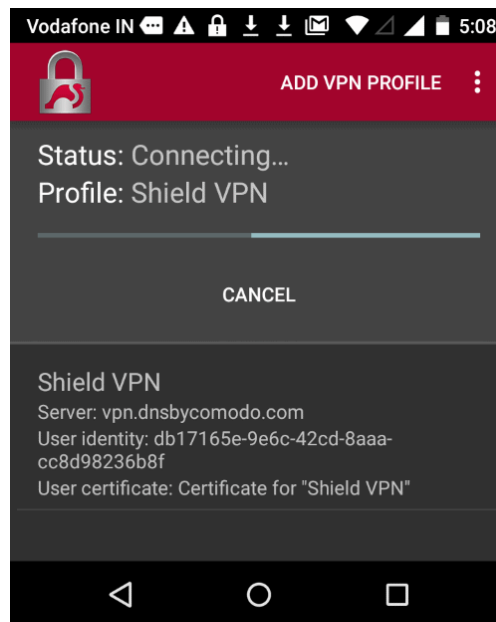
- Tap 'Allow' instead of 'Install'



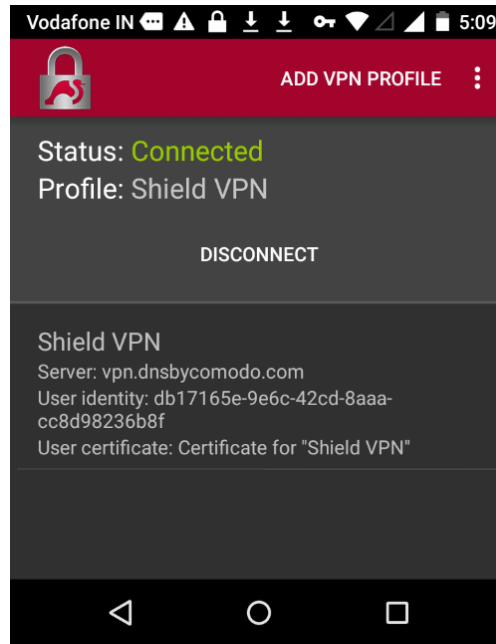
- Select 'Import' at the top-right



- Open the profile you just imported to start the connection to Secure Internet Gateway:

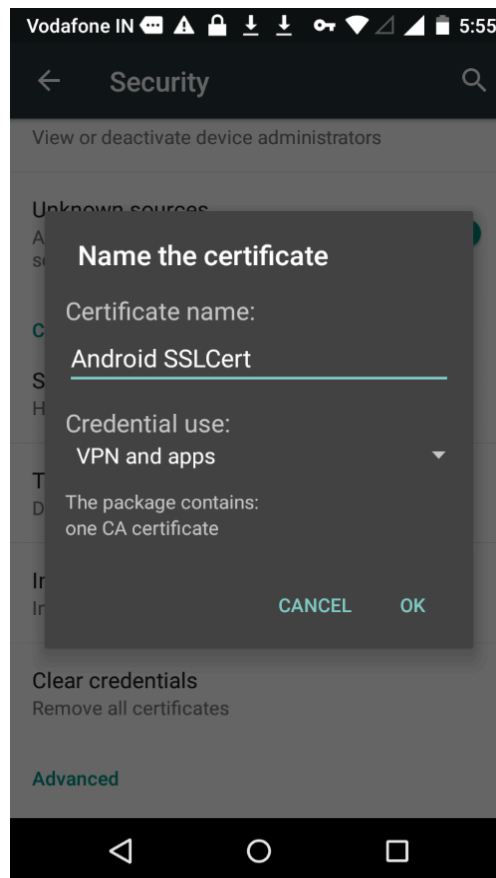


You will see the following screen when connected:



Note: You also need to trust the SSL certificates in order to view HTTPS pages over the VPN.

- Go to 'Settings' > 'Security' > 'Credential Storage' > 'Install from SD card'. Please note this may vary depending on the Android version.
- Select the 'AndroidSSLCert.pem' certificate from the download location, enter the name and tap 'OK'



You can view the certificate in 'Settings' > 'Security' > 'Trusted Credential' > 'User'. Note - The storage path may vary depending on the device and Android version.

The mobile device will be enrolled and shown as follows:

Mobile Devices								+ Add New Mobile Device
#	Company	Email	Remark	Mode	Status	Last Login/Logout Activity	Actions	
1	vtiger	fiatlina@gmail.com		VPN	Installed, Active	2018-11-12 11:51:11 - Login		
2	vtiger	gzd.lkn@gmail.com		VPN	Not installed	N/A		
3	vtiger	licencetype@zippiex.com		VPN + Mobile Agent	Not installed	N/A		

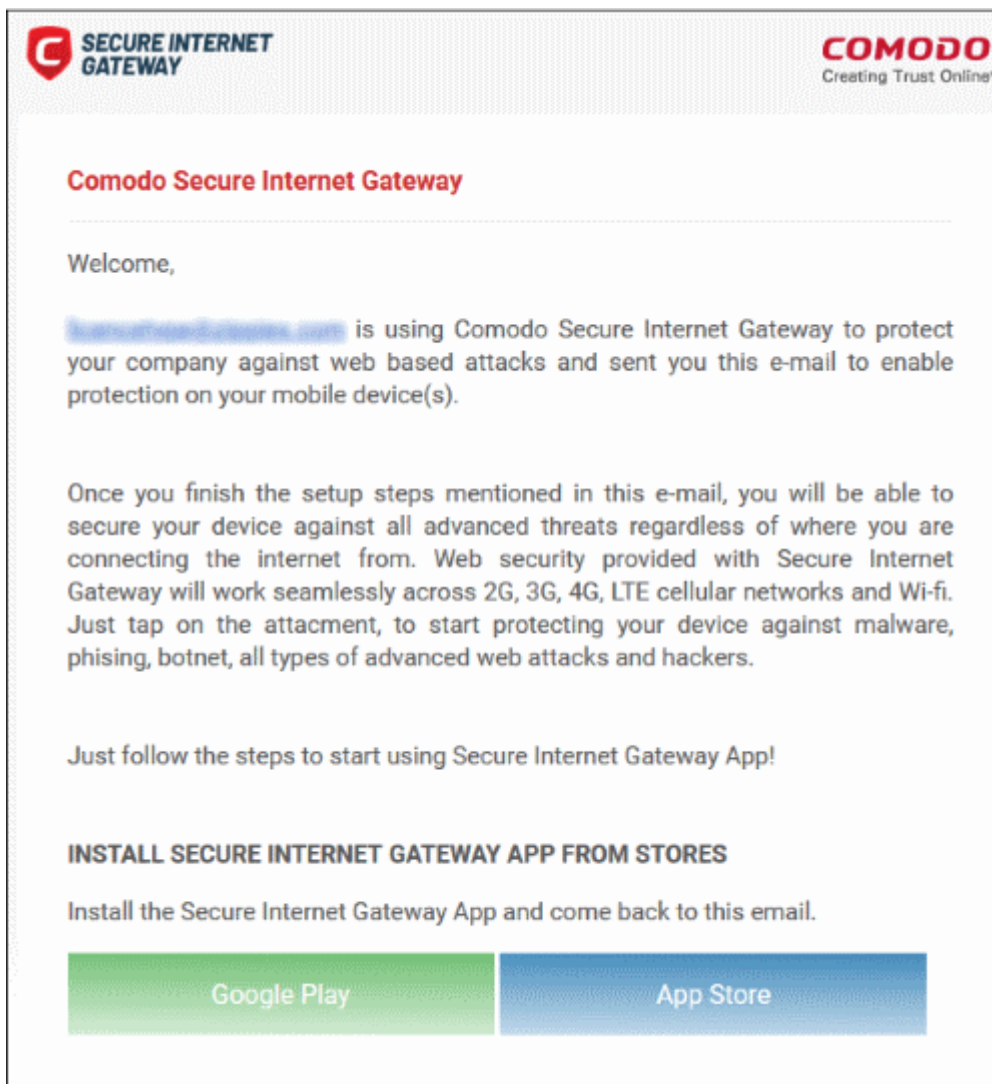
- No rules are applied to mobile devices by default.
- You can apply device specific policy according to your requirements. See '[Manage CSIG Rules](#)' and '[Apply Policies to Networks and Roaming / Mobile Devices](#)' for help to configure and deploy security policies to mobile devices.

CSIG Mobile App

- Users are initially added to the list with a device status of 'Not installed':
- CSIG will send device enrollment emails to all users that you add.

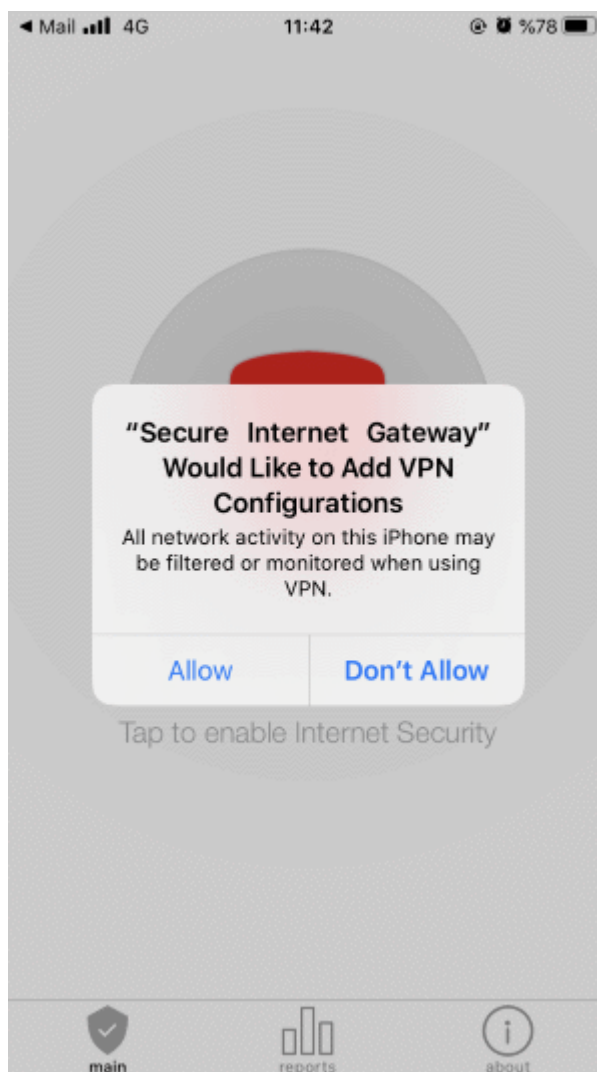
Mobile Devices								+ Add New Mobile Device
#	Company	Email	Remark	Mode	Status	Last Login/Logout Activity	Actions	
1	vtiger	fiatlina@gmail.com		VPN + Mobile Agent	Not installed	N/A		
2	vtiger	gzd.lkn@gmail.com		VPN	Not installed	N/A		
3	vtiger	licencetype@zippiex.com		VPN + Mobile Agent	Not installed	N/A		

- Users should open the email on their device. The email contains clear instructions how to install the CSIG app on Android and iOS devices:

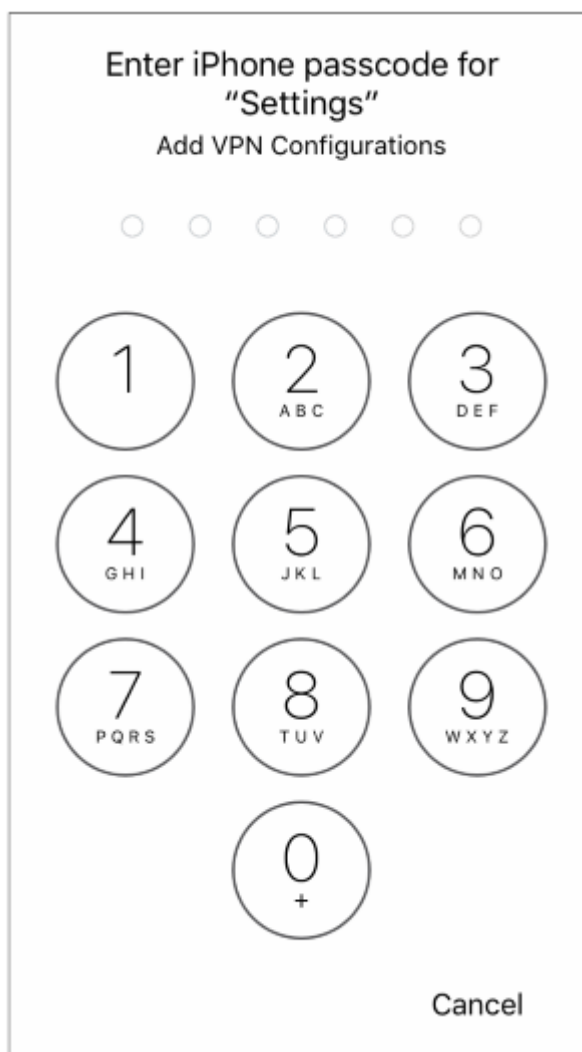


Instructions for iOS

- Open the enrollment mail on the iOS device
- Select 'App Store' and download the app from the Apple store.
- After installation, select 'Activate iOS App' in the mail.
- Next, open the app, tap the 'CSIG' button and hit 'Allow'

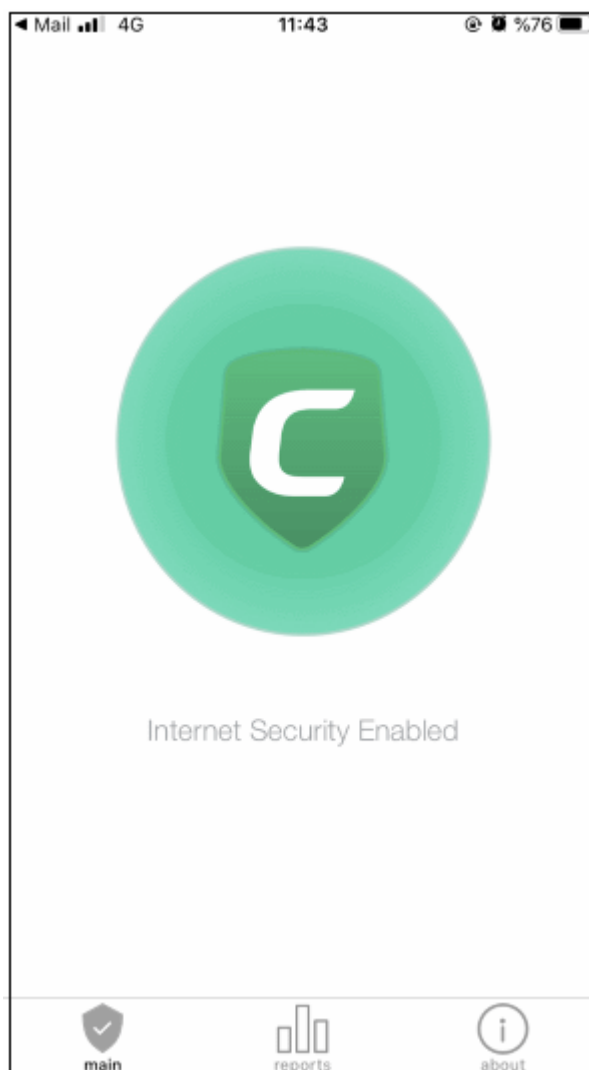


- Provide the device password if requested:



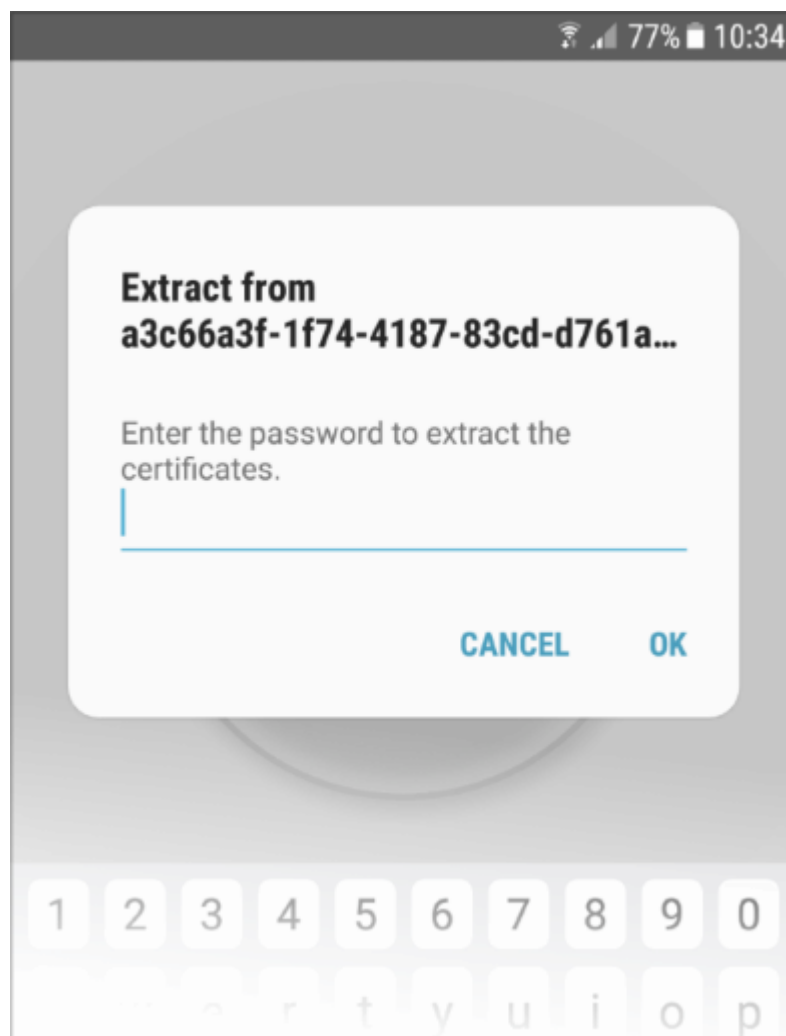
That's it. The iOS device is successfully enrolled to Secure Internet Gateway.

- You also need to trust the SSL certificates in iOS in order to view HTTPS pages over the VPN.
 - Go to 'Settings' > 'General' > 'About' > 'Certificate Trust Settings' and enable full trust for root certificates.
-
- Tap the CSIG shield icon to enable internet security
 - The following screen is shown once the device is connected:



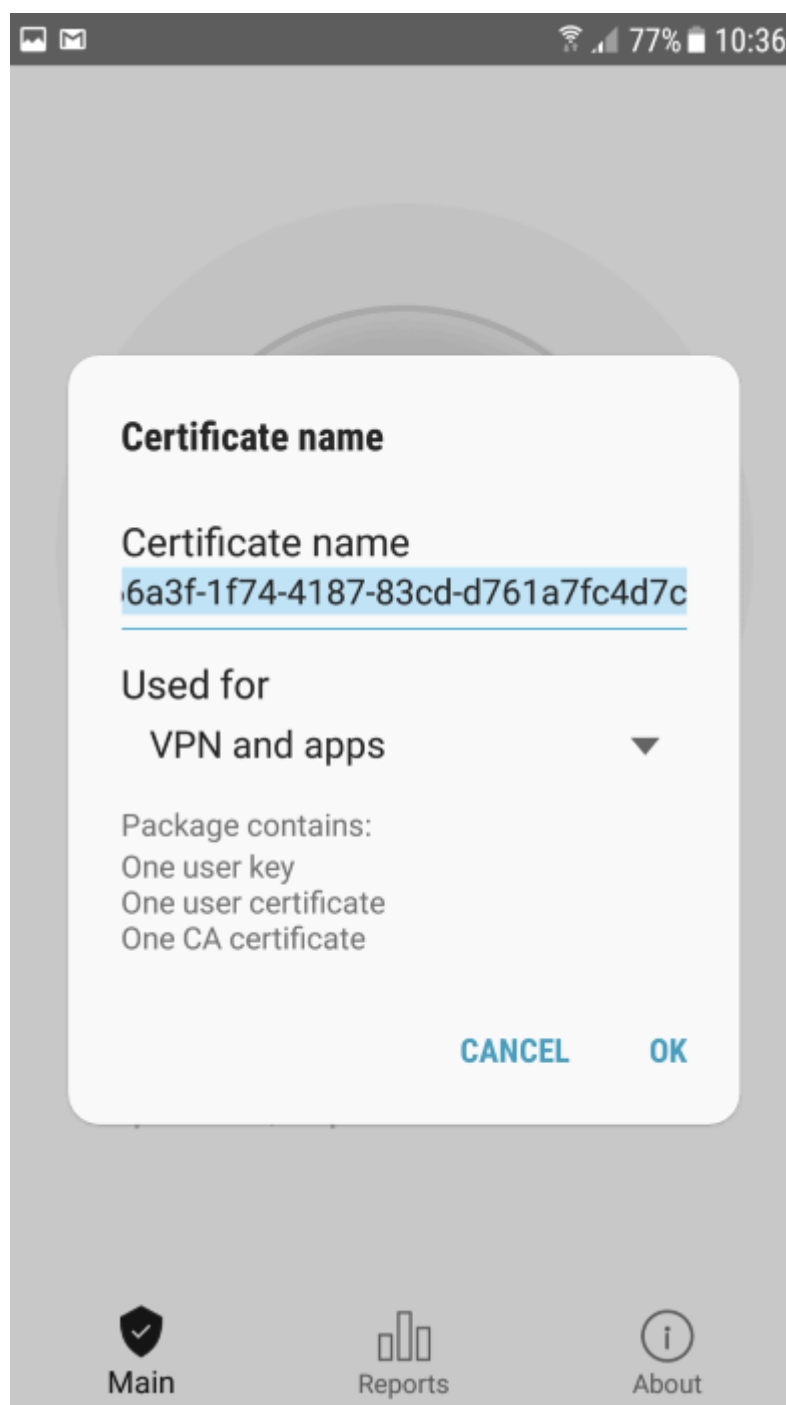
Instructions for Android

- Open the enrollment mail.
- Select 'Google Play' and install the app from the Play Store.
 - Please note, the screens may vary depending on the Android version.
- After installation, select 'Activate Android App' in the mail.
- The activation password is copied to the clipboard after selecting 'Activate Android App'.
- Next, tap the 'CSIG' icon:



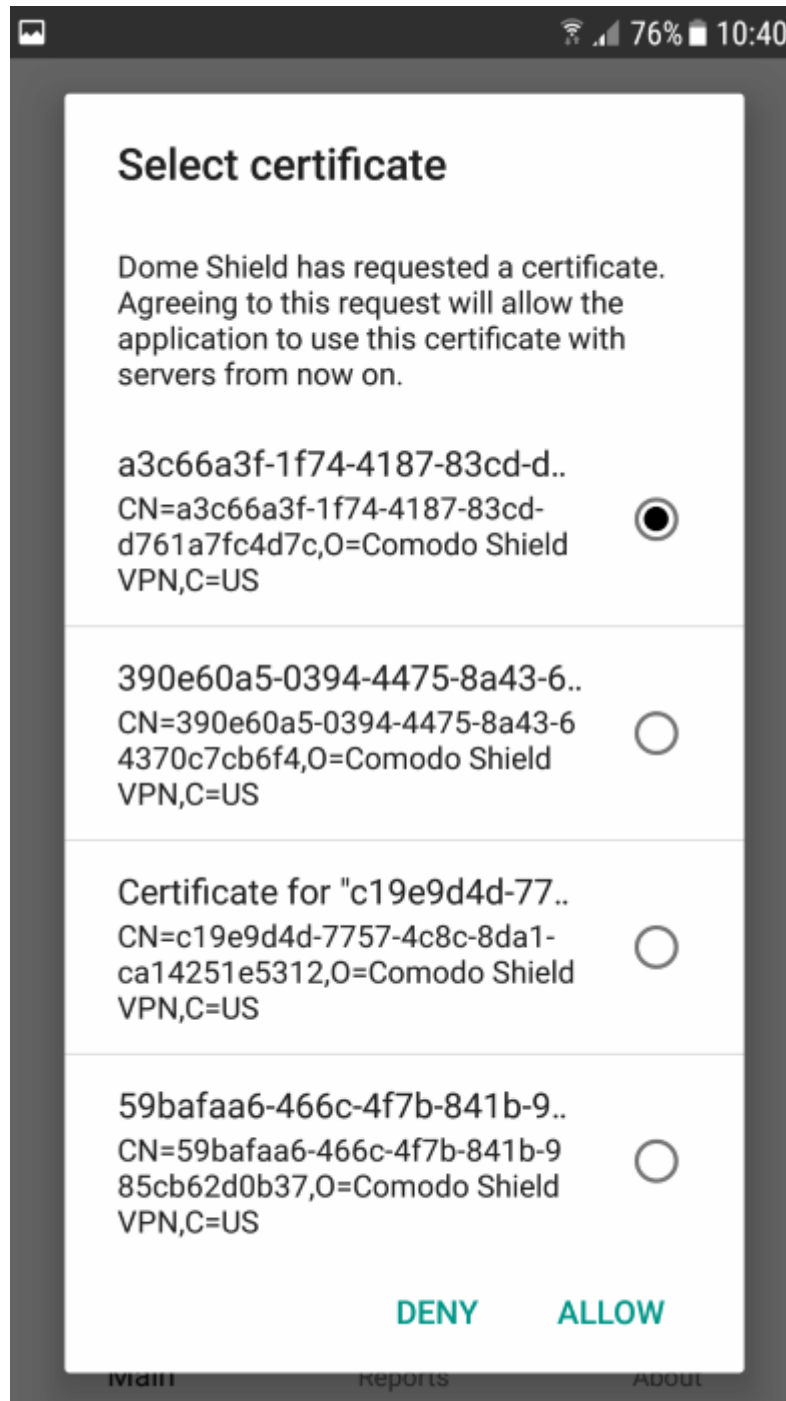
- Long press in the password field and select 'Paste'
- Select 'OK'

The certificate name field is auto-filled with the certificate's unique identifier:



- Touch 'OK'

The VPN certificate is pre-selected in the 'Select certificate' screen:



- Select 'Allow'

That's it. The app is activated and the device enrolled. Device details are shown in the 'Mobile Devices' screen in Secure Internet Gateway:

Mobile Devices + Add New Mobile Device

filter

#	Company	Email	Remark	Mode	Status	Last Login/Logout Activity	Actions
1	vtiger	fiatlina@gmail.com		VPN + Mobile Agent	Installed, Active	2018-11-12 12:33:22 - Login	<input type="button" value="⊞"/>
2	vtiger	gzdlakn@gmail.com		VPN	Not installed	N/A	<input type="button" value="⊞"/>
3	vtiger	licencotype@rippix.com		VPN + Mobile Agent	Not installed	N/A	<input type="button" value="⊞"/>

Important Note:

You also need to trust the SSL certificates in order to view HTTPS pages over the VPN.

- Go to 'Settings' > 'Security'
- Select 'Install from SD card'
- Select 'AndroidSSLCert.pem'
- Enter 'AndroidSSLCert' in the 'Name the certificate' screen.
- Hit 'OK' when finished

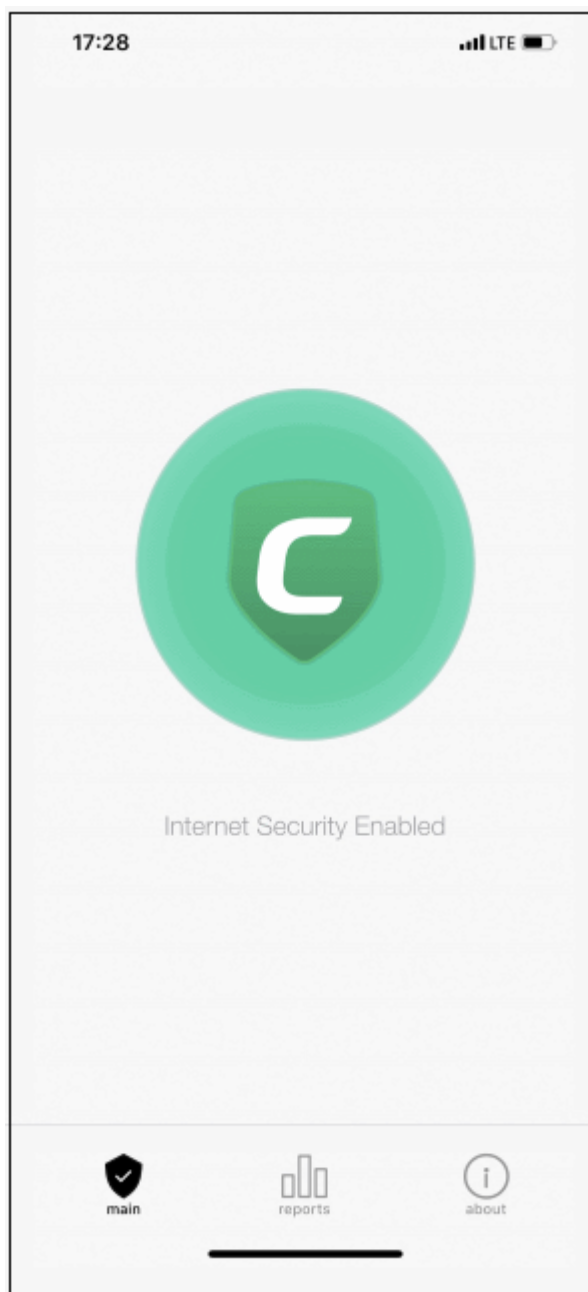
The CSIG app on the mobile device (iOS and Android) can be connected or disconnected by the user. Please note, protection is only available if the app is connected.



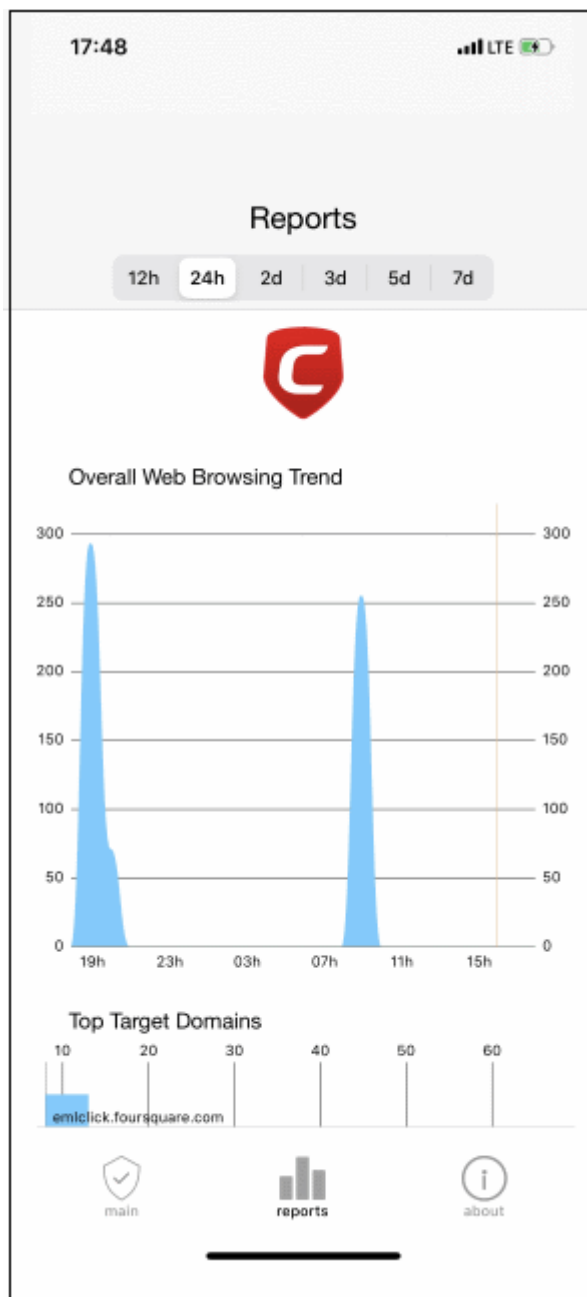
- Tap the CSIG icon

The CSIG app opens

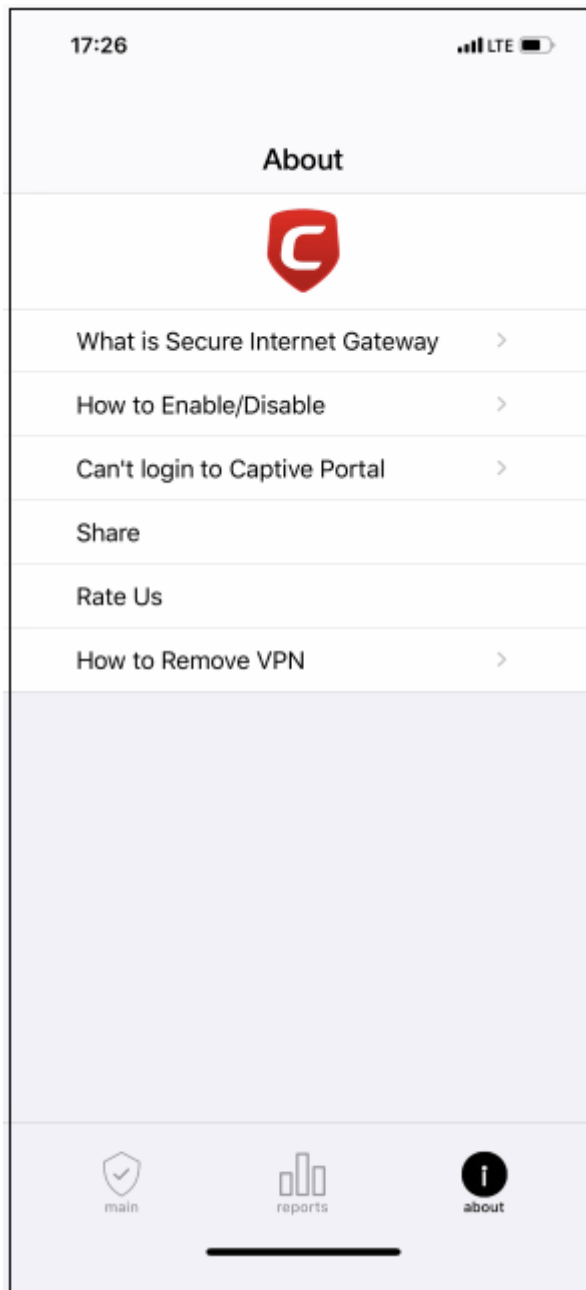
- Main - Select the icon to connect to CSIG / disconnect from CSIG.



- Reports - View reports for:
 - Overall Web Browsing Trend
 - Top Target Domains
 - Top Blocked Domains
 - Overall Advanced Threats
 - Top URL Categories



- About - Detailed information about Secure Internet Gateway

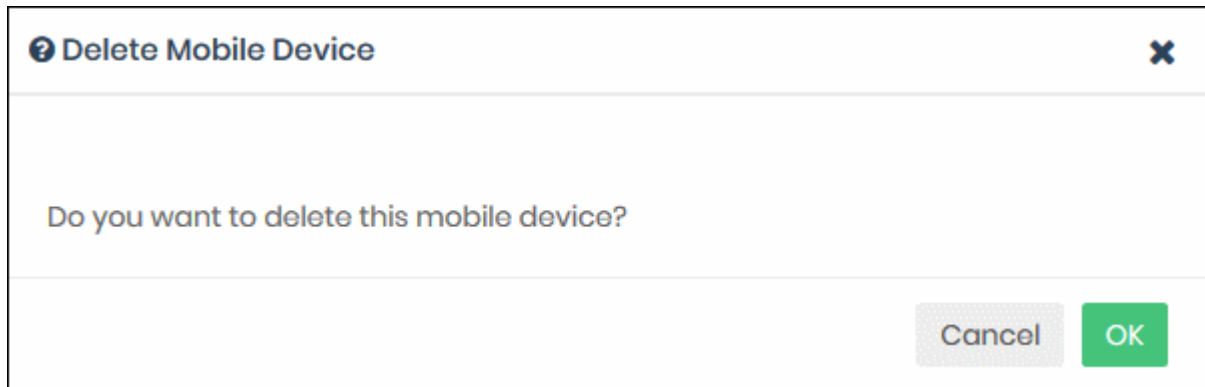


- What is Secure Internet Gateway - Brief description about the product
- How to Enable / Disable - Instructions how to connect / disconnect to CSIG
- Can't login to Captive Portal - Troubleshooting instructions
- Share - Send the app location details to your friends
- Rate Us - Rate the CSIG app
- How to Remove VPN - Instructions how to remove the CSIG VPN

Deleting a mobile device

Web protection policies will no longer be applied when you delete a mobile device.

- Click the trash can icon beside a device to delete it.



- Click 'OK' to confirm removal of the device from the list.

4.4 Manage Imported Sites and Virtual Appliances

- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances'

The sites & virtual appliances area lets you:

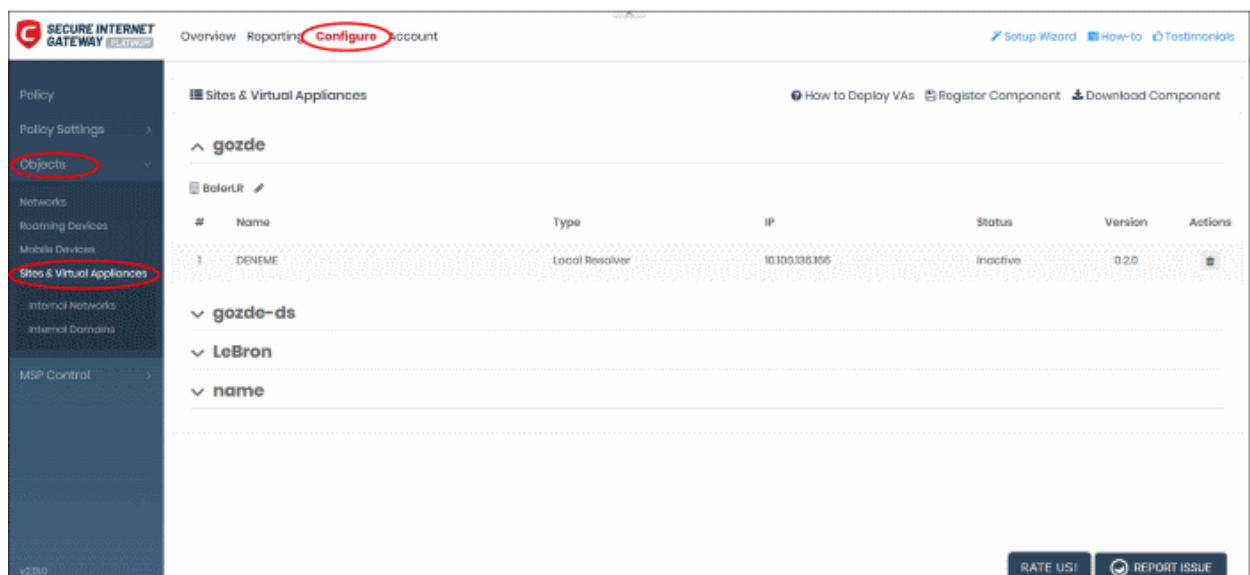
- Download local resolver virtual appliances for installation on your network sites
- Register the resolvers so the networks are imported to Secure Internet Gateway
- Manage the network sites which you have imported

See **Setup Local Resolver Virtual Machines and Import Sites** if you need help to install and register the resolvers.

- Note - the local resolver feature is only available with Platinum licenses.

Manage imported sites

- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances'



- The links on the right of the title bar let you download and register the VA's:
 - **How to Deploy VAs** - Opens guides which explain how to deploy the local resolver VA's.
 - **Register Component** - Enroll a virtual appliance that you have already deployed, and import the network on which it is implemented. See **Step 3 - Register the Master VA** in **Setup Local Resolver Virtual Machines and Import Sites** for more details.

- **Download Component** - The package required to deploy the virtual appliance. See **Step 1 - Download the Setup File** in **Setup Local Resolver Virtual Machines and Import Sites** for more details.
- The interface shows a list of registered virtual appliances.
 - MSP customers can sort the list by company name.

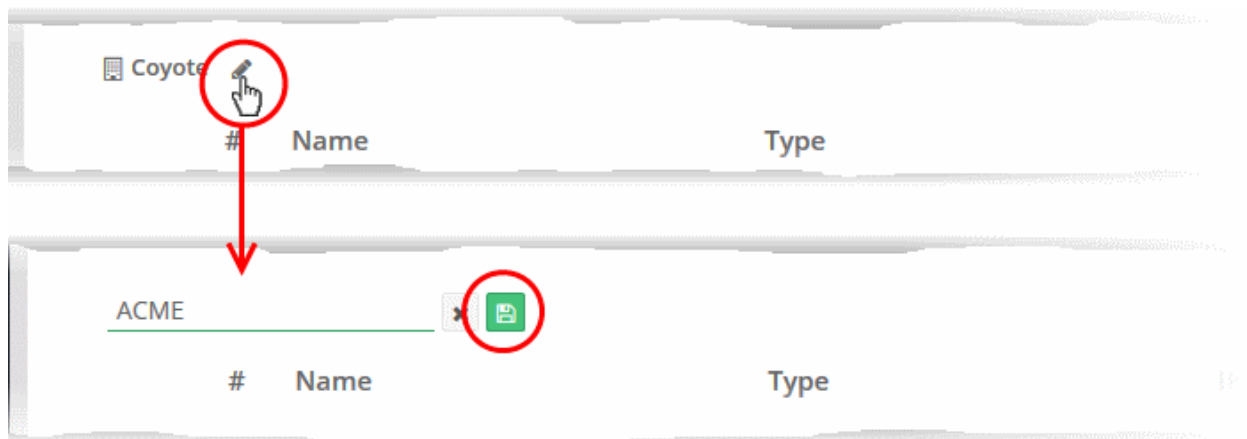
Sites & Virtual Appliances - Column Descriptions	
Column Header	Description
Name	Label assigned to the virtual appliance (VA) during initial configuration.
Type	The kind of VA which is installed on the network.
IP	IP address assigned to the VA.
Status	Connection status of the VA. The VA needs to be connected for Secure Internet Gateway to apply the policies to endpoints.
Version	Software version number of the VA.
Actions	Remove the appliance.

The interface lets you:

- **Edit the name of the network site**
- **Remove a virtual appliance**

Edit the name of a site

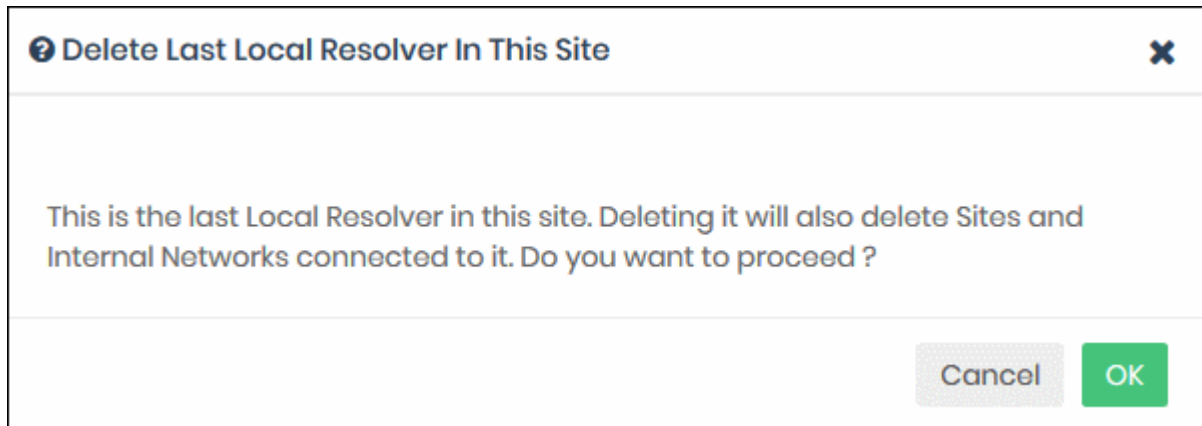
- Click the pencil icon beside the site name
- Enter a new name for the site



- Click the 'Save' icon

Remove a virtual appliance

- Click the trashcan icon in the row of the appliance
- Click 'OK' in the confirmation dialog:



The appliance is removed from Secure Internet Gateway.

- Web protection policies are no longer applied to endpoints.
- The site is also removed if no other appliance is registered on the same network.

Define Internal Networks and Internal Domains

- You can define internal IP addresses or ranges within the site as network objects. This lets you apply different web protection policies to them as required. See [Add Internal Networks](#)
- You can specify internal domains within imported sites. The resolvers will use local DNS servers to resolve requests from the clients for these domains. This reduces bandwidth usage as requests are not forwarded to global DNS servers. See [Add Internal Domains](#)

4.4.1 Add Internal Networks

- Click 'Configure' > 'Objects' > 'Internal Networks'

The local resolver lets you apply tailor-made security policies to individual endpoints and internal sub-nets.

- The internal networks interface lets you define individual IPs or ranges as objects. You can then apply security policies to these objects.

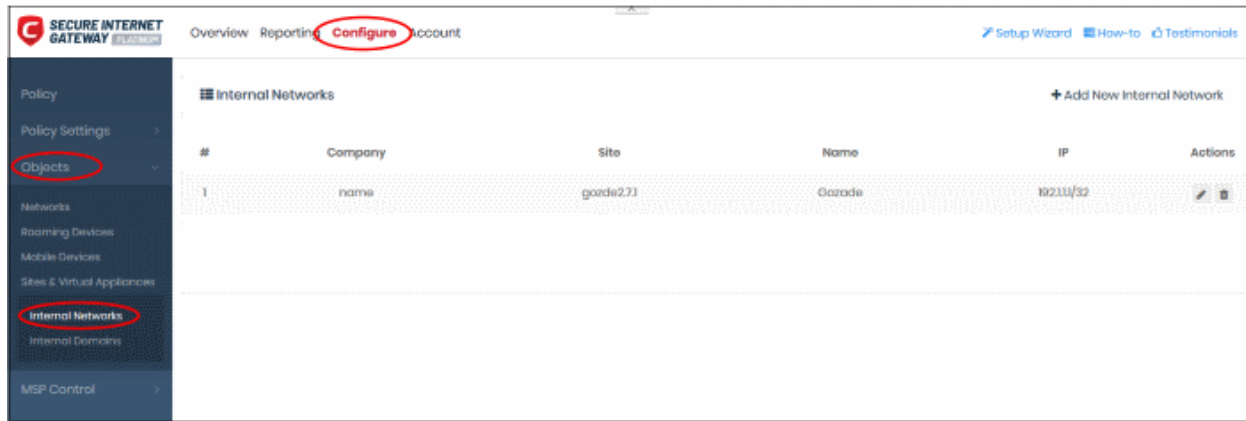
Process in brief:

- Add the IP address of the endpoint and/or IP range.
- Create rules for the endpoints/internal networks.
- Create a policy which uses the rules. The addresses you added earlier can be selected from the 'Objects' drop-down as policy targets.

Note - A policy applied to a 'Site' will over-rule any policy applied to its internal network objects. Secure Internet Gateway will apply the site policy to the individual objects and ignore any individual policies for those objects.

Manage Internal Networks

- Click 'Configure' > 'Objects' > 'Internal Networks'



Internal Networks - Column Descriptions

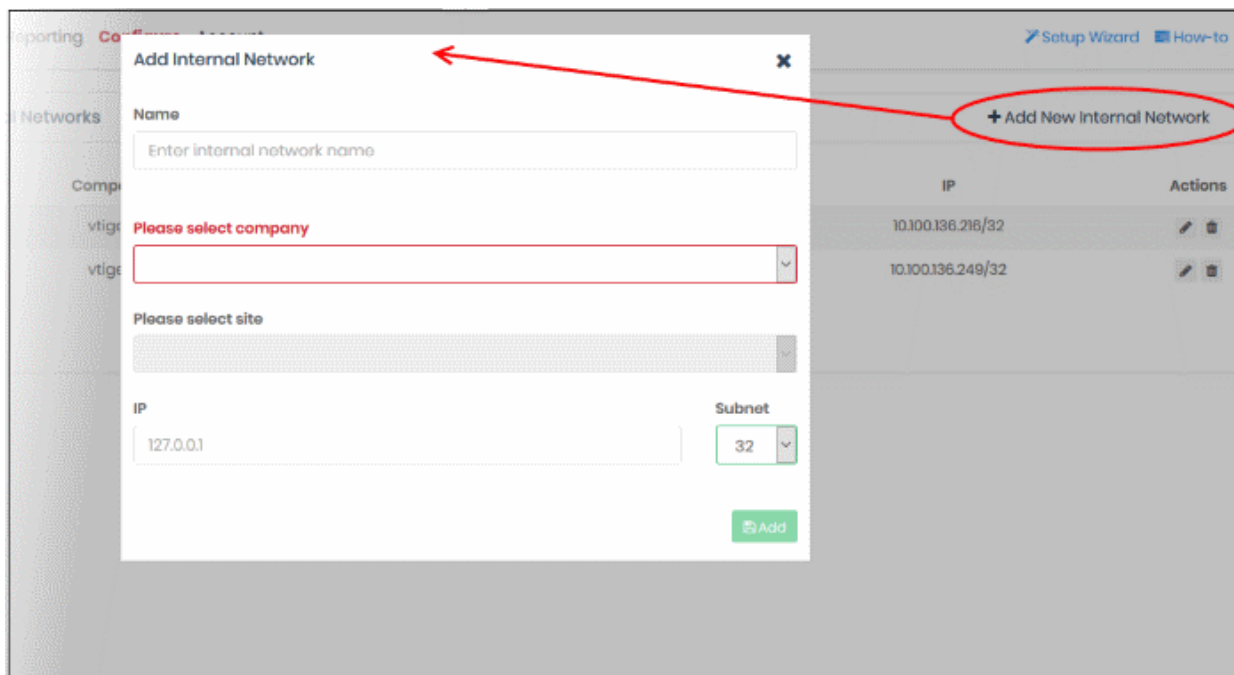
Column Header	Description
Company	MSPs only. Name of the organization to which the network site belongs.
Site	The network to which the endpoints or the sub-net belongs.
Name	The label of the endpoint or sub-net.
IP	The address of the endpoint or sub-net.
Actions	Edit or remove the endpoint/internal network.

The interface lets you:

- **Add internal networks**
- **Edit internal networks**
- **Remove internal networks**

Add Internal Network Objects

- Click 'Configure' > 'Objects' > 'Internal Networks'
- Click 'Add New Internal Network'



'Add Internal Network' dialog - Table of Parameters

Form Element	Description
Name	Label of the internal network object. This name appears in the object drop-down under the network site when you create a policy.
Please select company	MSP customers only. <ul style="list-style-type: none"> Choose the company for whom you want to add the network
Please select site	Choose the site to which the internal network belongs
IP	IP address of the internal network in CIDR notation. <ul style="list-style-type: none"> Enter the start IP address of the internal network block. Select the network prefix from the 'Subnet' drop-down. Secure Internet Gateway can accept network prefixes from /24 to /32. To add a single endpoint, enter the IP address of the endpoint and choose 32 as network prefix

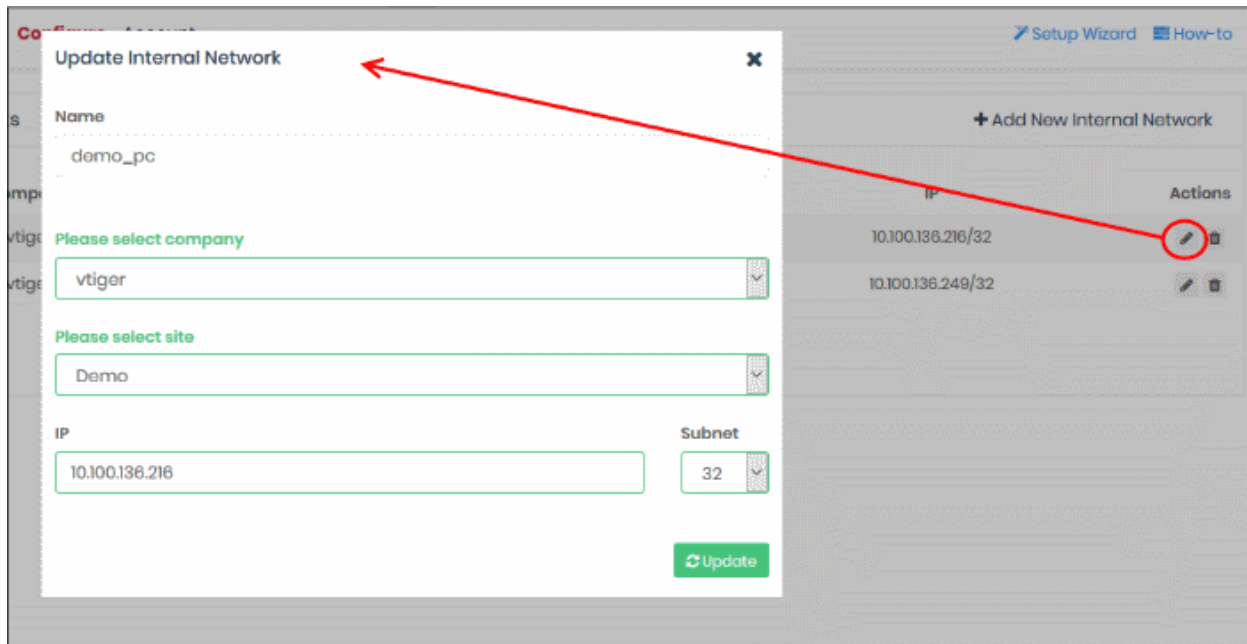
- Click 'Add'

The internal network object is added to the list. It will be available in the 'Object' drop-down as a target when creating a new policy. See [Apply Policies to Networks and Roaming / Mobile Devices](#) for more details.

Edit Internal Network Objects

You can change the site/IP range of an internal network object at anytime.

- Click 'Configure' > 'Objects' > 'Internal Networks'.
- Click the pencil icon beside the network object you want to edit:



The 'Update Internal Network' dialog opens.

- The dialog is similar to 'Add Internal Network' dialog.
- You cannot edit the name of the internal network object
- You can edit the company, site and the IP range for the object. See **above** if you need help with this.
- Click 'Update' to save your changes

The internal network object's policy will be applied to the endpoints in the new IP range.

Remove Internal Network Objects

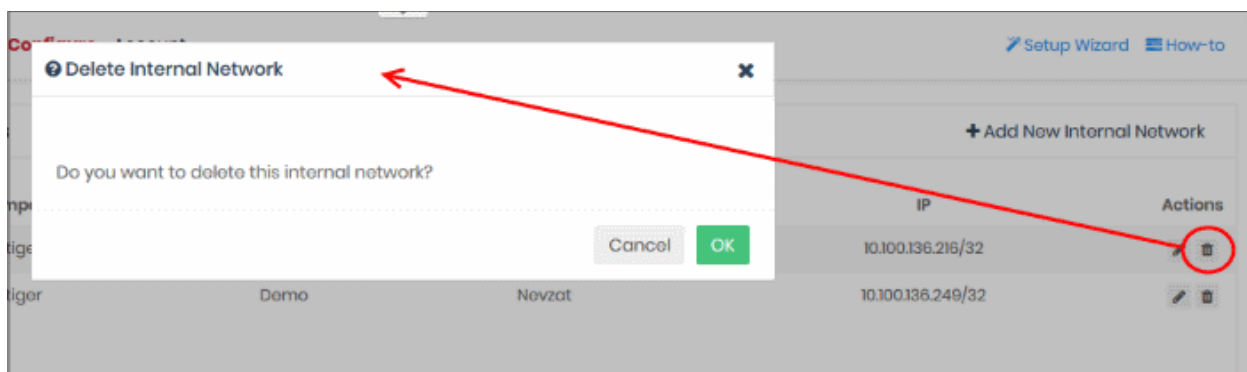
You can remove internal network objects if you no longer want to apply a policy to them.

Once removed:

- If a policy exists for the parent site of the internal network, then this parent policy is applied to the endpoints in the internal network
- If no policy exists for the parent site, then the default security policy is applied to the network's endpoints

Remove an internal network object

- Click 'Configure' > 'Objects' > 'Internal Networks'.
- Click the trash can icon beside the internal network object to be removed.



- Click 'OK' in the confirmation dialog to remove the internal network object.

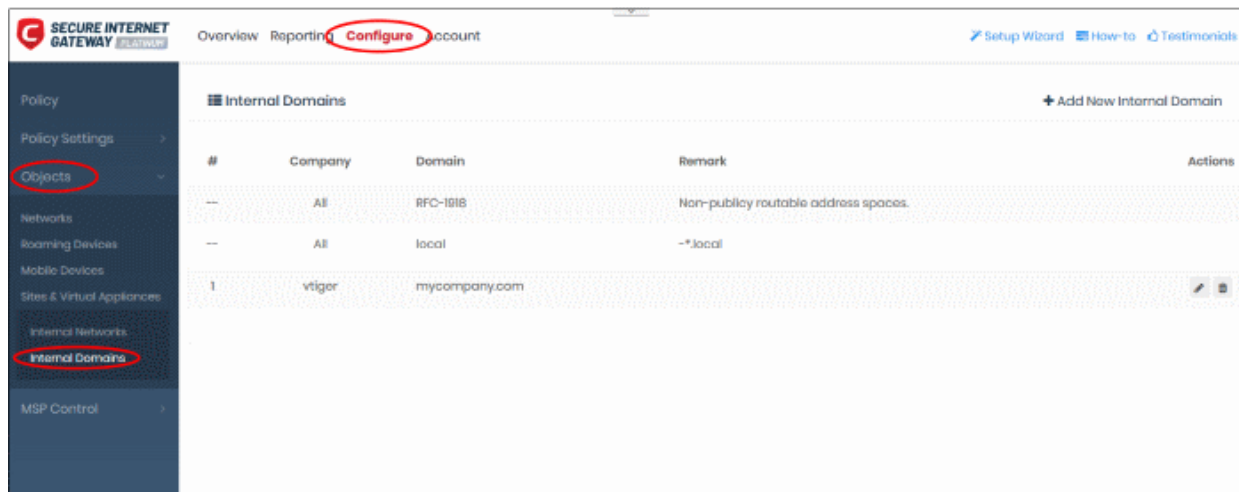
4.4.2 Add Internal Domains

Click 'Configure' > 'Objects' > 'Internal Domains'

- The resolvers will first check for local DNS requests from endpoints in imported sites
- If the request is for an internal domain then the resolver handles it using local DNS servers. This is instead of sending the request to CSIG's public DNS servers, saving your bandwidth.

Manage internal domains in imported sites

- Click 'Configure' > 'Objects' > 'Internal Domains'



Internal Domains - Column Descriptions

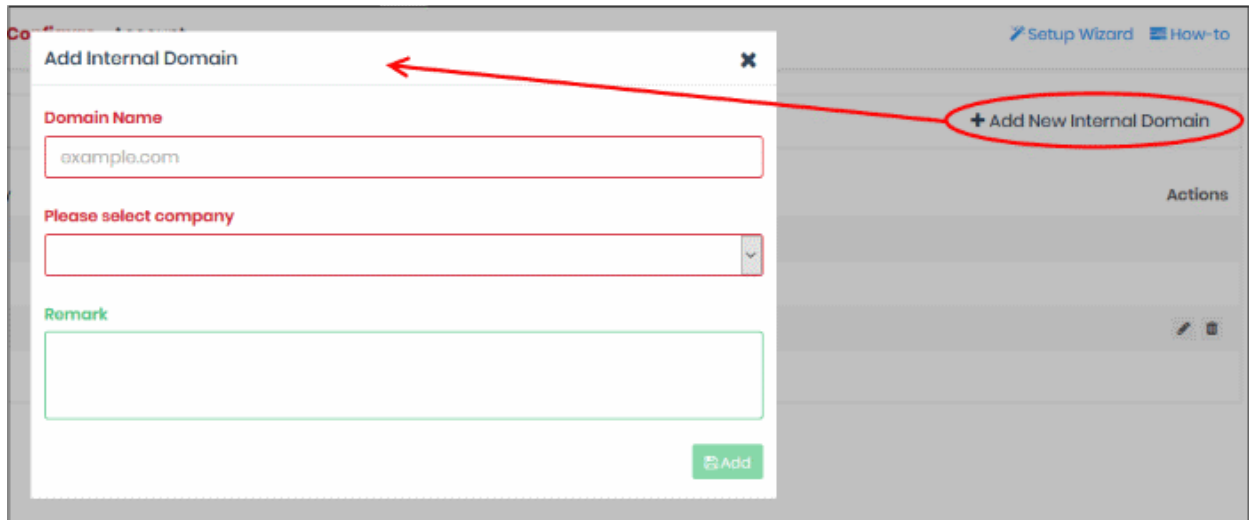
Column Header	Description
Company	MSPs only. Name of the organization to which the internal domain belongs.
Domain	The name of the internal domain.
Remark	A short description of the internal domain.
Actions	Edit or remove the internal domain.

The interface lets you:

- **Add internal domains**
- **Edit internal domains**
- **Remove internal domains**

Add Internal Domains

- Click 'Configure' > 'Objects' > 'Internal Domains'
- Click 'Add New Internal Domain'



'Add Internal Domain' dialog - Table of Parameters

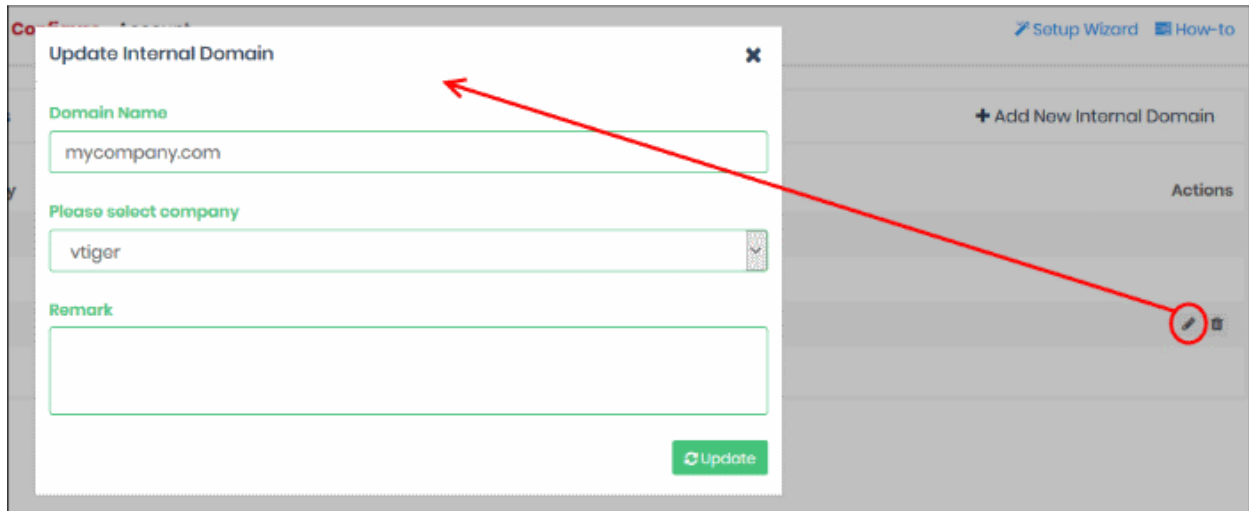
Form Element	Description
Domain Name	<p>The registered name of the internal domain.</p> <ul style="list-style-type: none"> Enter the full domain name (without https://, http://, or www) Prefix the domain with a wildcard character to include all sub-domains. Wildcard character = *. <p>For example: *.internaldomain.com</p>
Please select company	<p>MSP customers only.</p> <ul style="list-style-type: none"> Choose the company for whom you want to add the network
Remark	A short description of the internal domain

- Enter the parameters and click 'Add'.

The internal domain is added to the list.

Edit Internal Domains

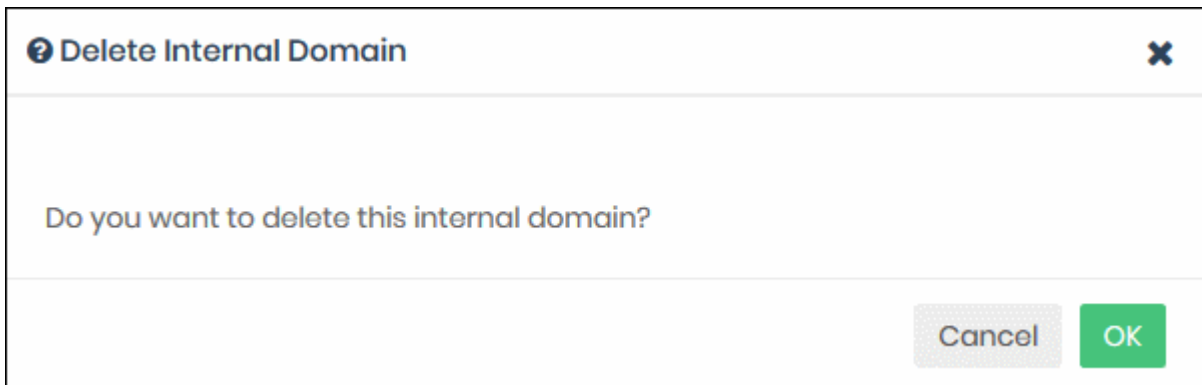
- Click 'Configure' > 'Objects' > 'Internal Domains'
- Click the pencil icon beside the internal domain you want to edit.
- Enter the domain name, company and any remarks in the configuration dialog:



- Click 'Update' to save your changes.
- Configuration is similar to the 'Add Internal Domain' process
- You can edit the company and internal domain name. See the explanation **above** for more details

Remove Internal Domains

- Click 'Configure' > 'Objects' > 'Internal Domains'
- Click the trash can icon beside the internal domain to be removed.

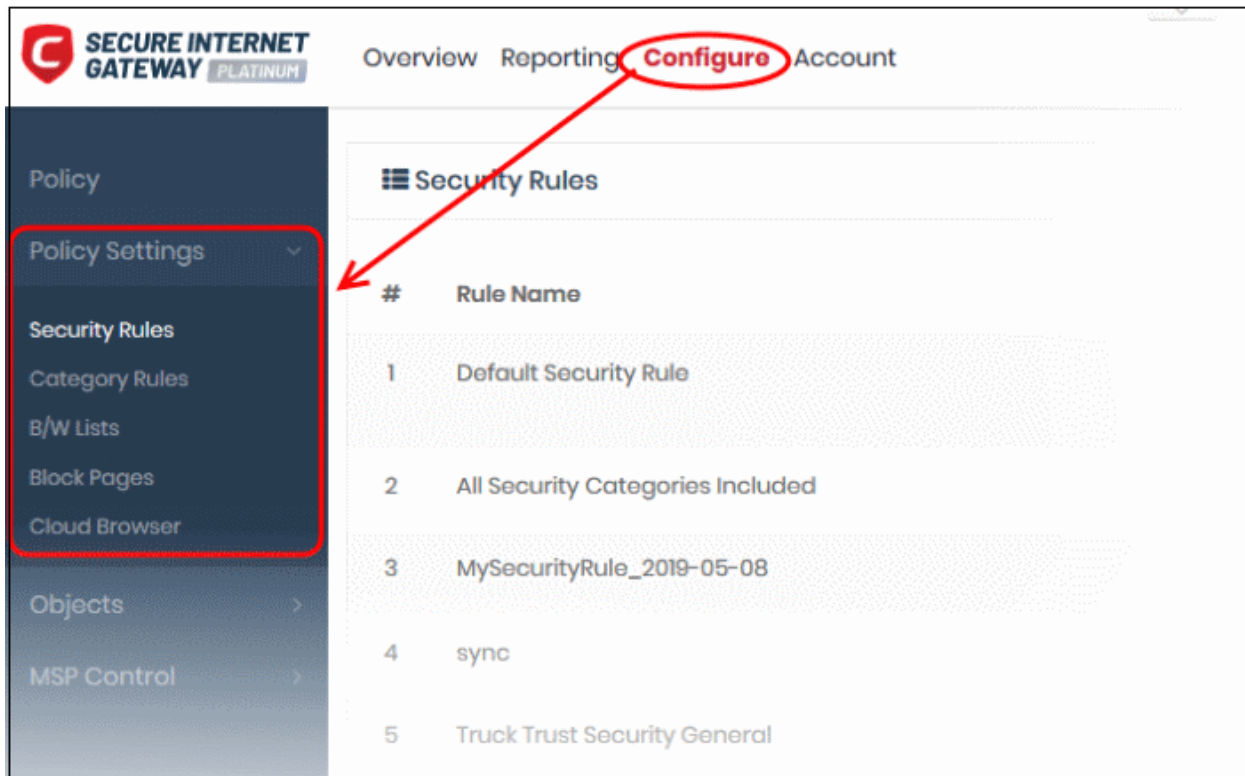


- Click 'OK' in the confirmation dialog to remove the internal domain from the list

5 Manage CSIG Rules

The 'Policy Settings' area lets you create and manage security rules which can be added to your policies.

- Click 'Configure' on the top menu. The 'Policy Settings' menu is on the left:



- Policies consist of security rules, category rules, and blacklist/whitelist rules. You can add one rule of each type to a policy.
- You can also create block pages which are shown to users who visit resources you have banned.
- There is a default security rule that blocks phishing, malware and spyware websites. This rule can be used as part of a policy, or you can configure new security rules as required.
- Rule changes are instantly deployed. Any edits you make to a rule are automatically reflected in any policies which use the rule.
- You can customize the block pages used in a policy. For example, you can specify different block pages for category, security and blacklist rules.
- Black and whitelists over-rule any 'Security' or 'Category' rules, allowing you to create exceptions in your policy.
- You can enable 'Comodo Cloud Browser' in a policy to redirect your users to virtual sessions.
- Click 'Configure' > 'Policy' > 'Check Domain Category' to view the details of each category.

Click the links below for more help:

- [Manage Security Rules](#)
- [Manage Category Rules](#)
- [Manage Domain Blacklist and Whitelist](#)
- [Manage Block Pages](#)
- [Configure Cloud Browser Settings](#)

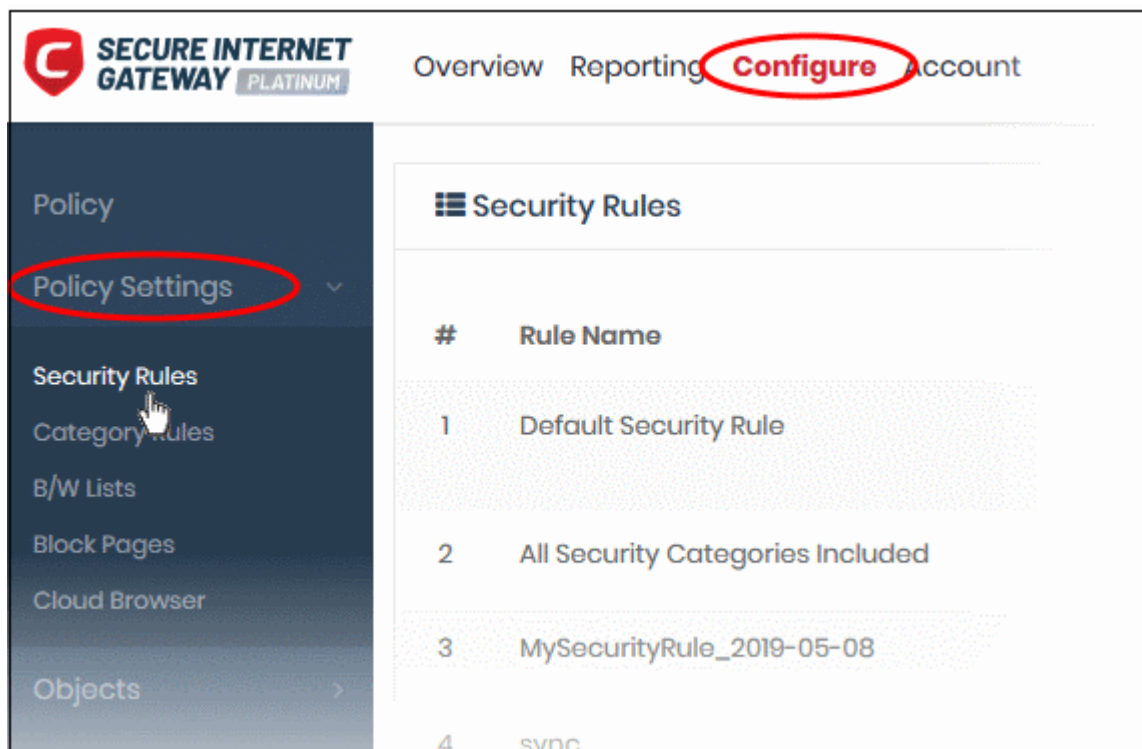
5.1 Manage Security Rules

Click 'Configure' > 'Policy Settings' > 'Security Rules'

- Comodo operates a huge database of harmful websites categorized by threat type. Secure Internet Gateway uses this database to power its security rules.
- Security rules let you block access to sites known to host specific types of threat. Security rule categories include:
 - Malware
 - Botnet/c2c Servers/Bot Infected Sources
 - Phishing
 - Spyware
 - Webspam
 - Drive-by Downloads
 - Tor Nodes
 - P2P Nodes
 - Fake AV
 - Blackhole/Sinkhole Systems
 - VPN Servers
 - Mobile Threats
 - Known DDoS Sources
 - Bitcoin Related
 - PUA Domains
 - Remote Access Services
 - Self Signed SSL Sites
 - Domains with no MX records
 - Spam Sources
 - Brute Forcer/Scanner

Click 'Configure' > 'Policy' > 'Check Domain Category' to view these categories in the interface.

- Secure Internet Gateway ships with a default security rule that blocks phishing, malware and spyware websites. You can use this rule in a policy, or you can configure custom rules as required.



The interface lets you:

- **Create a new security rule**
- **Edit a security rule**
- **Delete a security rule**

Create a new security rule

- Click 'Configure' > 'Policy Settings' > 'Security Rules'
- Click 'Create Security Rule' at top-right


The screenshot shows the 'Create Security Rule' dialog box. At the top right of the background interface, a button labeled '+ Create Security Rule' is circled in red. A red arrow points from this button to the title of the dialog box, 'Create Security Rule'. The dialog box has a close button (X) in the top right corner. Below the title, there are two sections: 'Name' and 'Settings'. The 'Name' section has a text input field. The 'Settings' section has a 'Remark' label and a large text area for entering remarks. A green 'Next' button is located at the bottom right of the dialog box.

- **Name and remarks** - Create a label for the rule and add any comments. These should help you, or another admin, identify the purpose of the rule.
 - Click 'Next' if you want to save your rule at this point.
OR
 - Click 'Settings' to configure the security categories that you want to allow/block:

- Use the switches on the right to allow or block sites in a specific category
- Click the 'Create' button to save your rule

Your new security rule will now be available for selection when **creating a policy**.

Edit a security rule

- Click the edit  button on the right side of the rule you wish to edit:


The 'Update Security Rule' dialog will appear. The dialog is similar to the 'Create Security Rule' dialog explained **above**.

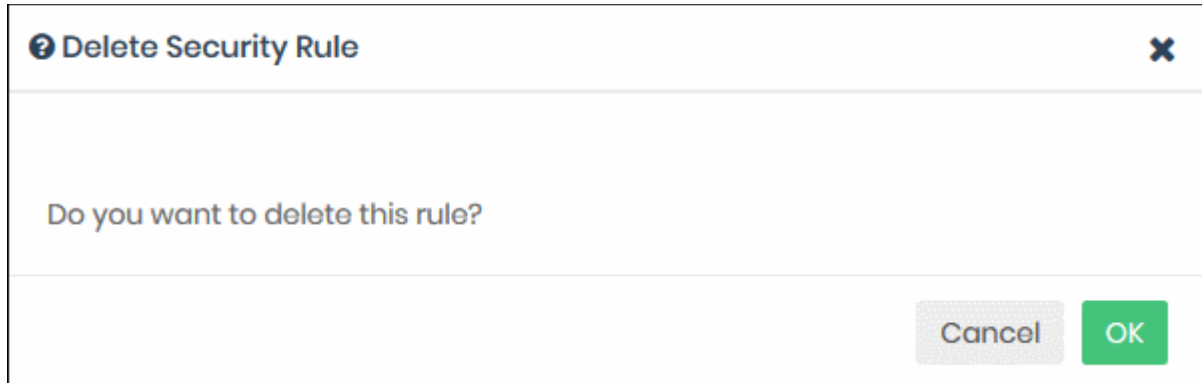
- Modify the name, description and/or category settings per your requirements.
- Click the 'Update' button

Any policies containing the rule are updated accordingly.

Delete a security rule

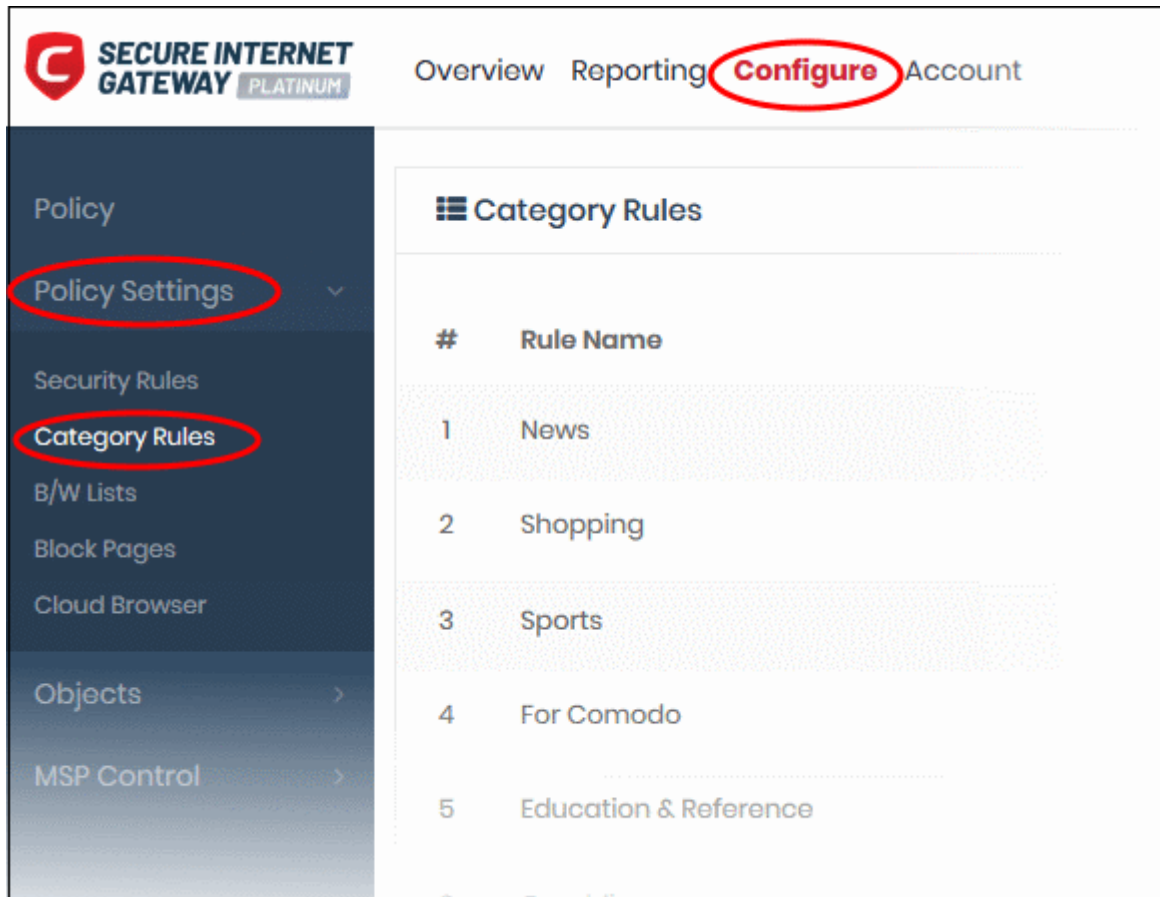
You cannot delete a rule that is currently active in a policy. You have to remove the rule from all policies before deleting it.

- Click the trash can icon  beside a rule to delete it.
- Click 'OK' in the confirmation box to remove the rule:



5.2 Manage Category Rules

- Category rules let you control access to websites based on their content type. For example, you may wish to block access to adult websites, comedy sites, social media sites or sports websites.
- You can add multiple website categories to a single category rule. Category rules are another component of a policy, in addition to security rules and B/W lists.
 - Security rules focus explicitly on harmful categories like phishing and malware. Category rules let you apply policy to sites that fall under a broader range of topics.
- Click 'Configure' > 'Policy Settings' > 'Category Rules' to open the category rules area:



Category Rules - Table of Column Descriptions

Column Header	Description
Rule Name	The label of the rule
Remark	Comments provided for the rule
Actions	Edit / delete the rule

Related information:

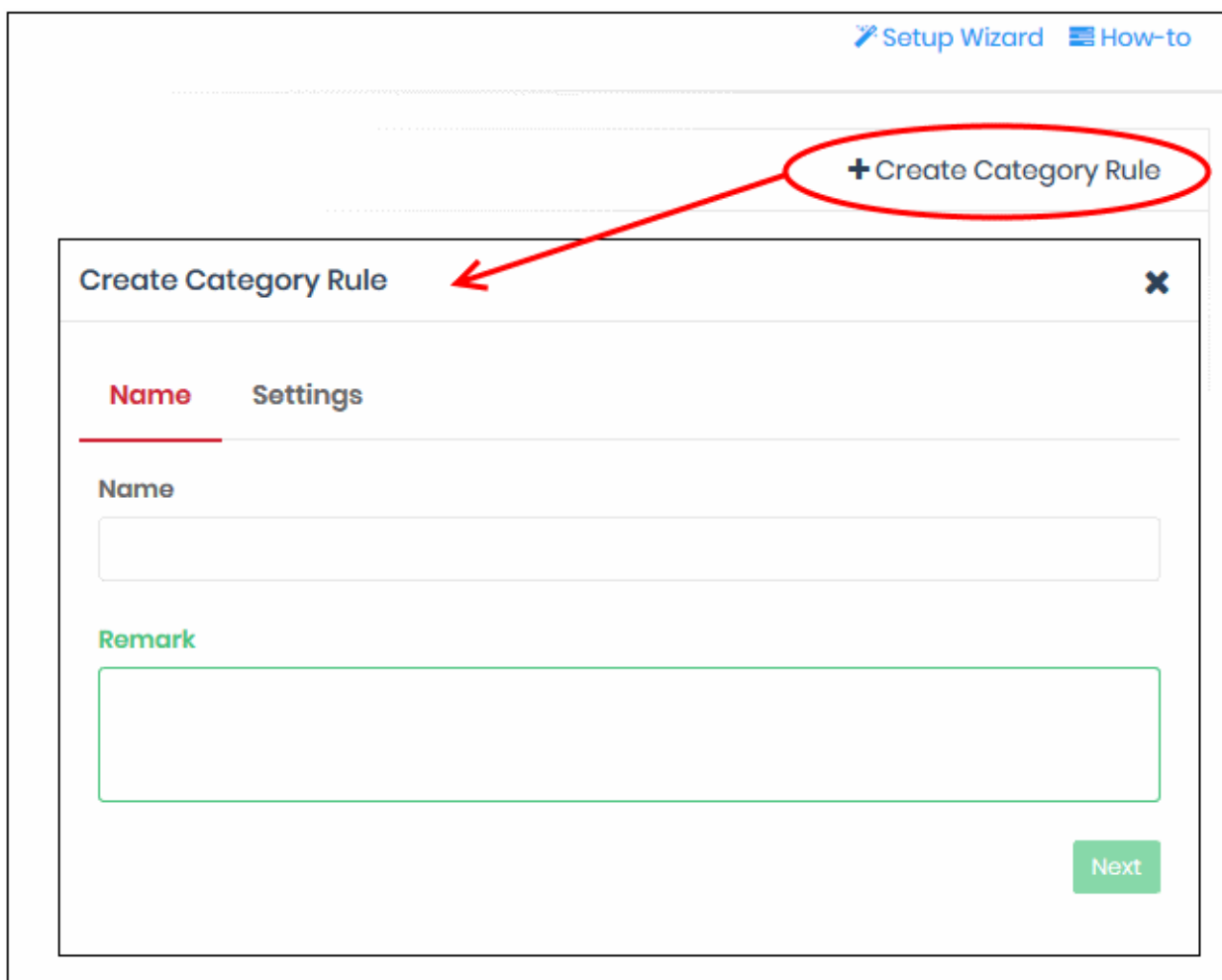
- Click 'Configure' > 'Policy' > 'Domain Classification Requests' to find the category of a particular site.
- You can also propose a new category and recommend that an unclassified site is added to our database. See **Domain Classification Requests** if you need help with this.

The category rules area lets you:

- **Create a new category rule**
- **Edit a category rule**
- **Delete a category rule**

Create a new category rule

- Click 'Configure' > 'Policy Settings' > 'Category Rules'
- Click 'Create Category Rule' at the top right



- Name and remarks - Create a rule label/comments which will help you and others identify the purpose of the rule.
- Click 'Settings' or 'Next' to choose which categories you want to block/allow:

Create Category Rule [X]

Name **Settings**

Select Category

None [v]

Search... [x]

Adult / Sexual

Nudity

Pornography

Adult Content

Intimate Apparel & Swimwear

Personals & Dating

Arts & Entertainment

Media Sharing

- **Select Category** - Use the drop-down to choose the types of website you want to block.
- Main categories are shown in **bold text**, with sub-categories listed underneath. If you select a main category, all sub-categories will be automatically selected. Please review and deselect any sub-categories you wish to allow.
- You can add multiple categories to your rule. The number of categories you have added are displayed at the end of the list:

Create Category Rule [X]

Name **Settings**

Select Category

Media Sharing, Information Security, Online Services, ... (5) [v]

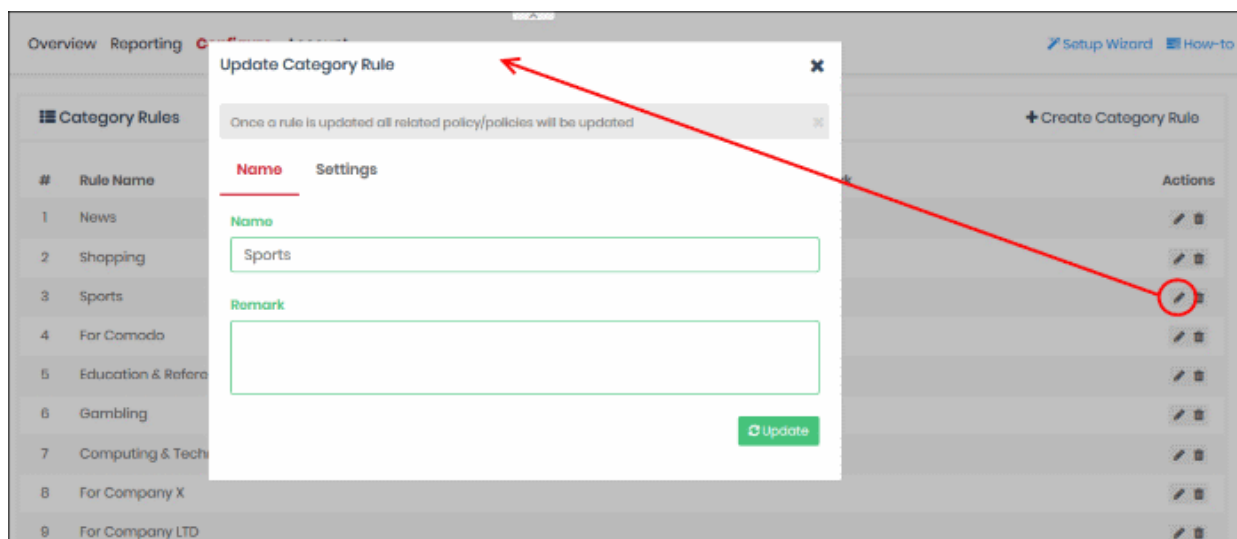
Create

- Click 'Create' when done.

The website category rule is added to the list and will be available for selection when **creating a policy**.

Edit a category rule

- Click the edit  button on the right of a rule:




The update rule dialog is similar to the create rule dialog explained **above**.

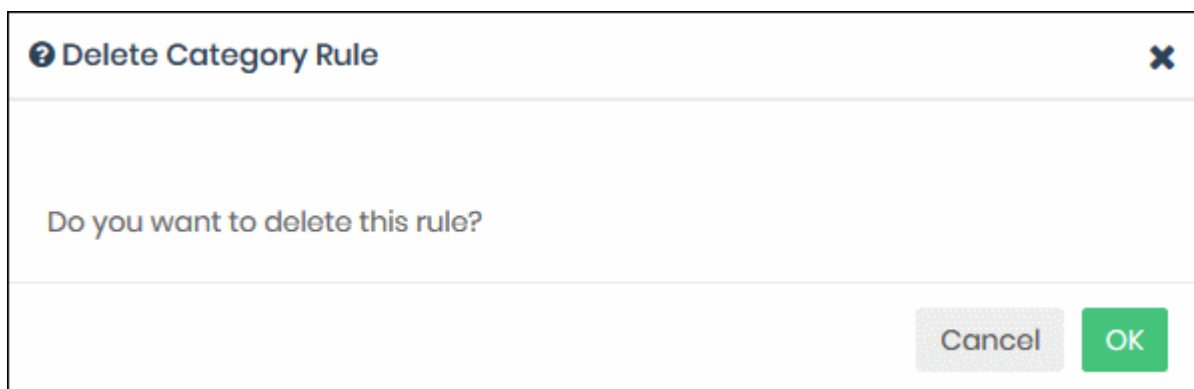
- Modify the name, description and/or category settings as required
- Click the 'Update' button

Any policies which use this rule are updated accordingly.

Delete a category rule

You cannot delete a category rule that is currently active in a policy. You have to remove the rule from all policies before it can be deleted.

- Click the trash can icon  beside a rule to delete it.
- Click 'OK' in the confirmation box to remove the rule:

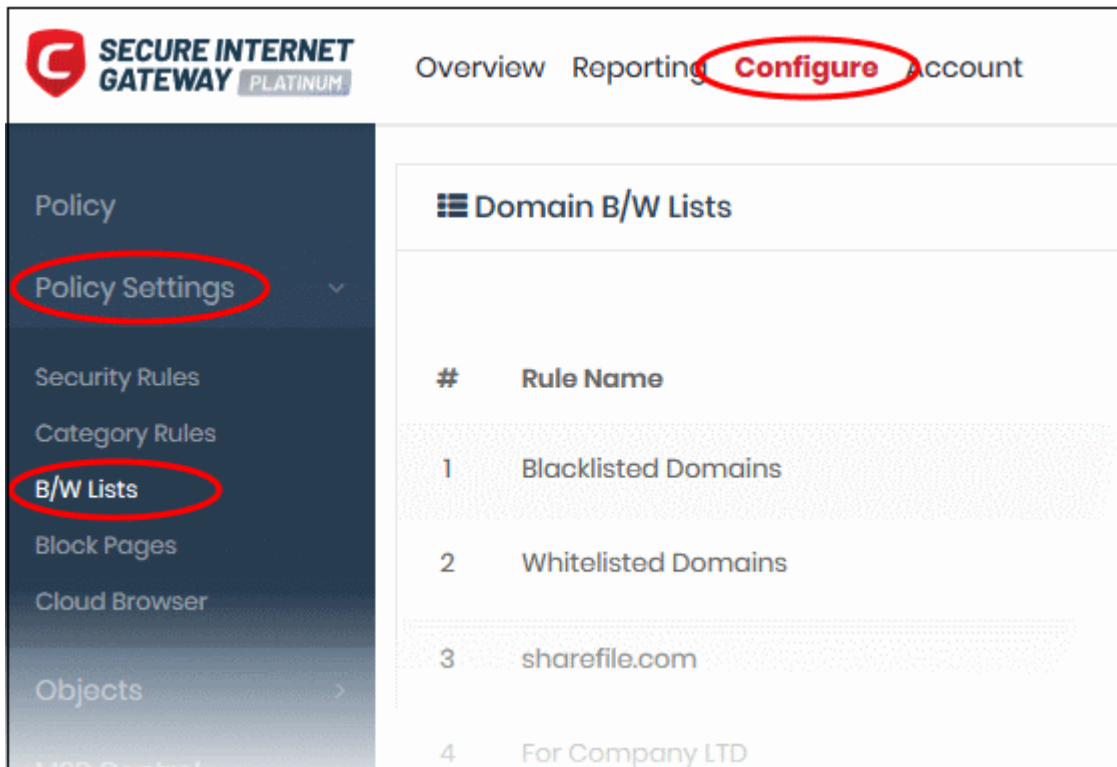


5.3 Manage Domain Blacklist and Whitelist

Black and white lists let you block or allow specific domains. Black/white lists are often used to create exceptions to security/category rules.

- You can add specific websites to a blacklist or whitelist according to your organization's web security policies.
 - Blacklists and whitelists over-rule category and security rules.
 - Whitelists over-rule blacklists

- E.g. - If you block shopping sites in a category rule, but add 'shop.com' to the whitelist, then 'shop.com' is allowed.
- If you enable 'Only B/W Mode' in a policy, then only the black and white lists are consulted. All security and category rules are ignored.
- Click 'Configure' > 'Policy Settings' > 'B/W Lists' to open the 'B/W Lists' area:



The list of B/W list rules are displayed.

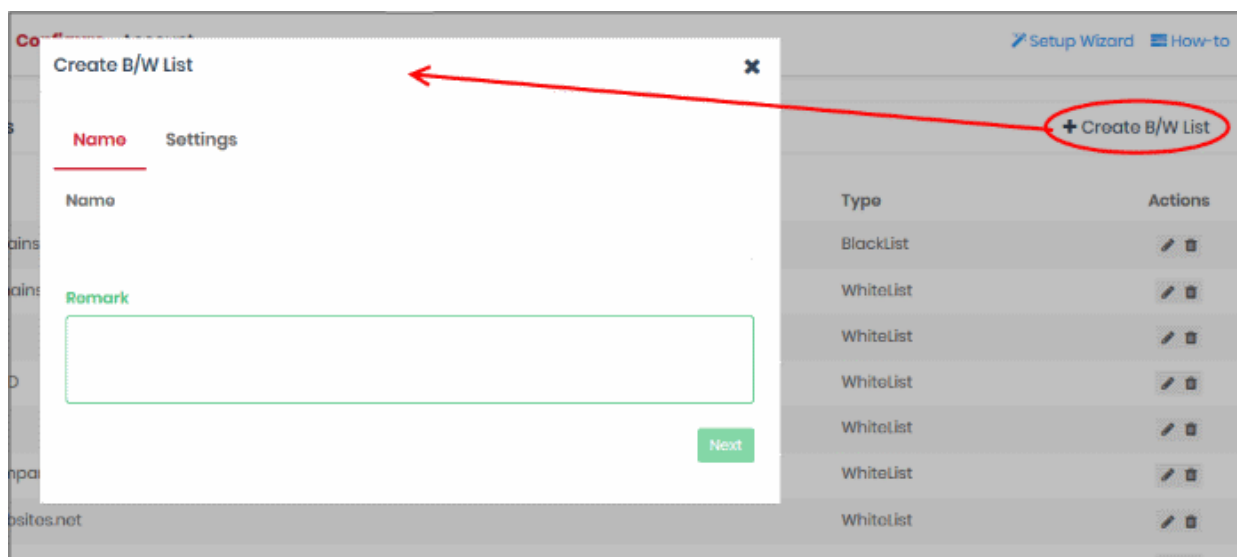
Domain B/W Lists - Table of Column Descriptions	
Column Header	Description
Rule Name	The label of the domain B/W list rule
Remark	Comments provided for the rule
Type	Indicates whether the rule is categorized as Whitelist or Blacklist
Actions	Controls to edit / delete the rule

The interface allows you to:

- **Create a new domain blacklist / whitelist**
- **Edit a domain blacklist / whitelist**
- **Delete a domain blacklist / whitelist**

Create a new domain blacklist / whitelist

- Click 'Configure' > 'Policy Settings' > 'B/W Lists'
- Click 'Create B/W List' at the top right



- Name and remarks - Create a label for the rule and add any comments. Ideally, these should help you and others identify the purpose of the rule.
- Click 'Next' or 'Settings' to add domains you want to blacklist or white-list.

Create B/W List ✕

Name **Settings**

If you want to whitelist/blacklist main domain and all of its subdomains, please add main domain to the list.
Example: "domain.com"

Whitelist Blacklist

Domains

Domain Name +

Please add at least one domain.

Select Country Domains

None ▾

Create

- Select 'Whitelist' or 'Blacklist'
- **Domains** - Enter the URL of the website without the 'http://' or 'https://' prefix. For example - www.example.com. Click '+' to add the domain to the rule. Repeat to add more domains.
- **Select Country Domains** - Add country code top-level domains (ccTLD) to the rule. The country TLD gets appended to the domain name you entered above. For example, if you enter amazon.com as the domain name and select 'Turkey', then CSIG adds amazon.com.tr to the rule. You can add multiple country domains.



Create B/W List ✕

Name **Settings**

If you want to whitelist/blacklist main domain and all of its subdomains, please add main domain to the list.
Example: "domain.com"

Whitelist Blacklist


Domains


amazon.com	
hdfcbank.co	

Domain Name +

Select Country Domains

▼

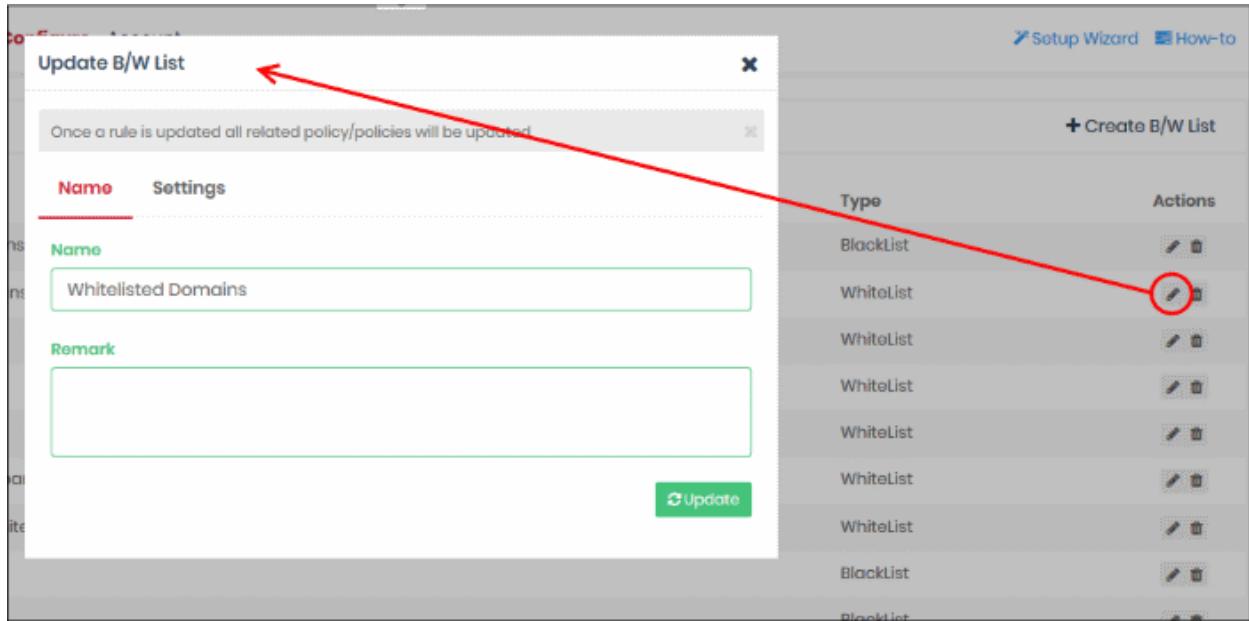
 Create

- To remove a domain name, click the trash can icon 
- Click the 'Create' button at the bottom of the dialog when finished.

The domains are added to B/W list and will be available for selection when **creating a policy**.

Edit a domain blacklist / whitelist

- To update a B/W list, click the edit  button beside the rule




The 'Update B/W List' dialog is similar to the create dialog explained **above**.

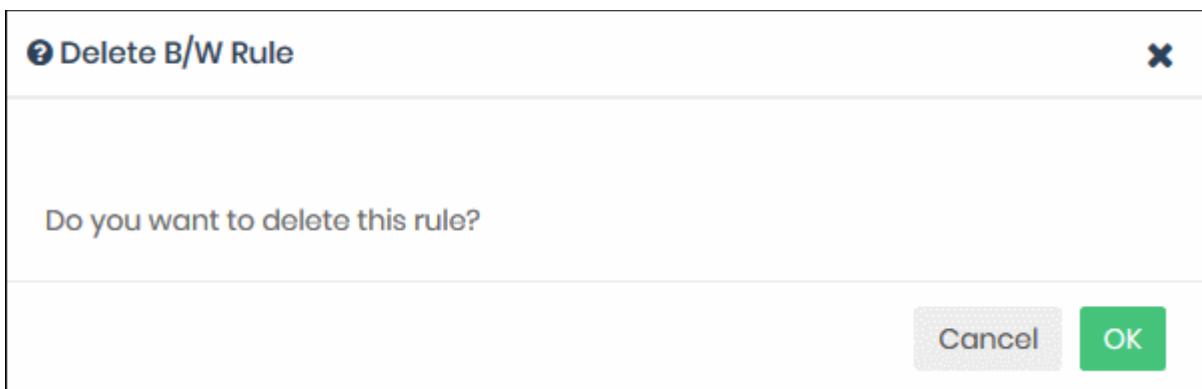
- Modify the name, description and/or domains in the B/W list as per your requirements.
- Click the 'Update' button.

Please note that the policy/policies containing the B/W list will also be updated according to the new settings and name.

Delete a domain blacklist / whitelist

Please note that you cannot delete a B/W list that is currently active in a policy. You have to disable the B/W list in all policies before deleting it.

- Click the trash can icon  beside a B/W list to delete it.
- Click 'Ok' in the confirmation box to remove the list

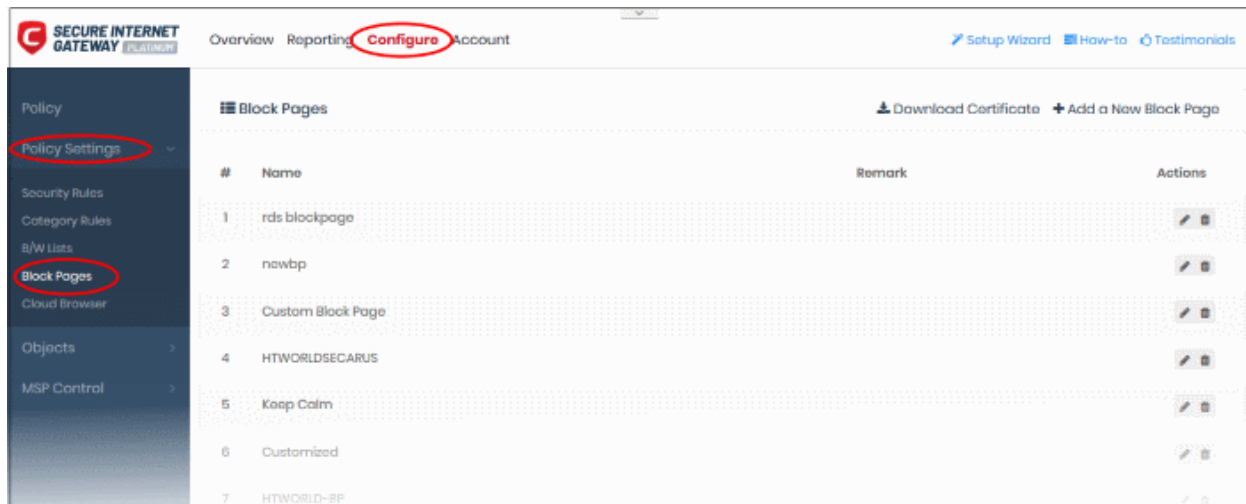


5.4 Manage Block Pages

- Click 'Configure' > 'Policy Settings' > 'Block Pages'

Block pages are shown to end-users when they attempt to visit a site that is banned by one of your policies. This includes users of endpoints in your protected networks, and all roaming endpoints.

- You can create any number of block pages and apply them to different policies.
- You can customize the content and behavior of block pages. The available options are:
 - Show the same block page for all types of rule violation
 - Show different block pages for category, security and blacklist rule violations
 - Display custom block messages with your custom banners
 - Redirect users to a specific web-page
- You need to install the Secure Internet Gateway SSL certificate on all protected endpoints. This so the block page displays correctly over HTTPS connections.



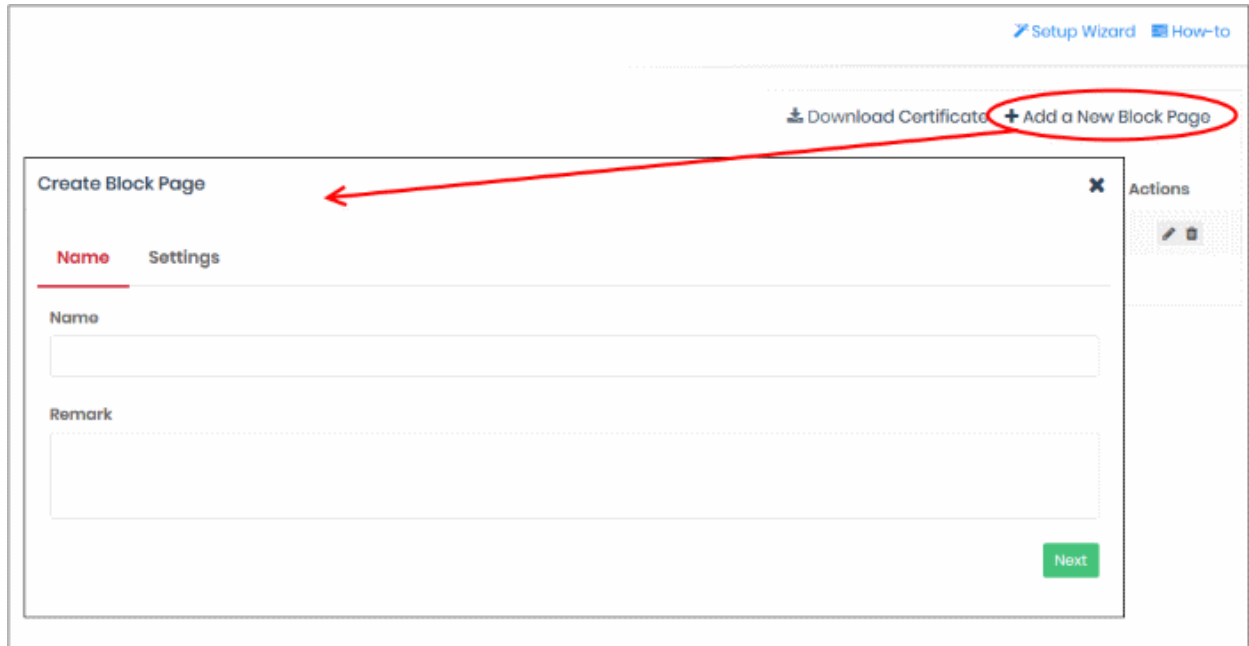
Block Pages - Table of Column Descriptions	
Column Header	Description
Name	Label of the block page
Remark	Comments provided for the page. The name and remark should identify the purpose of the page.
Actions	Controls to edit / delete the block page

The following sections explain how to:

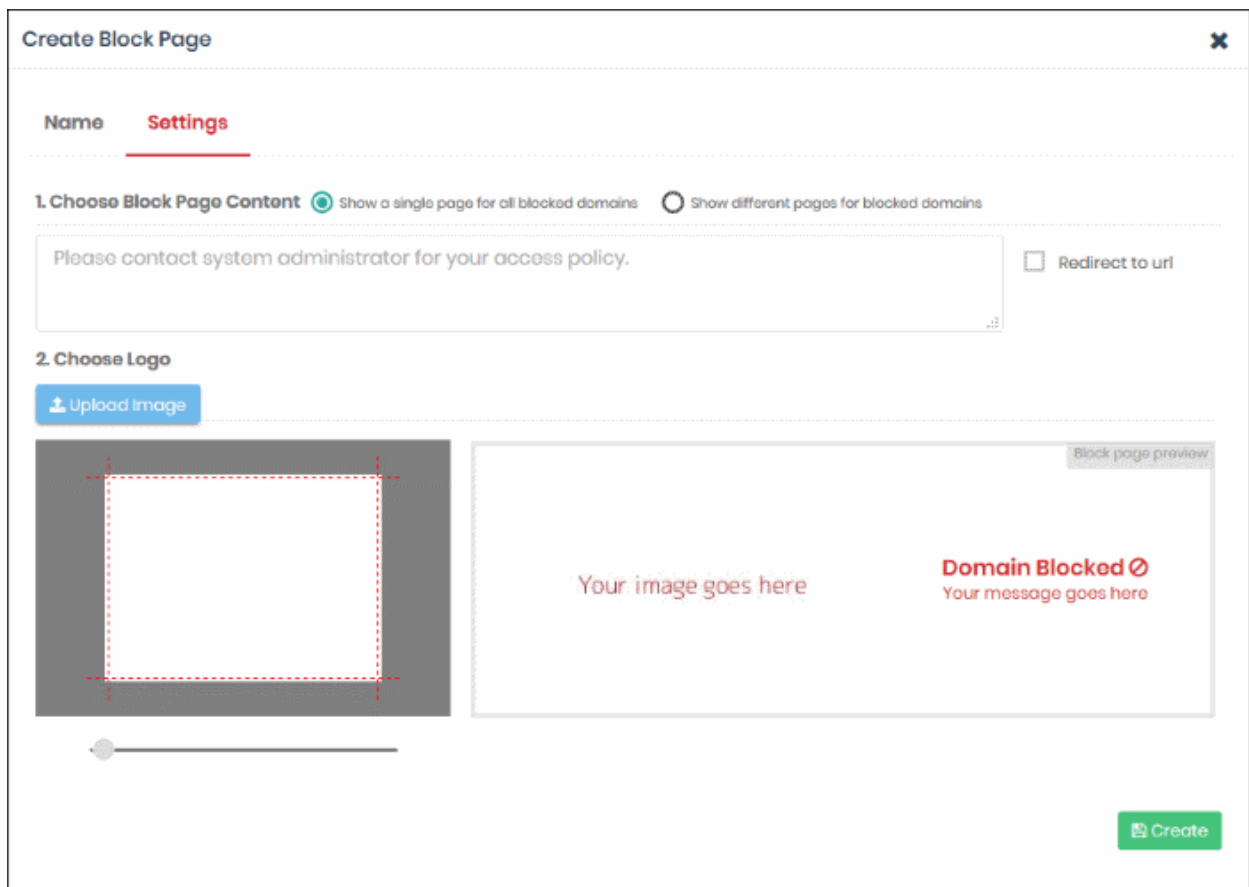
- **Create a new block page**
- **Install an SSL certificate for block pages**
- **Edit a block page**
- **Delete a block page**

Create a Block Page

- Click 'Configure' > 'Policy Settings' > 'Block Pages'
- Click 'Add a New Block Page' at top-right



- Name - Enter a descriptive label for the block page
- Remark - Type internal notes/comments about the page if required. Text you enter here will not be shown in the block page itself.
- Click 'Next' or 'Settings' to configure the block page

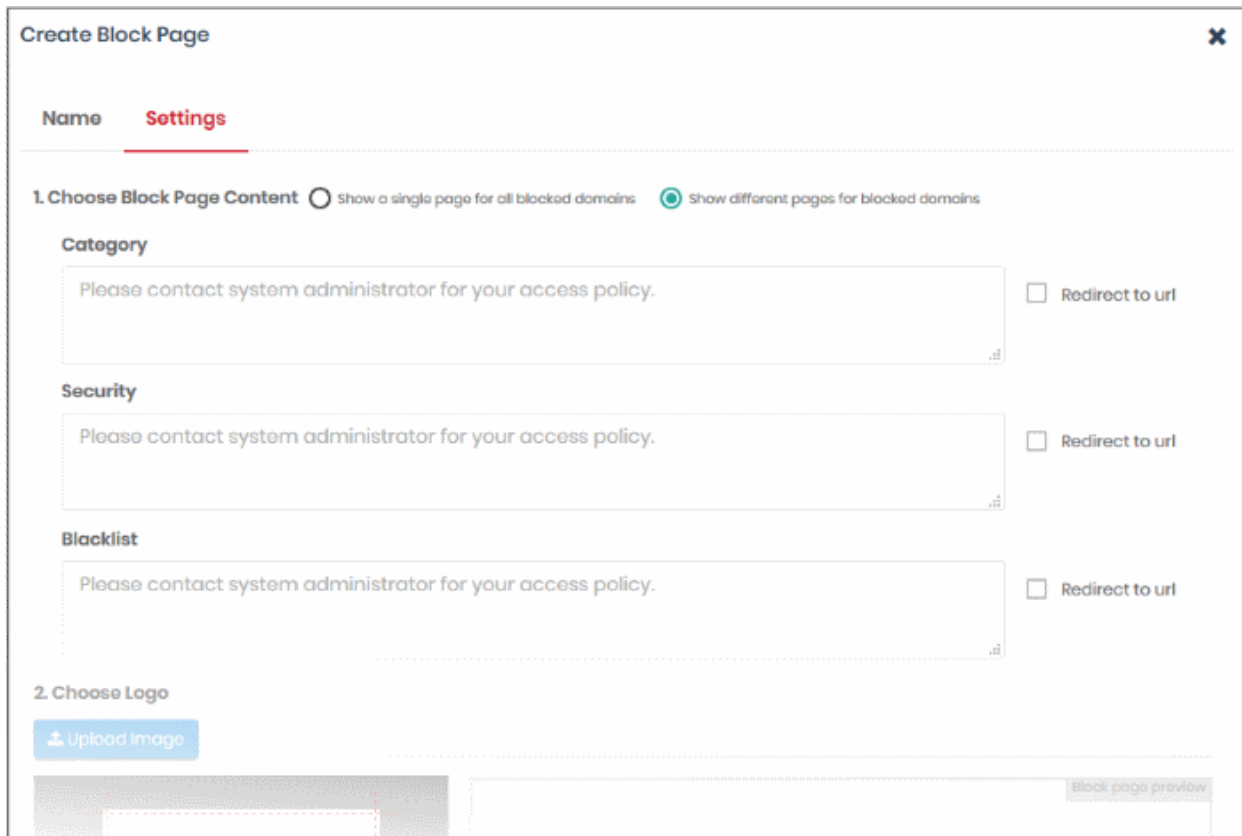


You now need to create your block page content and upload your logo:

Step 1 - Configure Block Page Content

First, choose whether to show a single block page or different block pages:

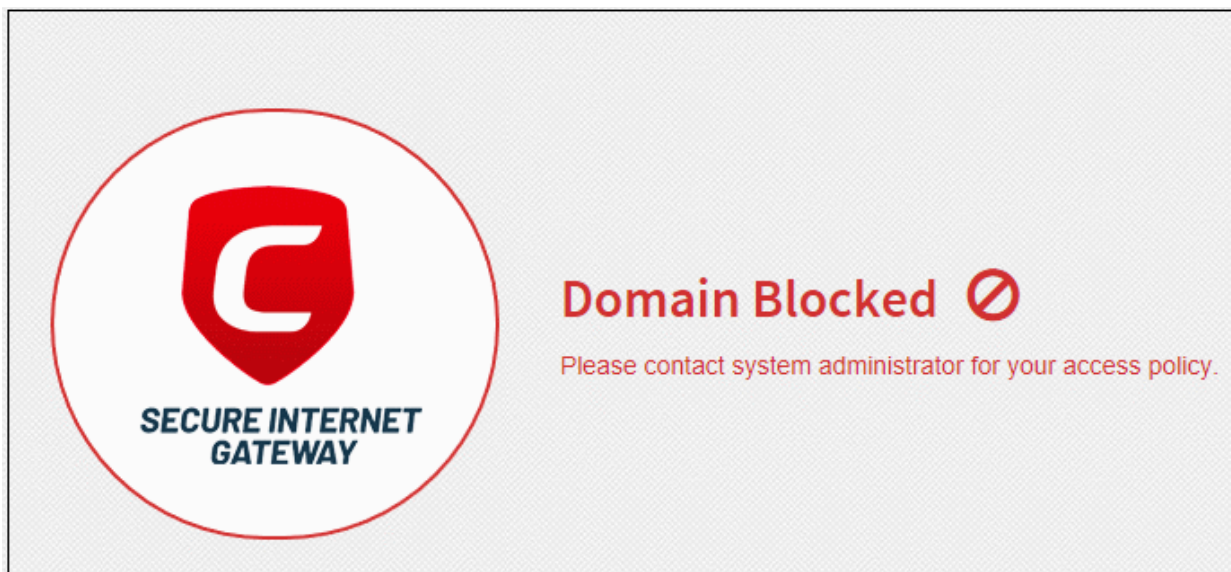
- **Show a single page for all blocked domains** - The same block page is shown regardless of the type of rule violated.
- **Show different pages for blocked domains** - Show specific block pages when a certain type of rule is violated. You can show different pages for category rule breaches, security rule breaches and blacklist rule breaches:



- You can type a custom message for each page if required.
- Alternatively, you can use the default message of 'Please contact your system administrator for your access policy'
- You also have the option to redirect to a different URL instead. Please specify the full URL if you use this option. For example, <https://www.example.com/security-redirect-page.php>.

Step 2 - Upload Your Logo

- The interface shows the Secure Internet Gateway logo on the block page by default.
- You can change this to your own company logo by uploading a suitable .png or .svg file



- Click 'Upload Image' under 'Choose Logo'. Browse to the location of your image and click 'Open'

Please contact system administrator for your access policy. Redirect to url

2. Choose Logo

Upload Image

Your image goes here

Block page preview

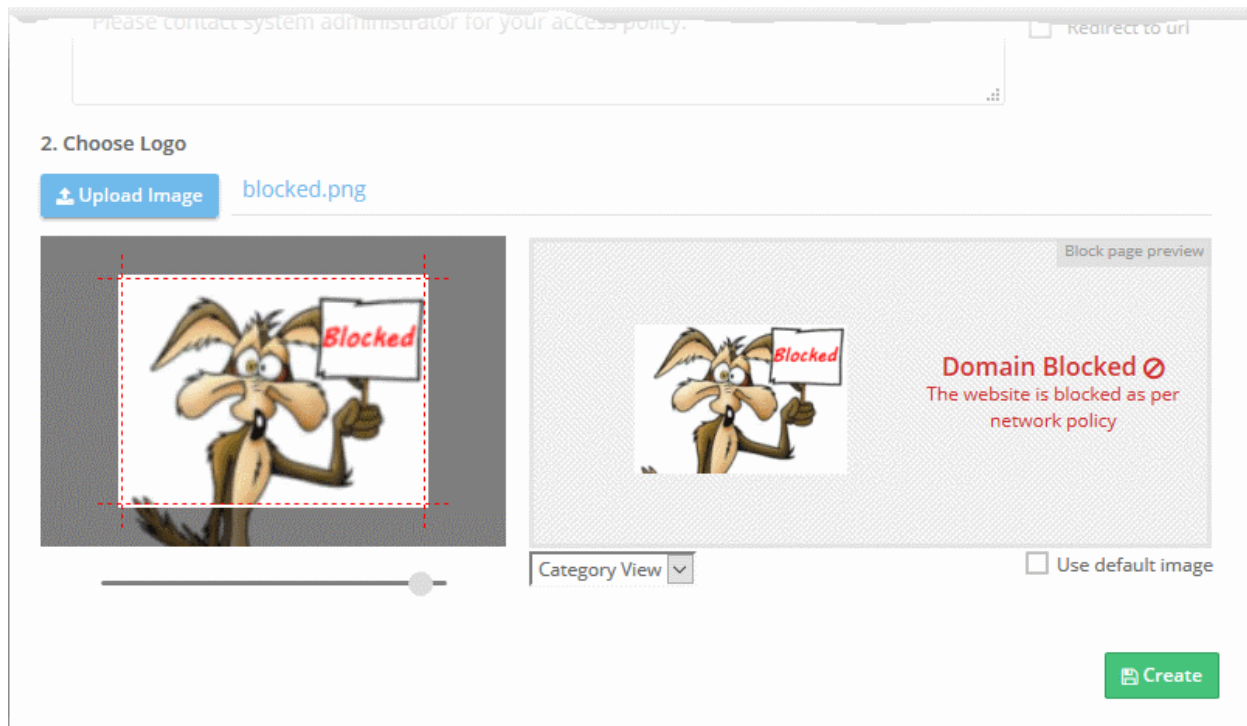
Domain Blocked

Your message goes here

Category View

Note: Max. file size = 50 kb. Images must be in .png or .svg format

Your image appears on the left:



- Use the slider below the image to enlarge or reduce the image. Position the image within the red border as desired.

A preview of your block page appears on the right.

- Use the drop-down below the preview to view your block pages for security, category and blacklist rules.
- 'Use default image' - The Secure Internet Gateway logo is shown as the block page.
- Click 'Create'

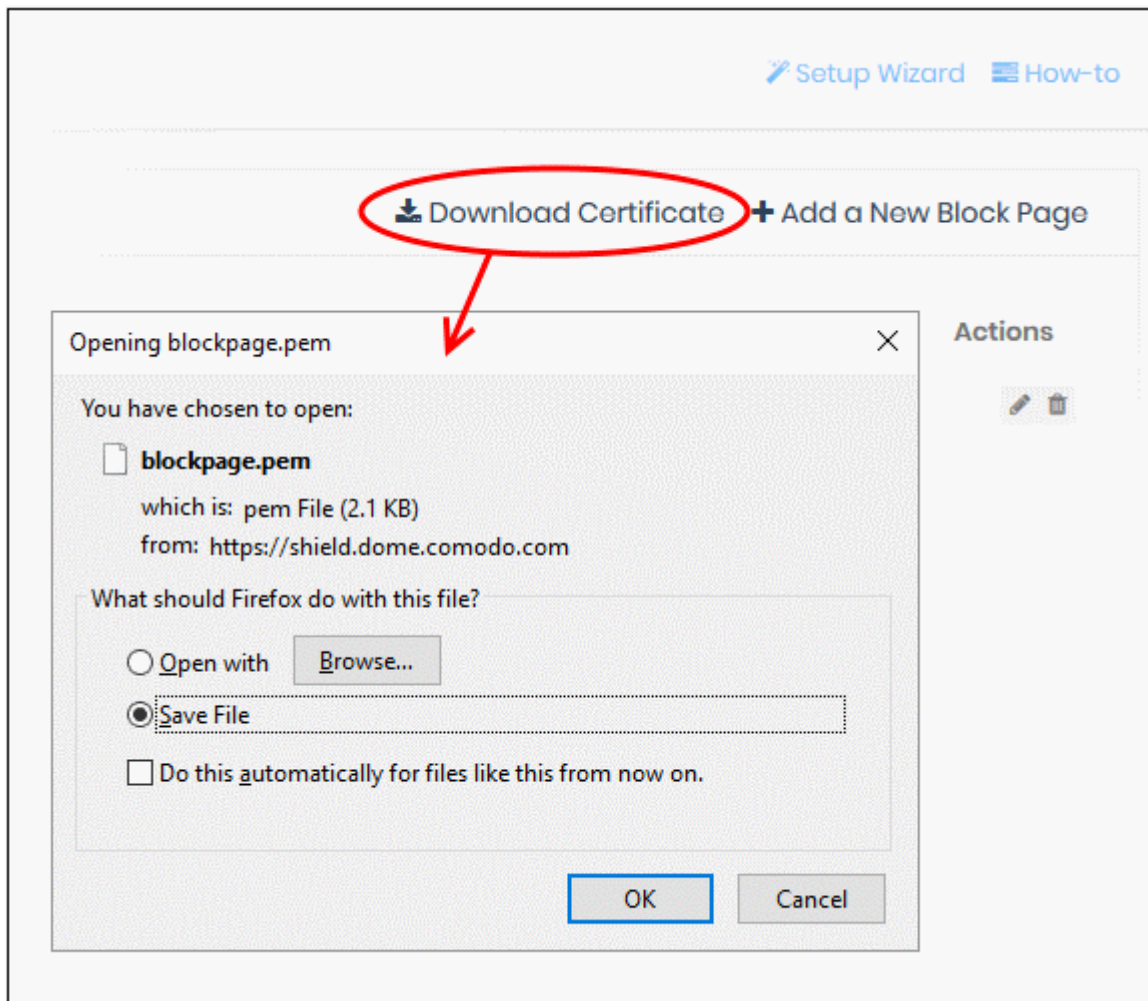
The new block page is available for selection when **creating a policy**.

Install SSL certificate for block pages

- Endpoint browsers may show an error message when some HTTPS pages are blocked by Secure Internet Gateway.
- You can avoid these errors by installing the CSIG SSL certificate on all protected endpoints.

Download and install the certificate

- Click 'Configure' > 'Policy Settings' > 'Block Pages'
- Click 'Download Certificate' at top-right



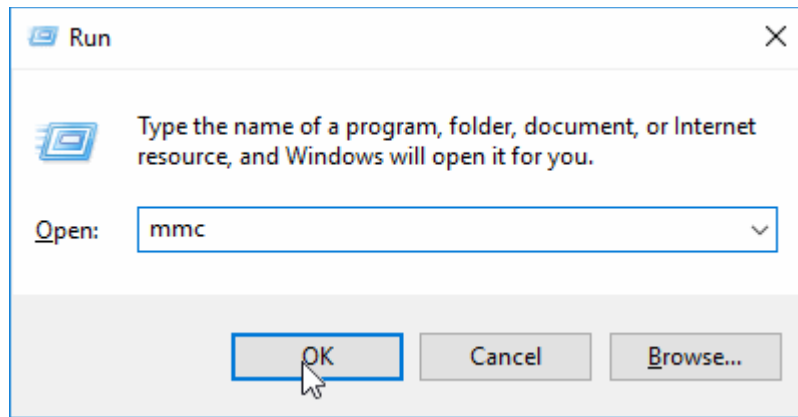
The certificate is downloaded in .pem format.

There are two steps to install the certificate on endpoints:

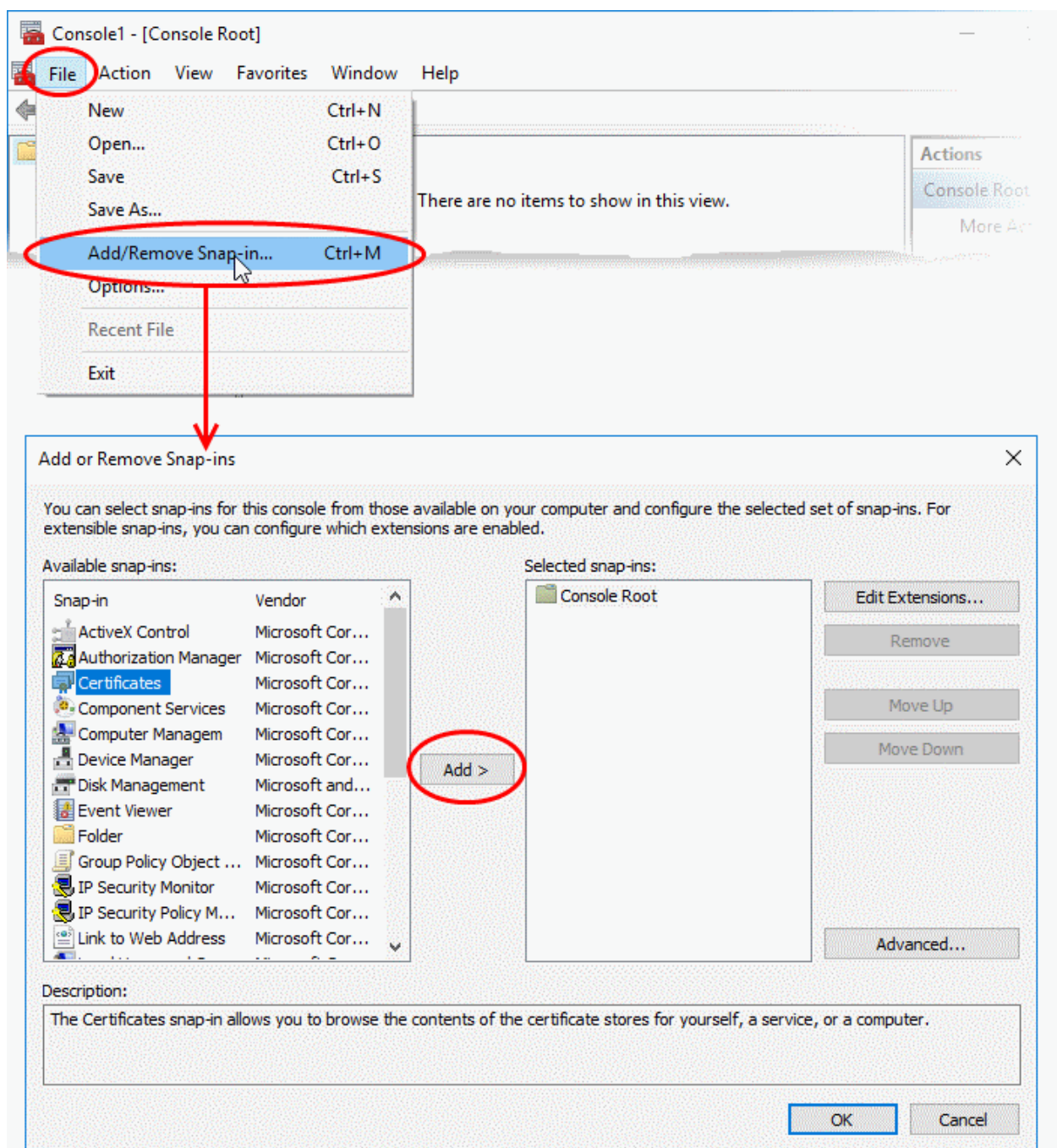
- **Step 1 - Add the 'Certificates' snap-in to Microsoft Management Console (MMC)** (if not already done)
- **Step 2 - Import the certificate to the trust certificate store**

Step 1 - Add 'Certificates' snap-in to Microsoft Management Console (MMC)

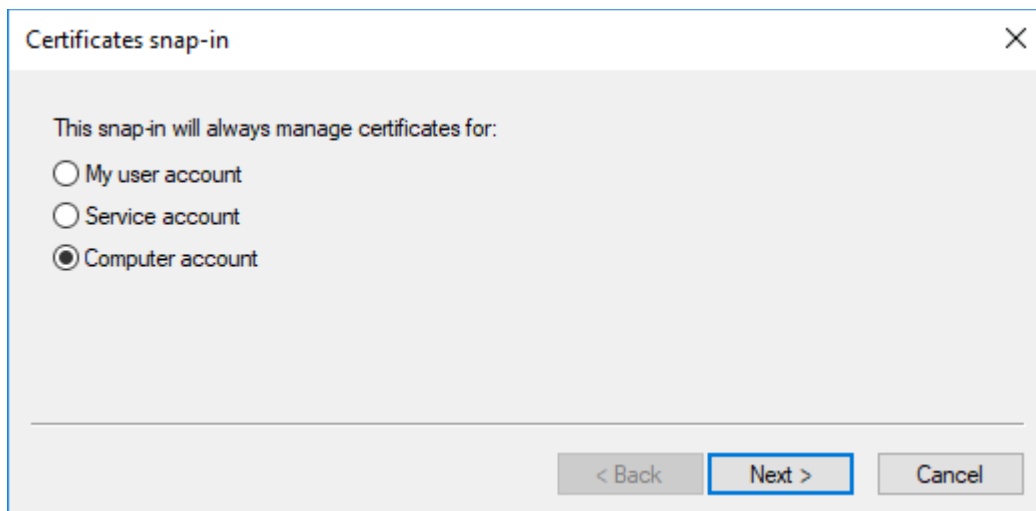
- Open the 'Run' dialog (Win' key + 'R')
- Type 'mmc' in the 'Run' dialog:



- Click 'File' > 'Add/Remove snap-in' in the console interface
- Select 'Certificates' in the list on the left. Click 'Add' to move it to the list of selected snap-ins.

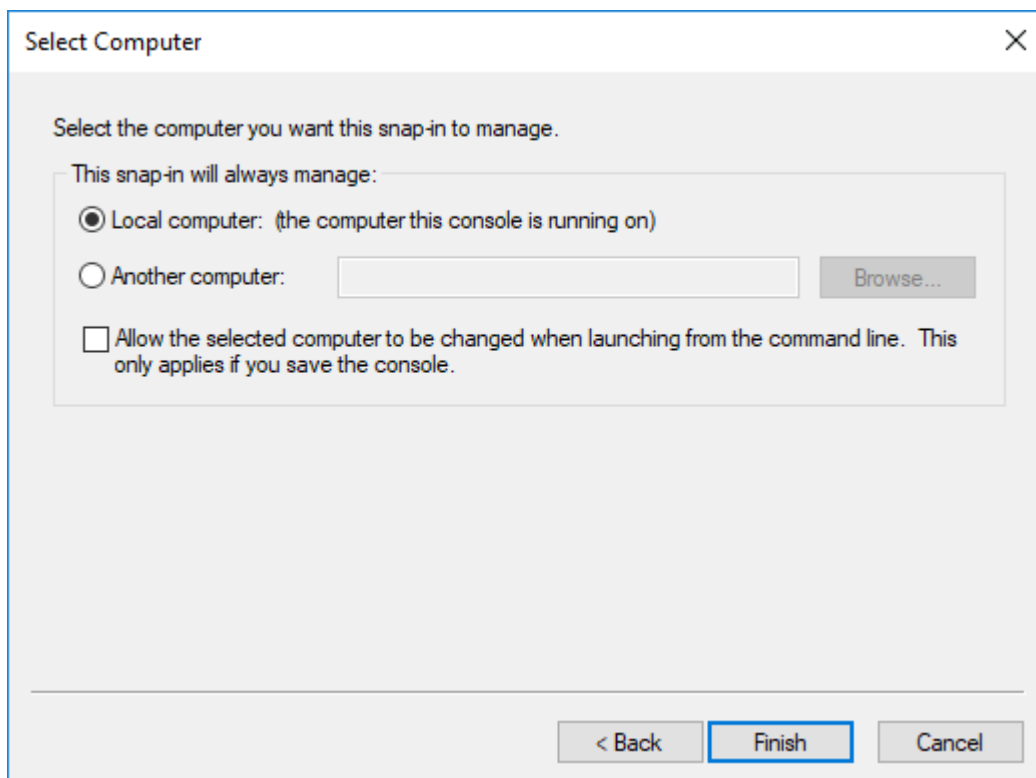


- You will be asked to select the computer and account to which the snap-in should be added:



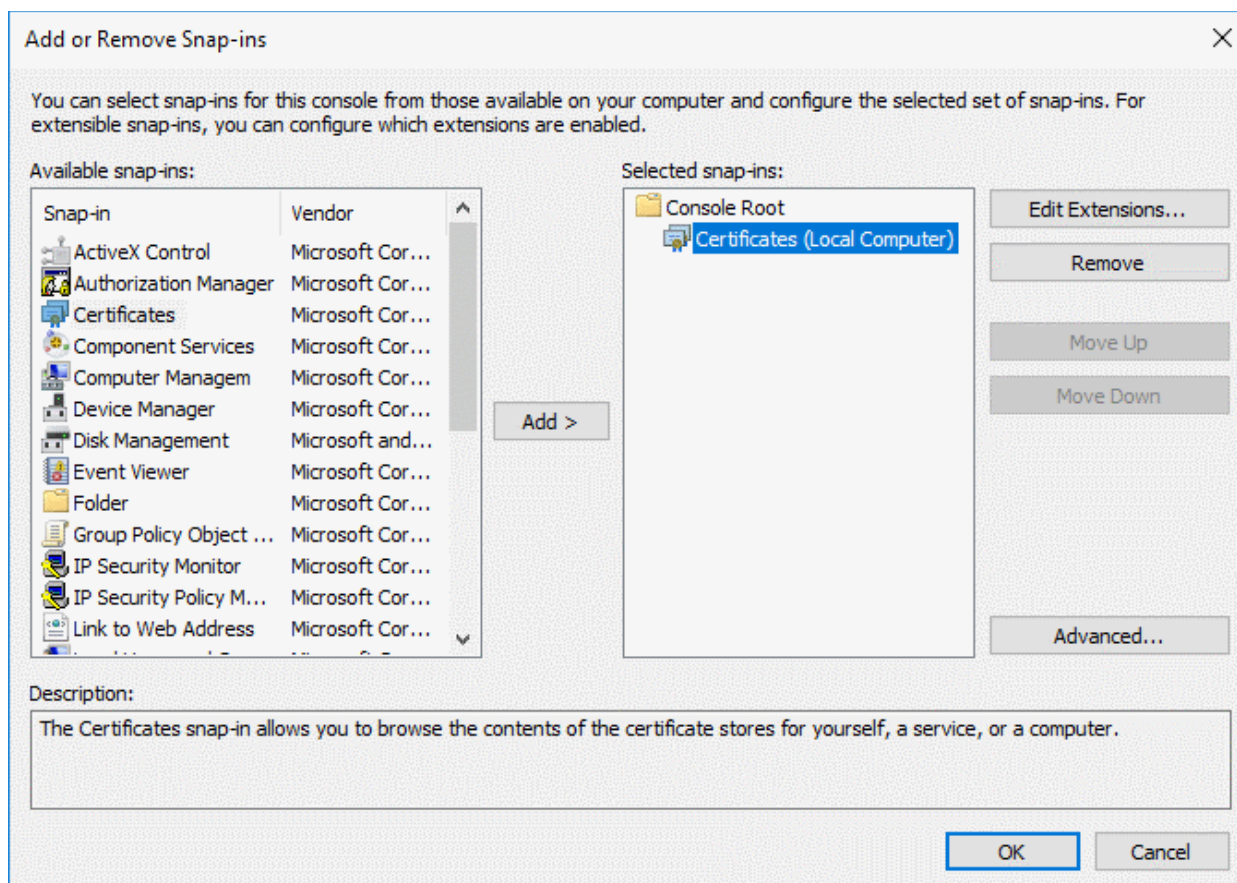
The 'Certificates snap-in' dialog box has a title bar with a close button (X). The main content area contains the text 'This snap-in will always manage certificates for:' followed by three radio button options: 'My user account', 'Service account', and 'Computer account'. The 'Computer account' option is selected. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

- Select 'Computer account' and click 'Next'
- Select 'Local computer' and click 'Finish':



The 'Select Computer' dialog box has a title bar with a close button (X). The main content area contains the text 'Select the computer you want this snap-in to manage.' followed by 'This snap-in will always manage:'. Below this are three options: 'Local computer: (the computer this console is running on)' with a selected radio button, 'Another computer:' with an empty text box and a 'Browse...' button, and a checkbox labeled 'Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.' At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'. The 'Finish' button is highlighted with a blue border.

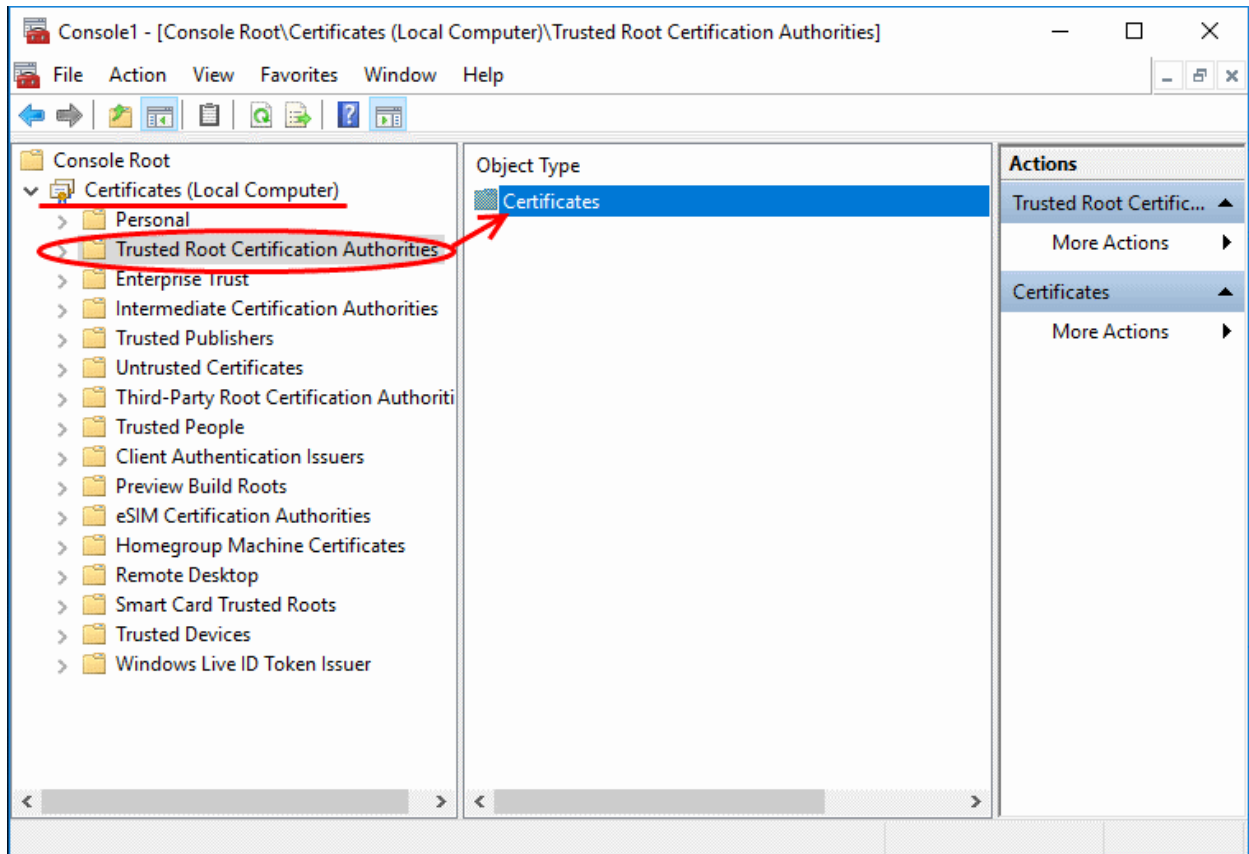
- The snap-in will be added to the list on the right



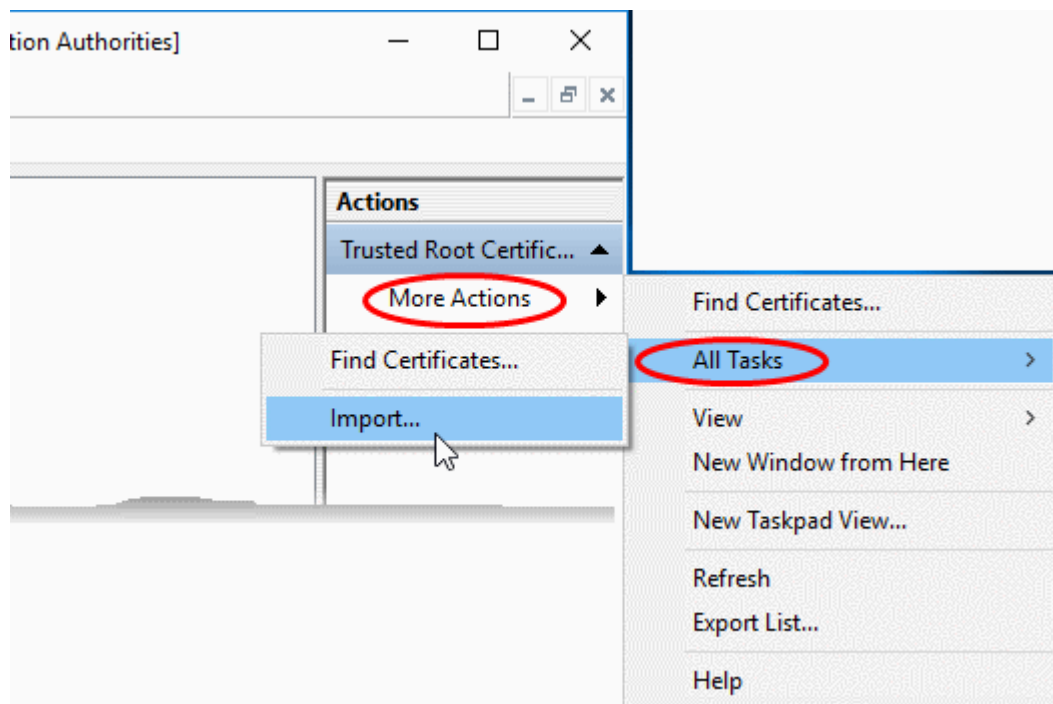
- Click 'OK' to add the snap-in to the console.
- Leave the console open. You will need it for step 2...

Step 2 - Import the certificate to the trusted certificate store

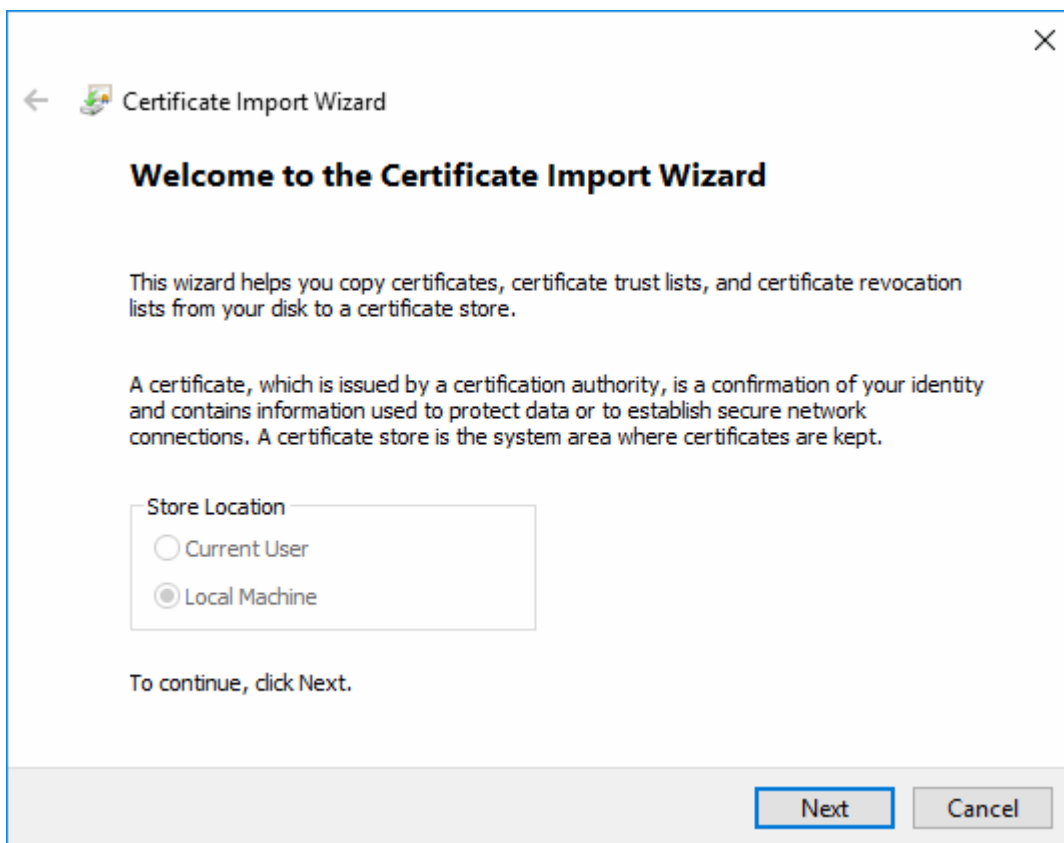
- Expand the 'Certificates (Local Computer)' tree on the left of the MMC console
- Select 'Trusted Root Certification Authorities':



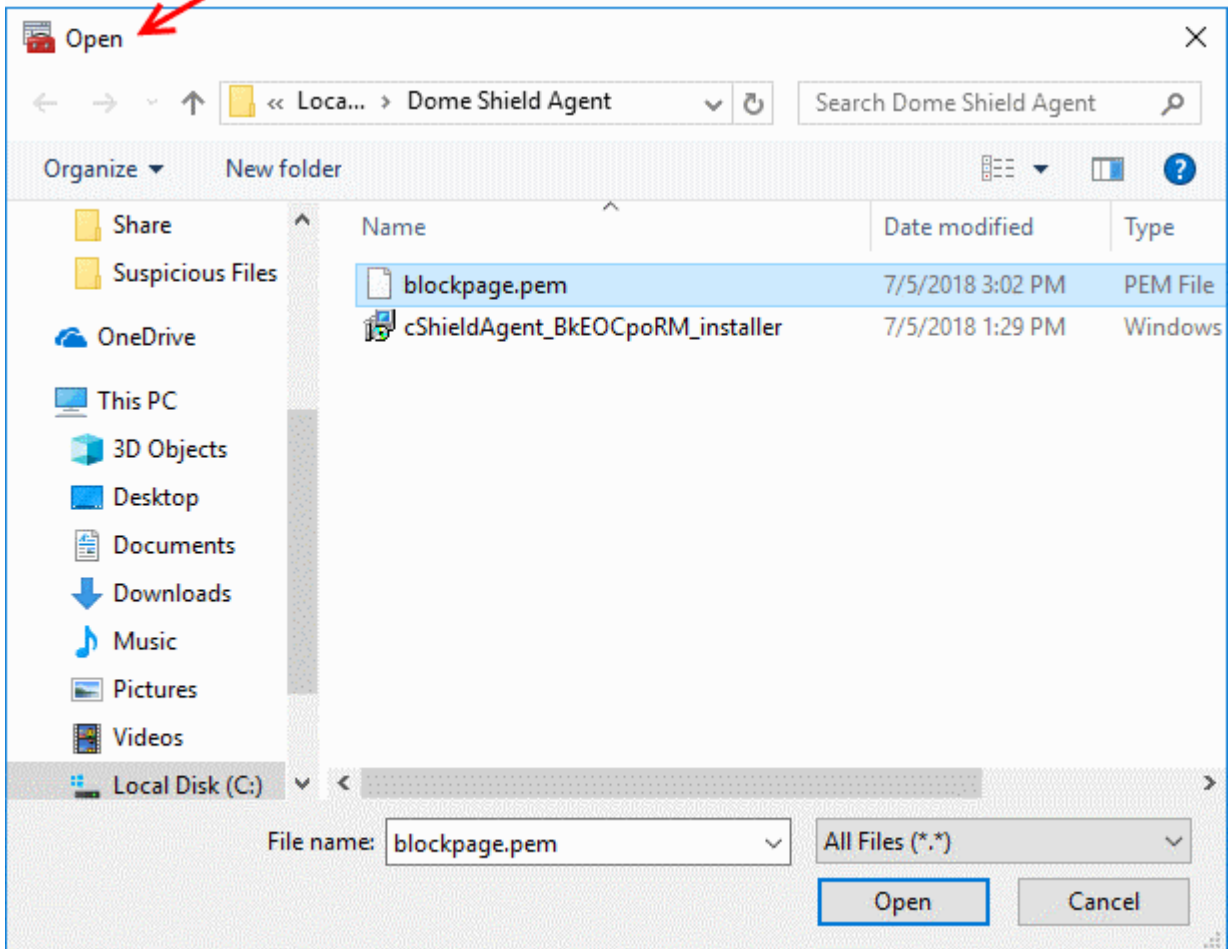
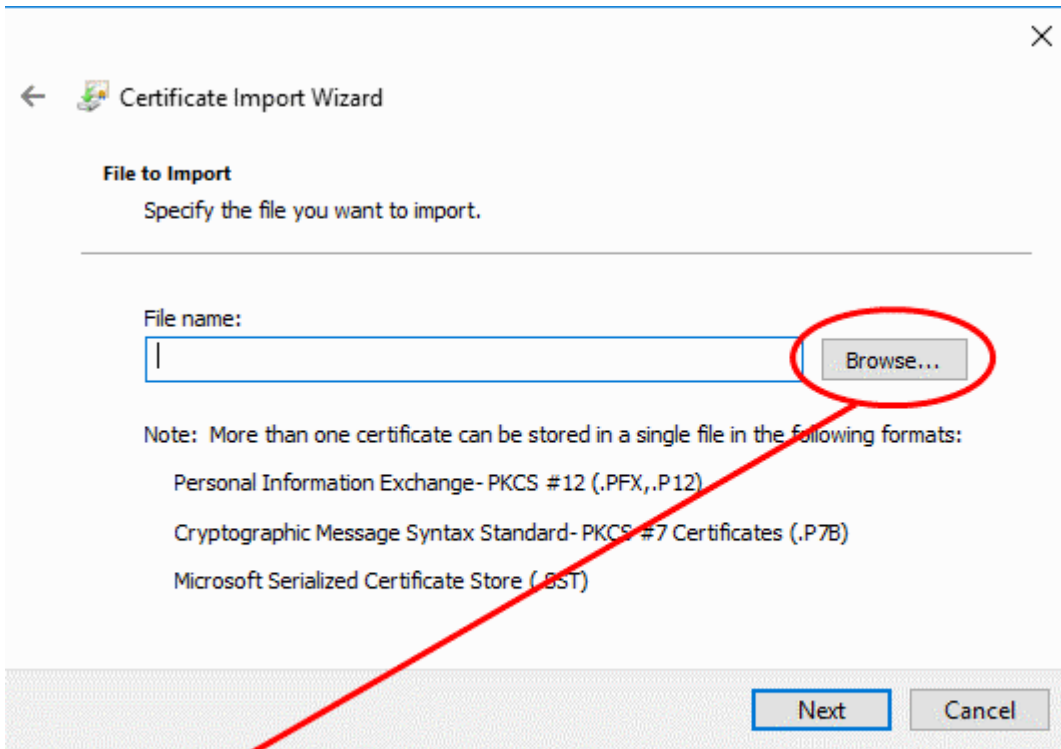
- Click 'More Actions' > 'All Tasks' > 'Import', on the right:



The certificate import wizard will start:

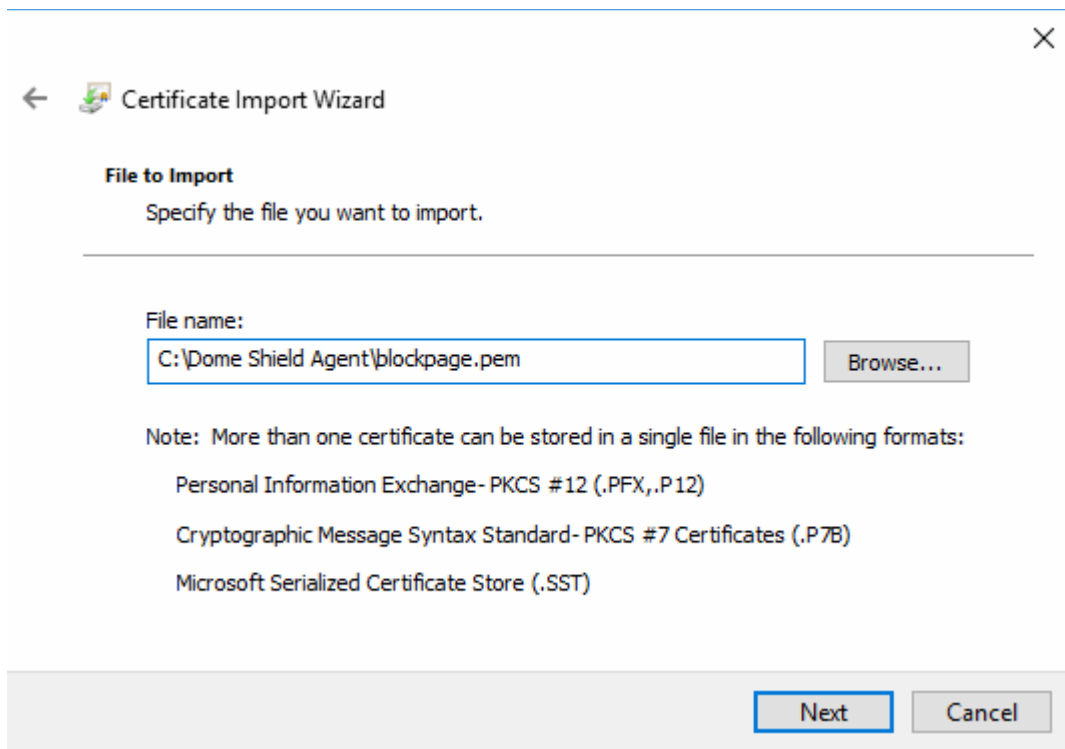


- Click 'Next' to open the certificate selection screen
- Click 'Browse', navigate to the location of the certificate and select 'blockpage.pem':

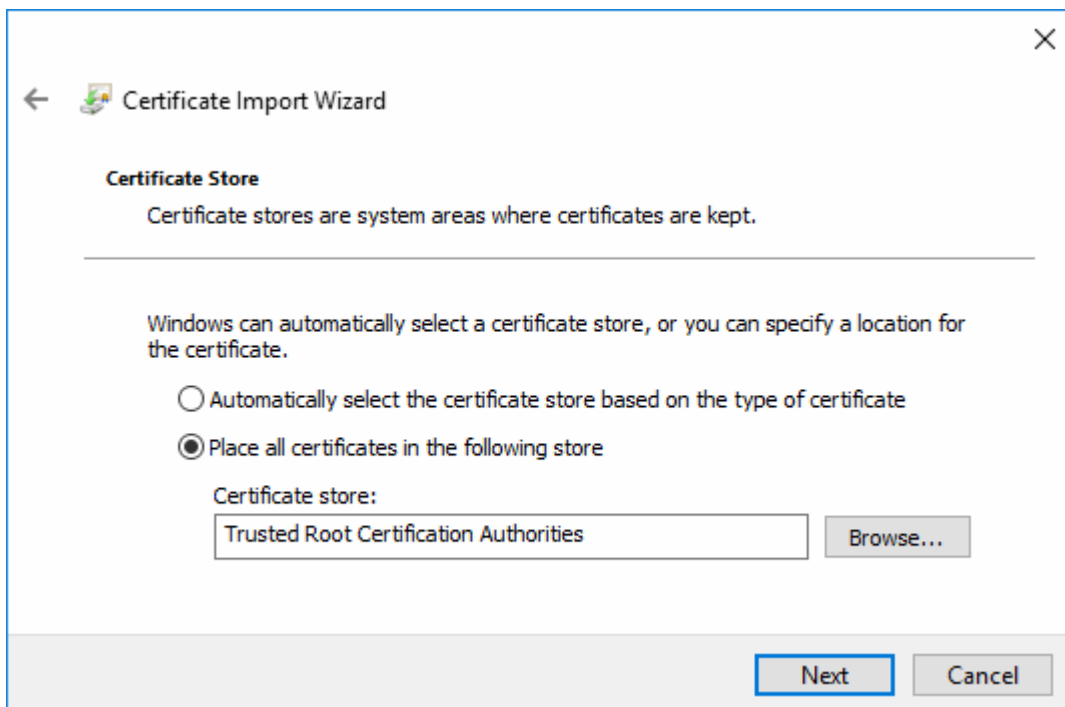


Tip: If the .pem file is not showing, select 'All Files' as the file type.

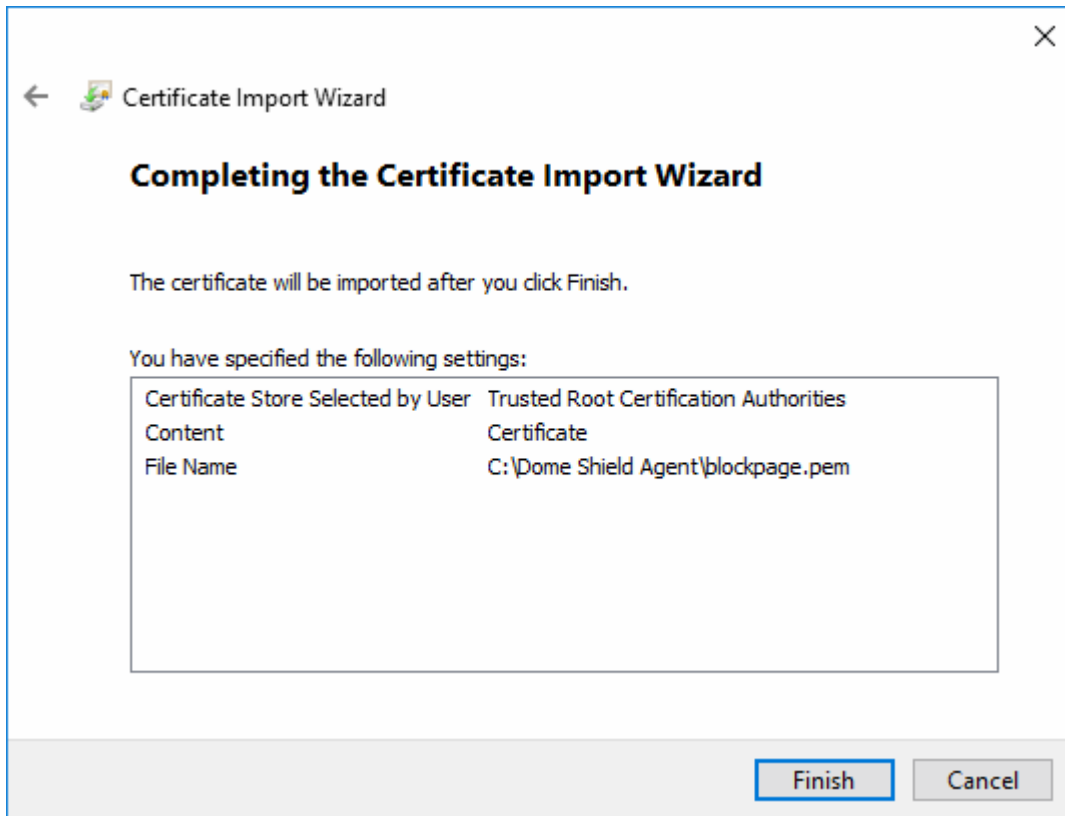
- Click 'Open'



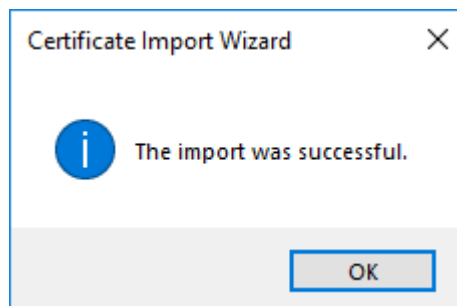
- Click 'Next'.
- The next step is to choose the certificate store.



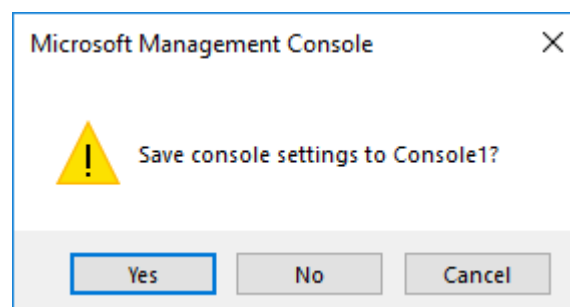
- Confirm that the 'Trusted Root Certification Authorities' store is pre-selected and click 'Next'



- Click 'Finish' to import the certificate.



- Click 'OK' to exit the wizard.



- Click 'Yes' in the console close dialog to save your changes.

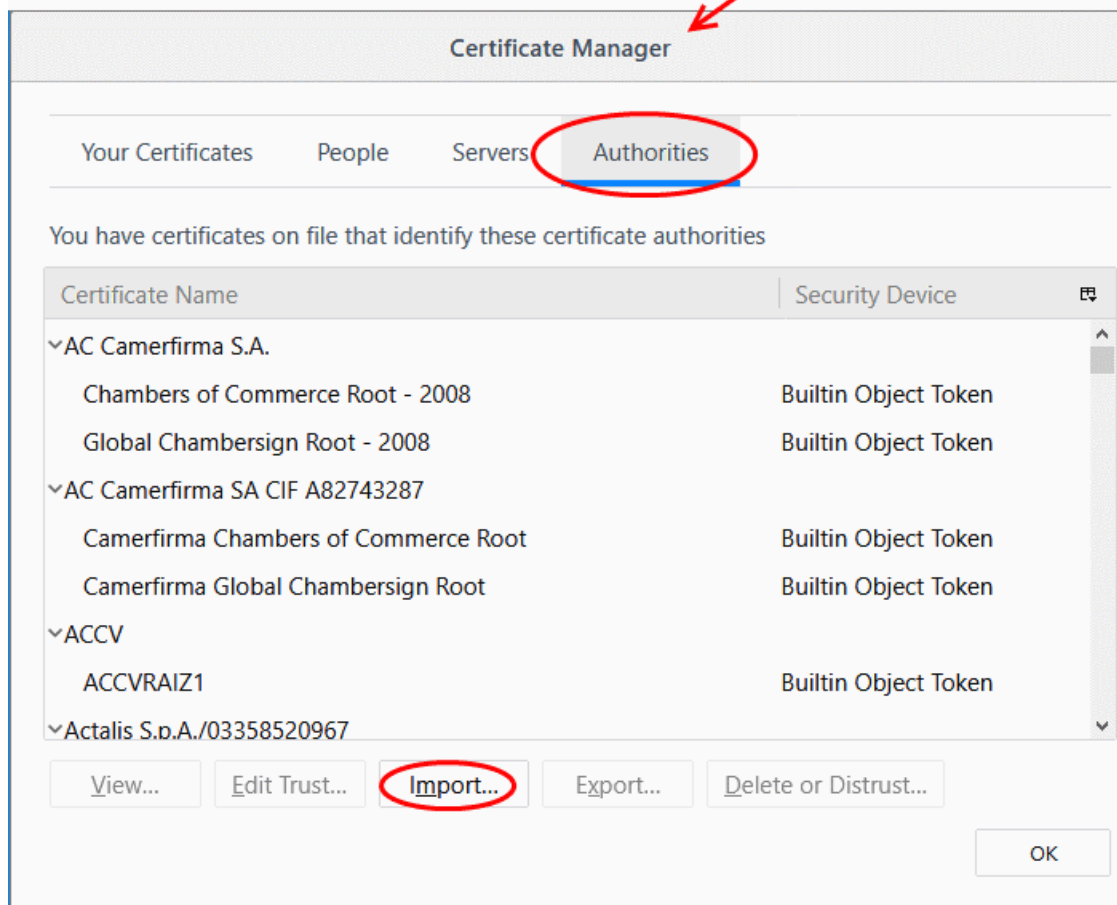
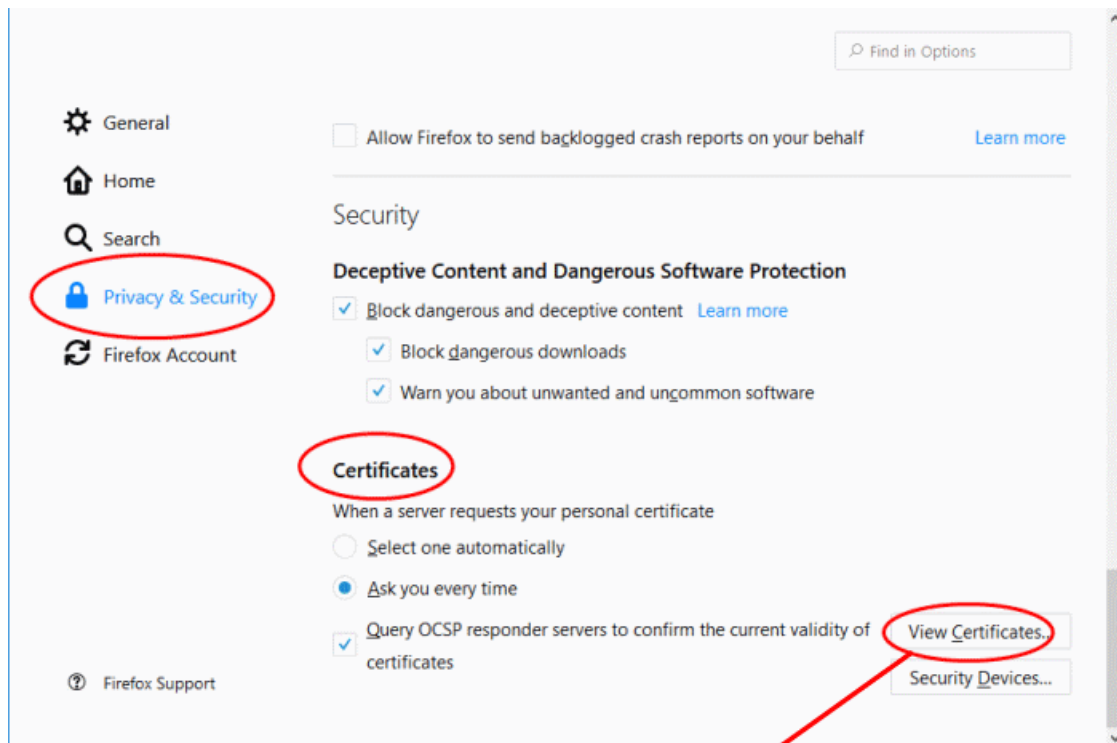
Mozilla Firefox users

- Firefox uses its own certificate store, instead of the Windows store used by Internet Explorer, Edge and Chrome.
- You need to import the certificate to the Firefox store if you want your block page shown in Firefox.

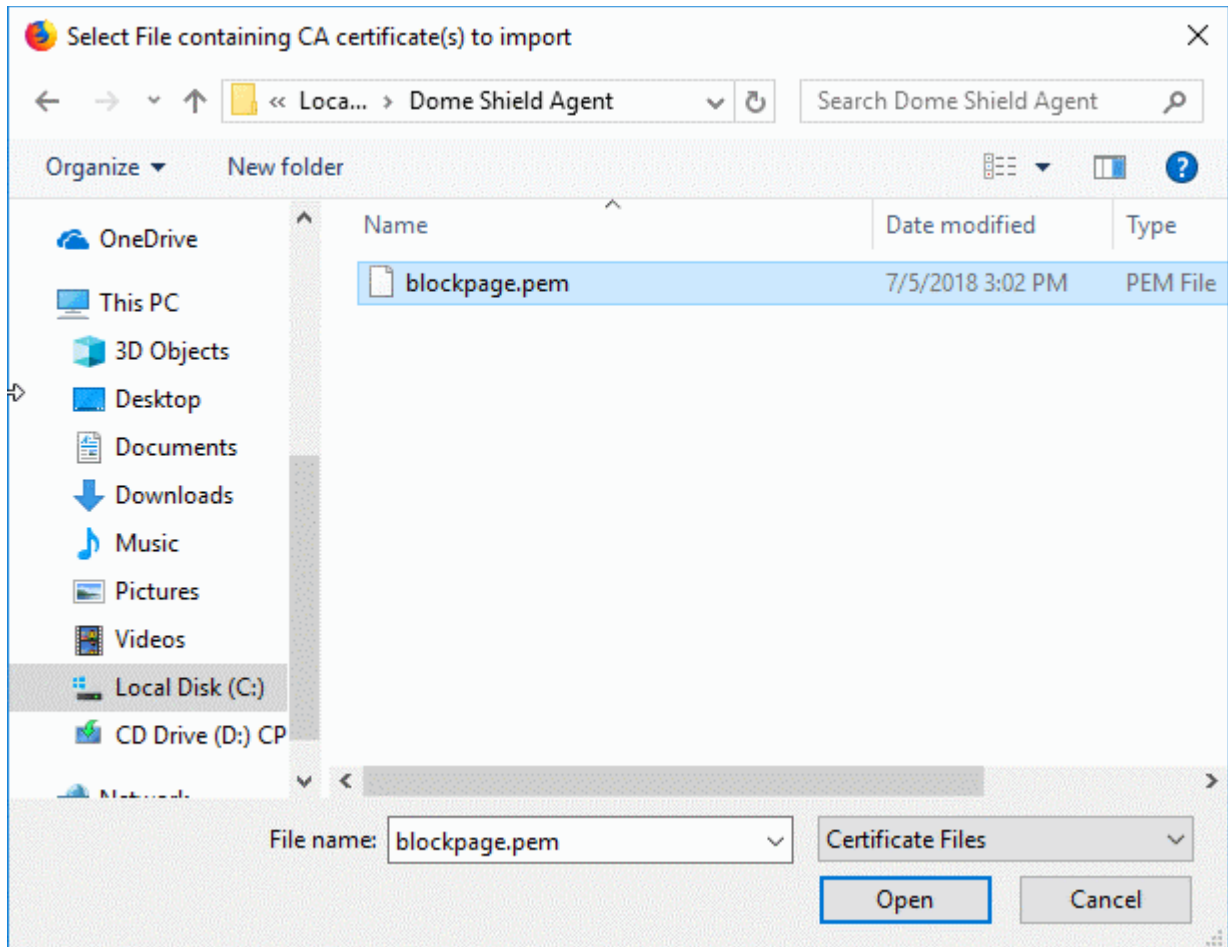
Import the certificate to Firefox certificate store

- Open Firefox

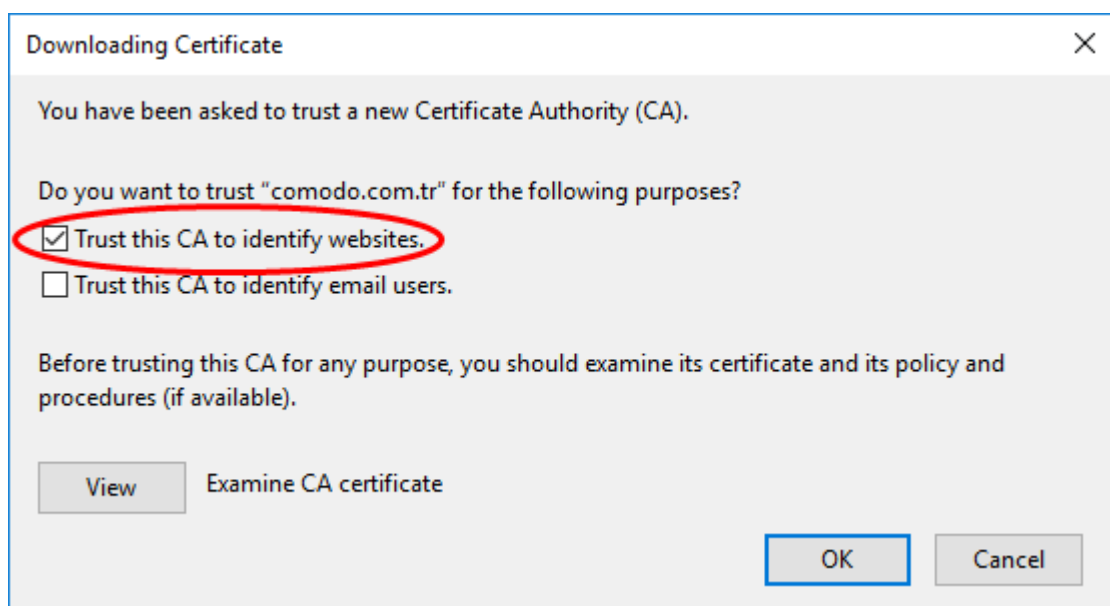
- Click the hamburger icon at top-right and choose 'Options'
- Click 'Privacy & Security' on the left then scroll down to the 'Certificates' area
- Click 'View Certificates' to open the certificate store:



- Select the 'Authorities' tab
- Click 'Import'

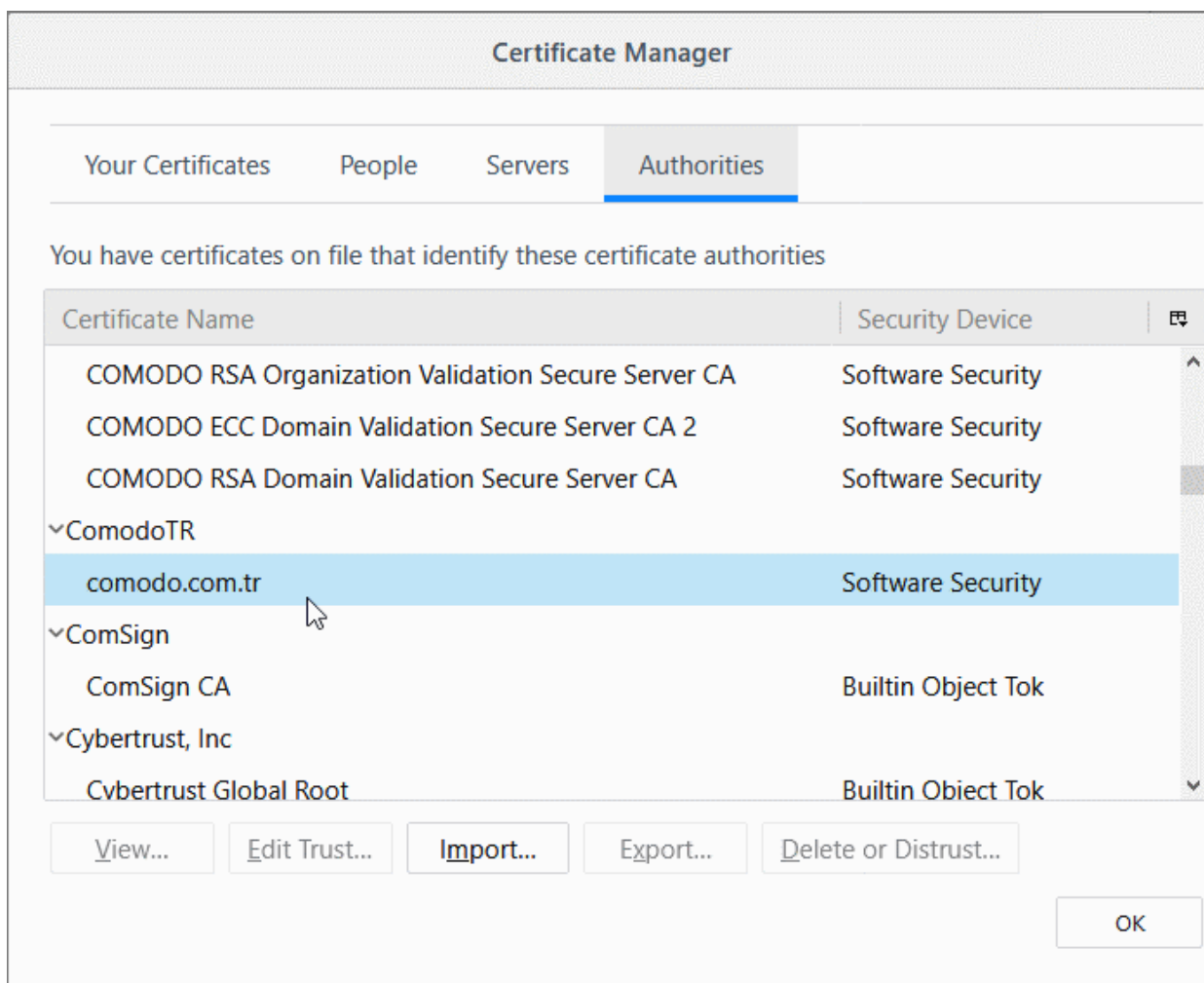


- Browse to and select 'blockpage.pem' then click 'Open'.



- Select 'Trust this CA to identify websites' and click 'OK'

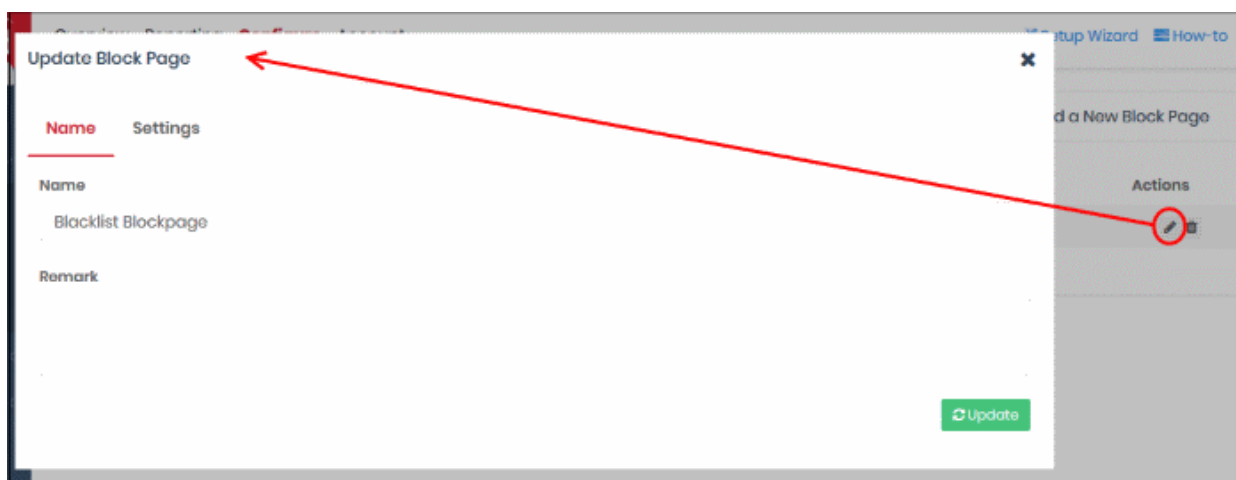
The certificate will be imported to the Firefox store:



- Click 'OK' to save your changes.

Edit a Block Page

- To update a block page, click the edit  button beside the page in the list



The 'Update Block Page' dialog will appear. The dialog is similar to 'Create Block Page' dialog explained **above**.


- Modify the name, description and/or block page settings, messages as per your requirements.
- Click the 'Update' button

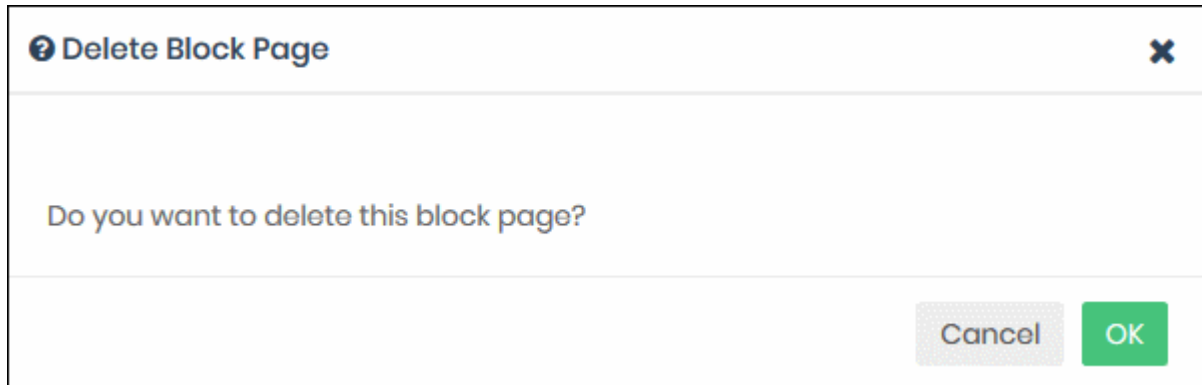
Please note that the policy/policies containing the block page will also be updated according to the new settings and

name.

Delete a category rule

You cannot delete a block page that is currently active in a policy. You have to remove the block page from all policies before deleting it from the list.

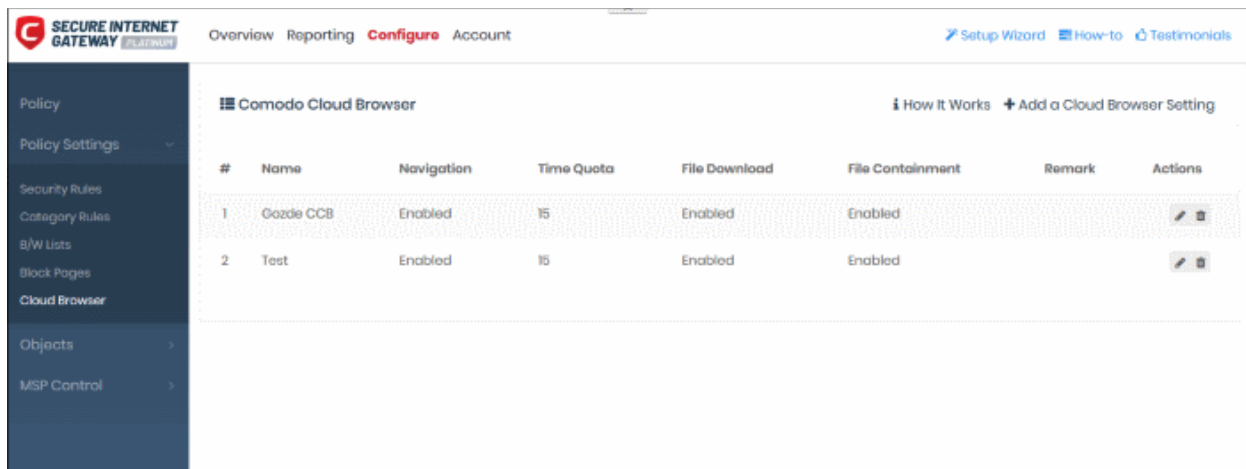
- Click the trash can icon  beside a rule to delete it.
- Click 'OK' to confirm the removal:







5.5 Manage Cloud Browser Settings

Click 'Configure' > 'Policy Settings' > 'Cloud Browser'

- The cloud browser feature lets you specify that sites blocked by a **security rule** are instead opened inside a virtual environment.
- Virtual browsing sessions are isolated from the host operating system, so any malware downloaded cannot infect the device and/or the network.
- You can choose to open all sites from the security category in the virtual environment, or pick specific sub-categories. For example, you might want to outright block sites in the 'Malware' category, but grant virtual access to sites in the 'Bitcoin related' category.



#	Name	Navigation	Time Quota	File Download	File Containment	Remark	Actions
1	Gozde CCB	Enabled	15	Enabled	Enabled		 
2	Test	Enabled	15	Enabled	Enabled		 

Comodo Cloud Browser - Table of Column Descriptions

Column Header	Description
Name	The label of the virtual session rule. This is shown in policy settings for you to select.

Navigation	Specify whether users can visit other sites besides the one that triggered the virtual session (the initial URL) <ul style="list-style-type: none"> • Disabled - Users can only visit websites that are specified in the security rule on their policy. They cannot change the URL or visit sub-domains. • Enabled - Users can visit sites in the security category and any sub-domains of those sites. Users cannot change the URL or visit other domains.
Time Quota	How long the virtual session remains open. The session will automatically end after this time period.
File Download	Specify whether users can save files from virtual sessions. <ul style="list-style-type: none"> • Disabled - Users cannot download files from websites in virtual sessions • Enabled - Users are allowed to save files in virtual sessions. To protect your devices and networks, enable file containment described below.
File Containment	Enabled - CSIG will scan downloaded files for viruses and other threats. Only known-safe files are allowed to run on the host machine. Unknown and malicious files are run in the container (sandboxed).
Remark	Comments about the virtual session rule
Actions	Lets you update or delete a virtual session rule

The following sections describe how to:

- **Create a new cloud browser rule**
- **Edit a cloud browser rule**
- **Delete a cloud browser rule**

Create a new cloud browser rule

- Click 'Configure' > 'Policy Settings' > 'Cloud Browser'
- Click 'Add a Cloud Browser Setting' at top-right

The screenshot shows the 'Comodo Cloud Browser' configuration page. At the top right, there is a button labeled '+ Add a Cloud Browser Setting' which is circled in red. A red arrow points from this button to a modal window titled 'Create - Comodo Cloud Browser'. The modal window contains a table with columns for '#', 'Name', and 'Settings'. Below the table, there are two input fields: 'Name' and 'Remark'. At the bottom right of the modal, there is a green 'Next' button.

- Name and remark - Create a label for the rule and add any comments. Ideally, these should help you and

others identify the purpose of the rule.

- Click 'Next' or 'Settings' to configure a virtual session setting

Create - Comodo Cloud Browser

Name **Settings**

1. Navigation

Disabled Enabled (*inside initially browsed URL*)

2. Time Quota (in minutes)

15

3. File Download Enabled

Scan and contain the following files Enabled

zip exe pdf jpg

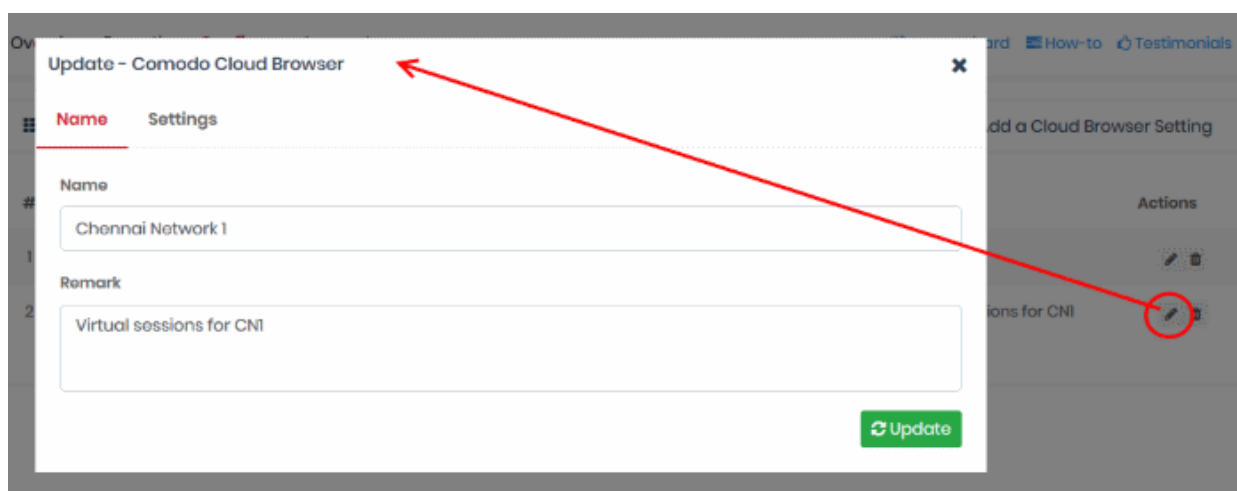
Create

- **Navigation** - Allow or block users from visiting sub-domains of the initial URL.
 - Disabled - Users cannot browse anywhere other than the website that triggered the virtual session.
 - Enabled - Users can browse the initial URL, the resources under the initial URL, and any sub-domains. Users cannot change the URL itself nor visit another website.
- **Time Quote** - Set how long the virtual session should run for. The session will end when this time elapses.
- **File Download** - Allow or block users from saving files in the virtual session. We recommend you 'Scan and contain' downloaded files if you enable this setting.
- **Scan and contain the following files** - Specify which types of files are scanned.
 - Enabled - Select the file types that CSIG should scan.
- Click 'Create' when done

The rule is saved and listed in the CCB interface. You can now add this rule to the security section of a policy. [Click here](#) if you need help to create policies.

Edit a cloud browser rule

- To update a CCB rule, click the edit  button beside the rule




The 'Update - Comodo Cloud Browser' dialog is similar to the create CCB rule explained [above](#).

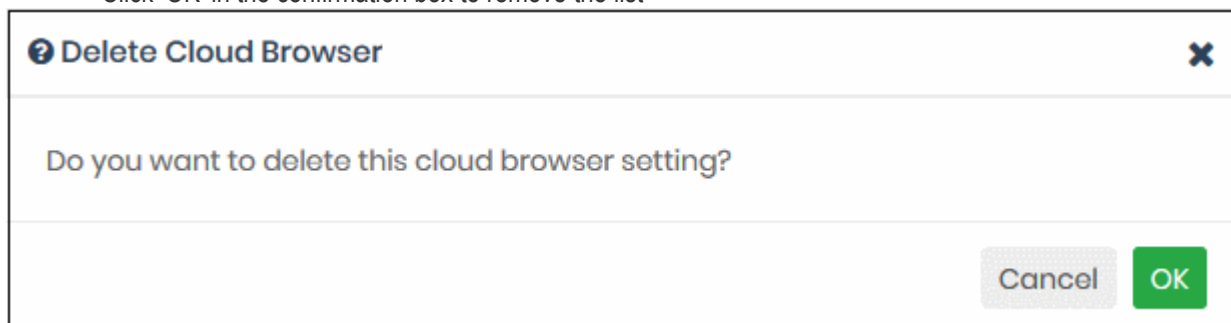
- Modify the name, description and/or the settings as per your requirements.
- Click the 'Update' button.

Policies which feature the rule are dynamically updated with the rule's new settings.

Delete a cloud browser rule

You cannot delete a virtual session rule that is currently active in a policy. You must first disable it in all policies before deleting it.

- Click the trash can icon  beside a CCB rule to delete it.
- Click 'OK' in the confirmation box to remove the list



6 Apply Policies to Networks and Roaming/Mobile Devices

- Click 'Configure' > 'Policy' to open the 'Policies' screen
- A policy is a security profile which contains at least one 'Security Rule', 'Category Rule' or 'Black/White list'.
- You add the rules to a policy then apply the policy to a device or network. You can also add block pages which are shown when users visit a banned website.
- You must have already created at least one rule before you can create a policy. See ['Manage CSIG Rules'](#) for help.
- You must also have added at least one device or network, or have imported a site using the local resolver.
 - See [Add Networks, Roaming Endpoints and Mobile Devices](#) to manually add networks and

devices

- See [Setup Local Resolver Virtual Machines and Import Sites](#) to setup a local resolver and automatically import a network site.
- You can create multiple policies. You can add multiple networks/devices to a single policy.
- You can also apply policies to internal network objects covering a single endpoint or IP address block.

How CSIG applies rules in a policy:

- CSIG checks the whitelist first, then the blacklist, then the security/category rules.
- For example, if the visited domain is whitelisted, then access is allowed. CSIG will check no further.
- If it is not in the whitelist, CSIG checks the blacklist. If found then it is blocked.
- If it is not in blacklist, CSIG checks the security / category rules. If the site belongs to a banned category then it is blocked.
- If the site isn't in the blacklist or category rules, then it is allowed.

Click 'Configure' > 'Policy' to open the 'Policies' screen

#	Policy Name	Remark	Actions
1	AgentsPolicy		[Edit] [Delete]
2	clifton		[Edit] [Delete]
3	seattle		[Edit] [Delete]
4	marsilya		[Edit] [Delete]
5	Manchester agent		[Edit] [Delete]
6	Goode Mobile		[Edit] [Delete]

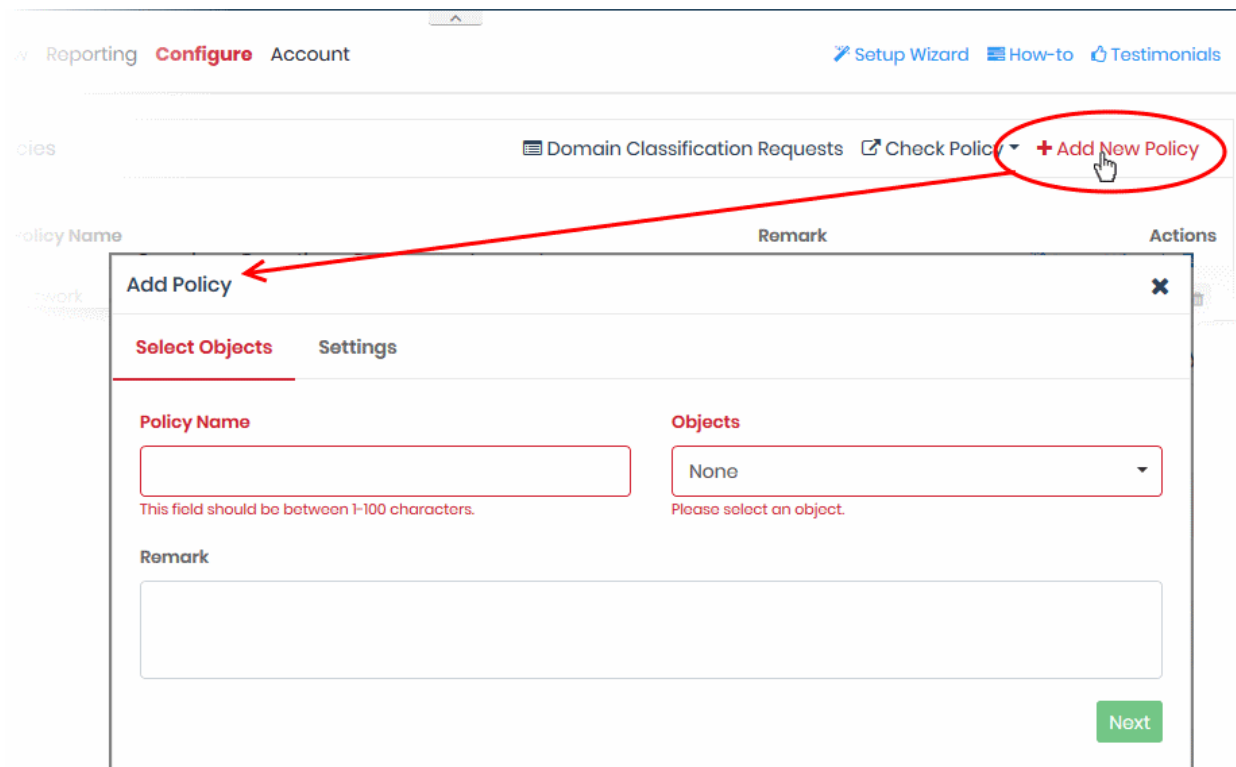
- The links on the right of the title bar let you:
 - **Add New Policy** - Create a new policy and apply it to networks, devices and imported network sites. See [Create a new policy](#) for help with this.
 - **Domain Classification Requests** - View the category of a domain, suggest a different category, and propose an unclassified site is added to our database. See [Domain Classification Requests](#)
 - **Check Policy** - Test whether your rules function correctly. See [Test whether your policy works](#) for help.

The following links contain help on this interface:

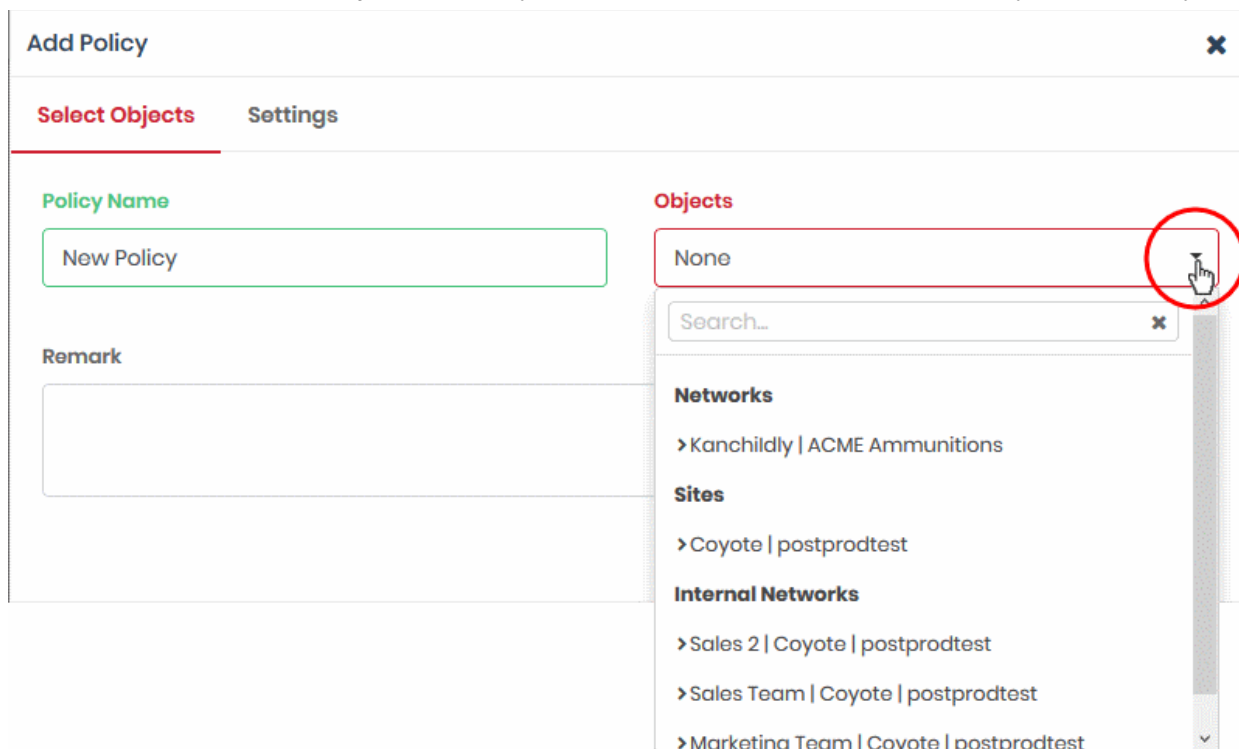
- [Create new policies and deploy them to networks and devices](#)
- [Edit a policy](#)
- [Test whether your policy works](#)
- [Delete a policy](#)

Create a new policy

- Click 'Configure' > 'Policy'
- Click 'Add New Policy'



- **Policy Name** - Enter a label for the policy
- **Objects** - Select the items to which the policy should apply. This can be a network, roaming device, site, internal network or mobile device. You can select multiple instances of each.
 - **Note** - The 'Objects' menu only shows networks, devices or sites that do not yet have a policy.



- **Networks** - List of manually added networks
- **Agents** - List of roaming Windows and Mac OS devices enrolled by installing the Secure Internet Gateway agent
- **Mobile Agents** - List of enrolled Android and iOS devices
- **Sites** - List of network sites imported by deploying the local resolver VA

- **Internal Networks** - Internal network objects within imported sites. Note - Policies applied to a site will over-rule policies applied to internal network objects.
- You can apply a policy to any number of objects.
- **Remark** - Enter a description for the policy (optional)
- Click 'Next' or 'Settings' to configure the policy:

Add Policy
✕

Select Objects
Settings

Only B/W Mode Disabled

Block All Mode Disabled

Safe Search Disabled

Security Rule

None

Category Rule

None

Redirect to CCB

Please select at least a Security Rule or a Category Rule or a B/W List.

Domain B/W List

Name	Type	☐
Blacklisted Domains	BlackList	☐
Whitelisted Domains	WhiteList	☐
sharefile.com	WhiteList	☐
For Company LTD	WhiteList	☐

Block Page Appearance ⚠

None

Add

- **Only B/W Mode** - If enabled, you can only add blacklist and/or whitelist rules to this policy. You cannot add security or category rules to the policy.
- **Block All Mode** - If enabled, all domains are blocked EXCEPT the domains mentioned in the whitelist(s) selected for this policy. You can only add whitelists to the policy under this setting.
- **Safe Search** - Activates the content filtering feature of search engines like Google, Bing and Yahoo. Safe search eliminates explicit and potentially offensive websites from the results page of a search. This setting is disabled by default.
- **Security Rule** - Select a rule to block websites that host specific types of threats. The drop-down lists security rules that have been added in the 'Policy Settings' section. See '[Manage Security Rules](#)' for more details.
 - **Redirect to CCB** - If enabled, sites in this policy are instead opened in a virtual environment. Enable this and select a virtual session rule from the drop-down. See '[Manage Cloud Browser Settings](#)' if you need more information on virtual session rules.
- **Category Rule** - Select a 'Category Rule' to block websites by content-type. The drop-down lists category rules that have been added in the 'Policy Settings' section. See '[Manage Category Rules](#)' for

more details.

- **Domain B/W List** - Select a black/white list to block specific domains. B/W lists added to the the 'Policy Settings' section are shown in the dialog.
 - Select the B/W list(s) you want to add to the policy.
See '**Manage Domain Blacklist and Whitelist**' for more details.

Please note - B/W lists will over-rule security/category rules in the event of a conflict over a particular domain.
- **Block Page Appearance** - Choose the block page to be shown to users if they try to visit a site prohibited by your policy. The drop-down displays block pages added via the 'Policy Settings' area. See **Manage Block Pages** for more details.
 - **Note** - The block page is shown on all devices to which the policy is applied, except mobile devices.

Example policy settings are shown in the following screenshot:

- Click 'Add' to save your policy.

The policy is applied to the chosen networks and devices.

Edit a policy

- Click 'Configure' > 'Policy'
- Click the edit button in the row of the policy you want to update:

The screenshot shows the 'Configure' section of the admin console. At the top, there are navigation tabs: Overview, Reporting, **Configure**, and Account. On the right, there are links for Setup Wizard, How-to, and Testimonials. Below this is a sub-header for 'Policies' with options for Domain Classification Requests, Check Policy, and Add New Policy. A table lists two policies: 'New Network Policy' (ID 1) and 'Mobile Device Policy' (ID 2). The 'New Network Policy' row has an edit icon circled in red. A red arrow points from this icon to the 'Update Policy' dialog box below. The dialog has tabs for 'Select Objects' and 'Settings'. It contains input fields for 'Policy Name' (New Network Policy), 'Objects' (Kanchildly | ACME Ammunitions), and 'Remark' (Policy for ACME network). A green 'Update' button is at the bottom right.

The 'Update Policy' dialog appears. The dialog is similar to the 'Add Policy' dialog explained **above**.

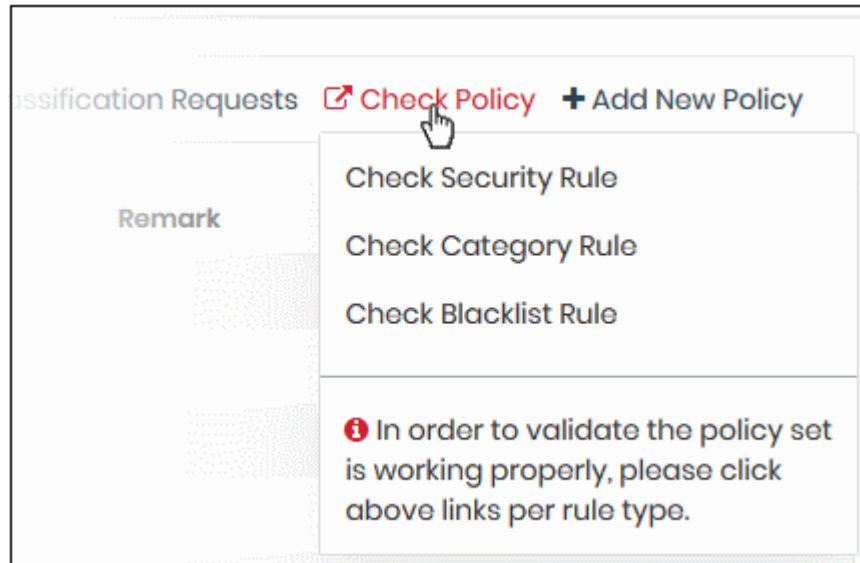
- Modify the name, description and/or settings as required.
- Click the 'Update' button

The updates will be applied to all devices on which the policy is active.

Test whether your policy works

The policies interface lets you check whether your rules are functioning correctly on your networks and roaming devices.

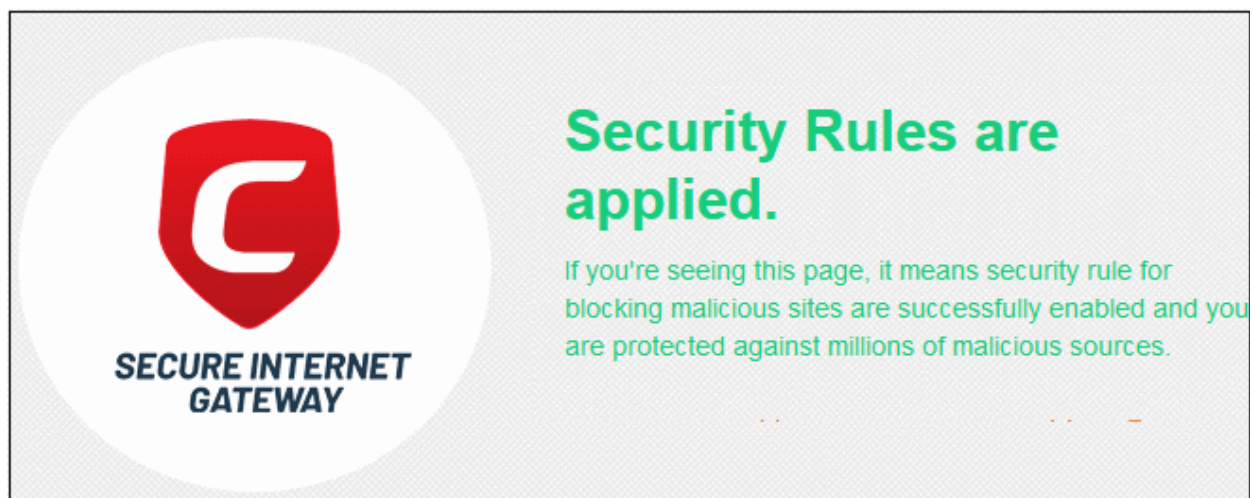
- Login to Secure Internet Gateway from any endpoint in an enrolled network, or from an enrolled roaming/mobile device.
 - See **Logging-in to the Administrative Console** if you need help with this.
- Click 'Configure' > 'Policy'
- Click 'Check Policy' at the top-right



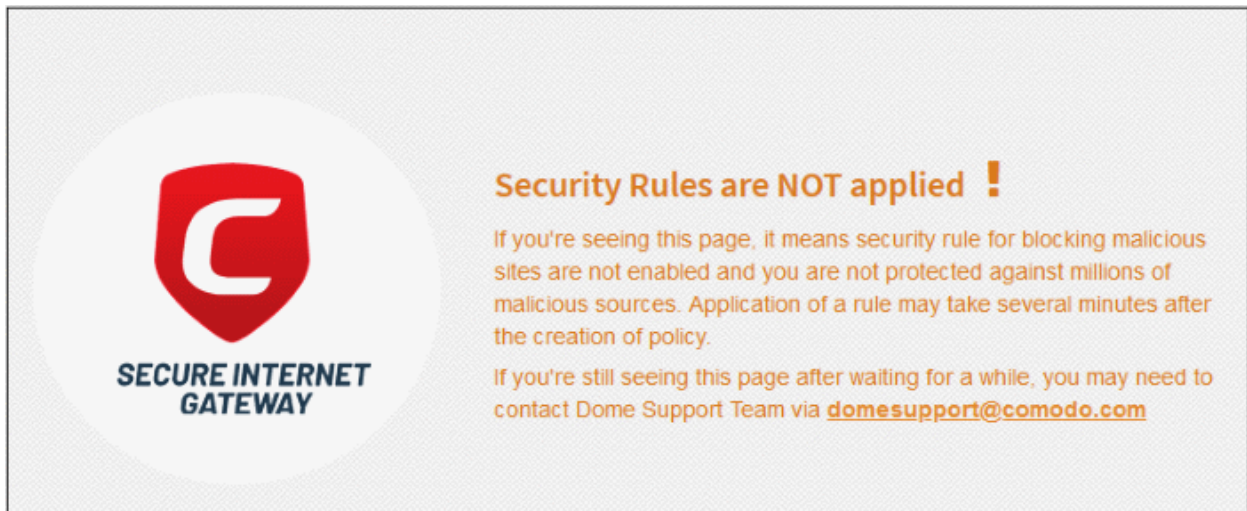
- **Check Security Rule** - Test whether policy security rules are working correctly on your devices
- **Check Category Rule** - Test whether policy category rules are working correctly on your devices
- **Check Blacklist Rule** - Test whether policy blacklist rules are working correctly on your devices

You need to repeat this process on each device you want to test.

You will see the following message if the rule is active:



You will see the following if the rule is not active:

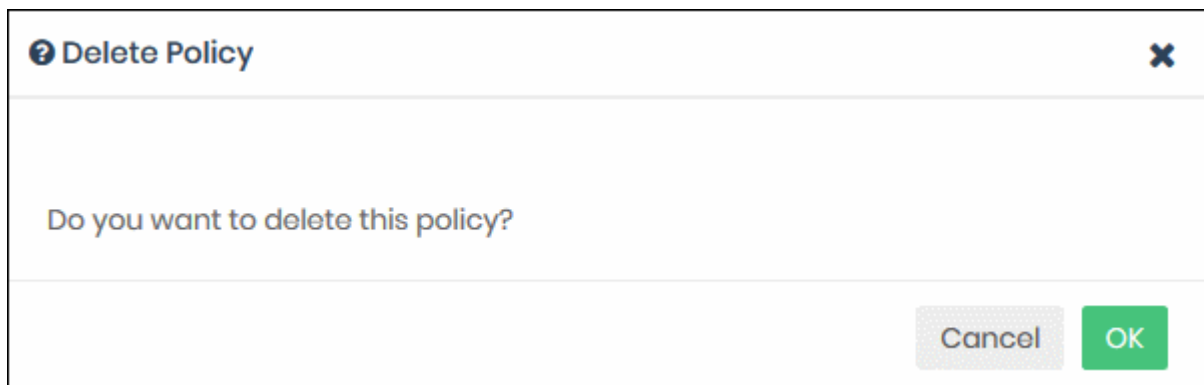


Please check that you have configured your policy correctly and that you have applied it to target devices.

Delete a policy

- Click 'Configure' > 'Policy'
- Click the trash can icon beside a policy

A confirmation dialog is shown:



- Click 'OK' to confirm removal of the policy from the list.

The policy is removed from the networks/endpoints/devices on which it was active.

7 Domain Classification Requests

Click 'Configure' > 'Policy' > 'Domain Classification Requests'.

- Secure Internet Gateway uses a massive database of websites which are classified into various categories.
- These website categories can be added to a 'Category Rule'.
- You can then add the rule to a policy to allow or block sites in the category.

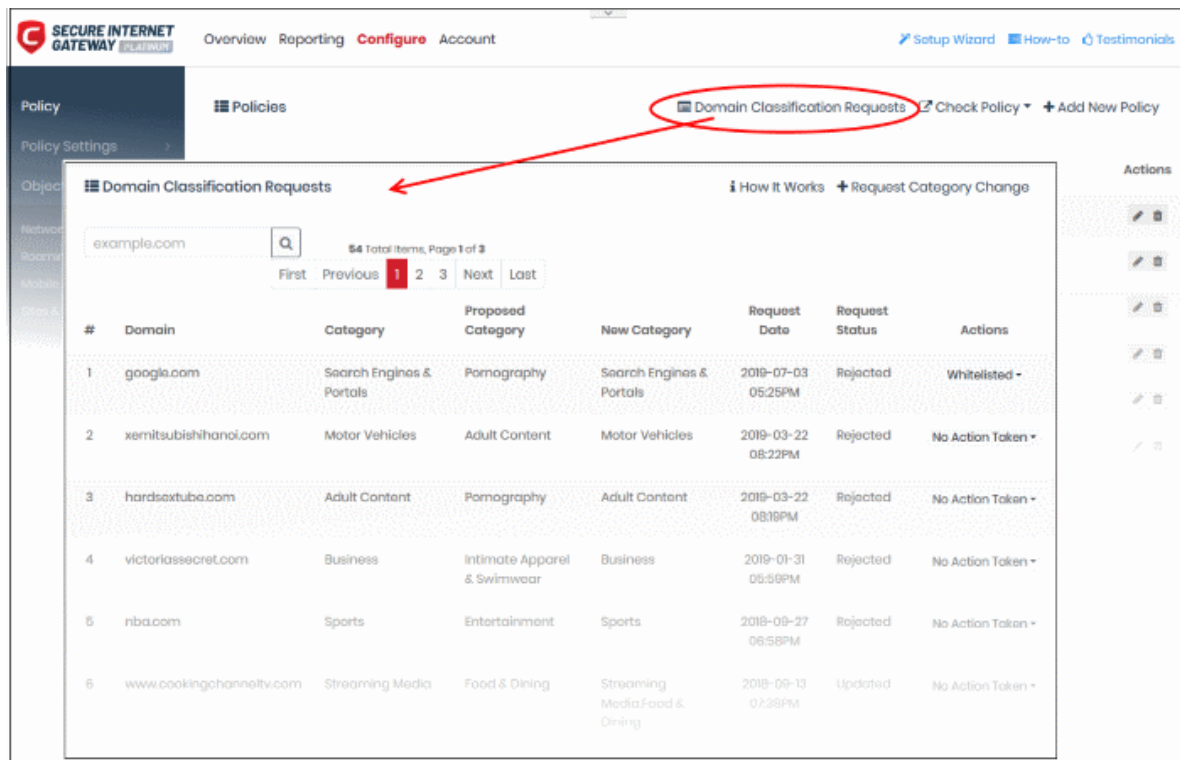
Domain classification tools:

- You can recommend that a specific website is added to one of our categories. For example, you might find a gambling site which is not yet recognized by the filter.
- You can also suggest a different category for an existing domain if you think it has been incorrectly classified.

Your submission will be analyzed by Comodo. The status of your request can be viewed in the interface.

Open the 'Domain Classification Requests' area

- Click 'Configure' > 'Policy'
- Click 'Domain Classification Requests' on the title bar



The interface shows a list of all previous requests.

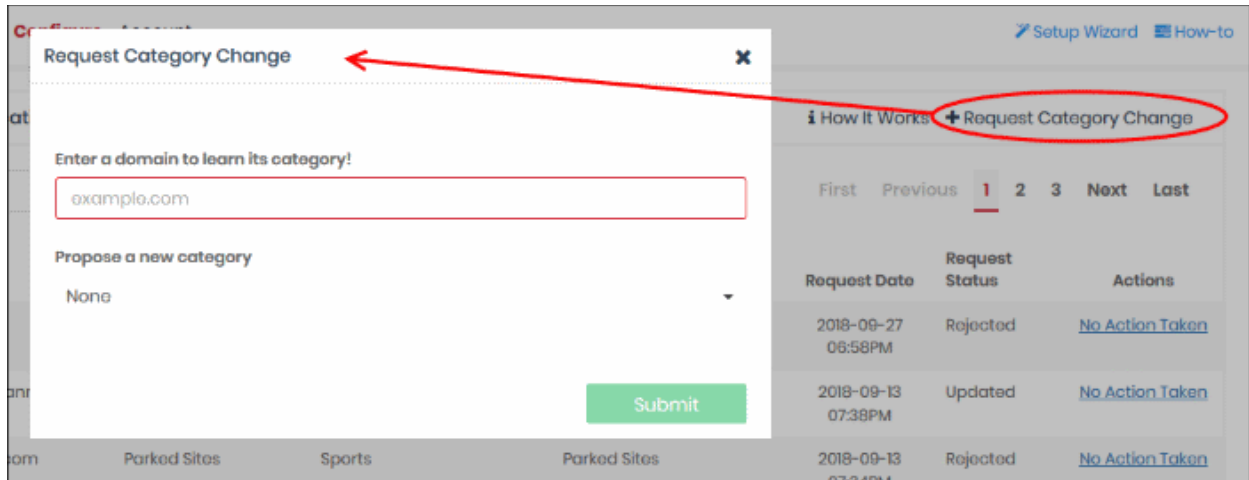
Domain Classification Requests	
Domain	The URL of the website for which you have requested a category change.
Category	Class of websites to which the site currently belongs. This is available only for sites that are already in our filtering database.
Proposed Category	The class of sites that you have suggested for the domain.
New Category	The class of sites to which the domain was assigned after analysis by Comodo.
Request Date	The date and time at which the request was submitted.
Request Status	Whether the request was accepted or rejected.
Actions	Whitelist or blacklist the domain, or remove the request entirely. See Whitelist/Blacklist a Domain for more details.

- **Submit a domain classification Request**
- **Whitelist/Blacklist a Domain**

Submit a Domain Classification Request

You can submit a domain classification request if you think a site should belong to a specific category.

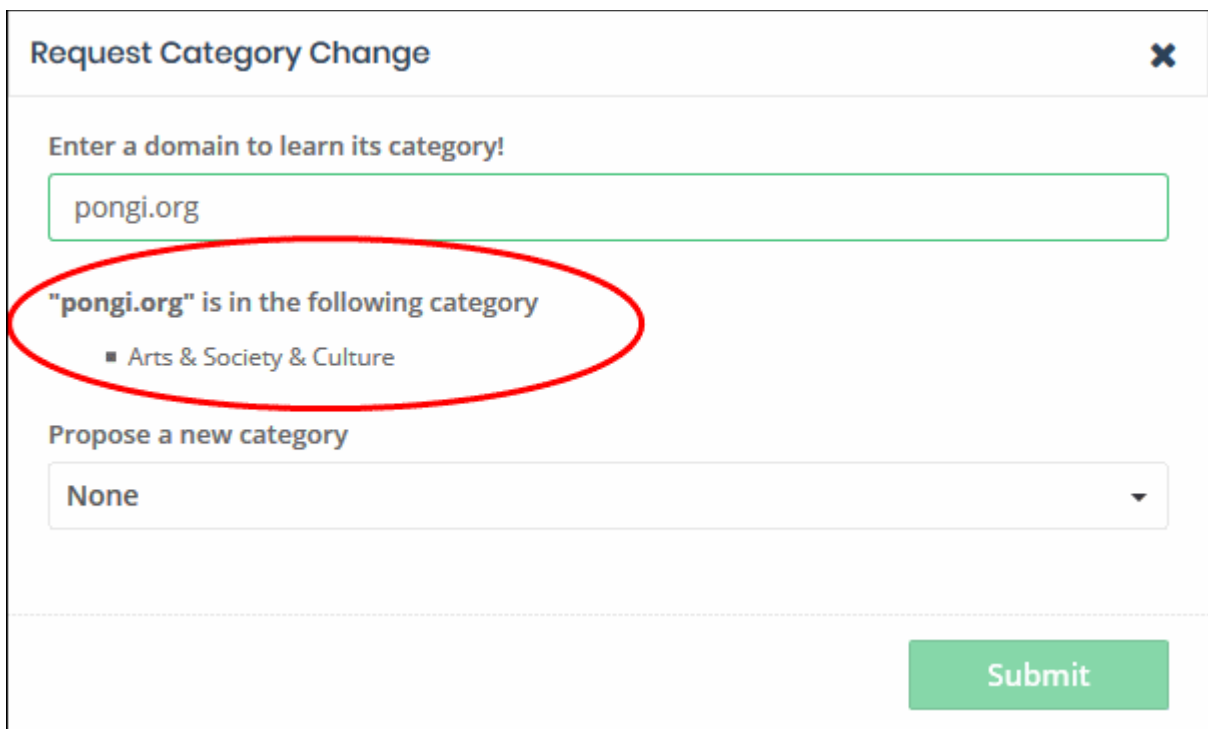
- Click 'Configure' > 'Policy' > 'Domain Classification Requests'
- Click 'Request Category Change'



- Enter the name of the domain. Secure Internet Gateway will search whether the domain has been registered.

Pre-registered Domain

- If the domain is already classified, its current category is shown as follows:



- If you wish to suggest a new category, select it from the 'Propose a new category' drop-down and click 'Submit'

Request Category Change ✕

Enter a domain to learn its category!

pongi.org

"pongi.org" is in the following category

- Arts & Society & Culture

Propose a new category

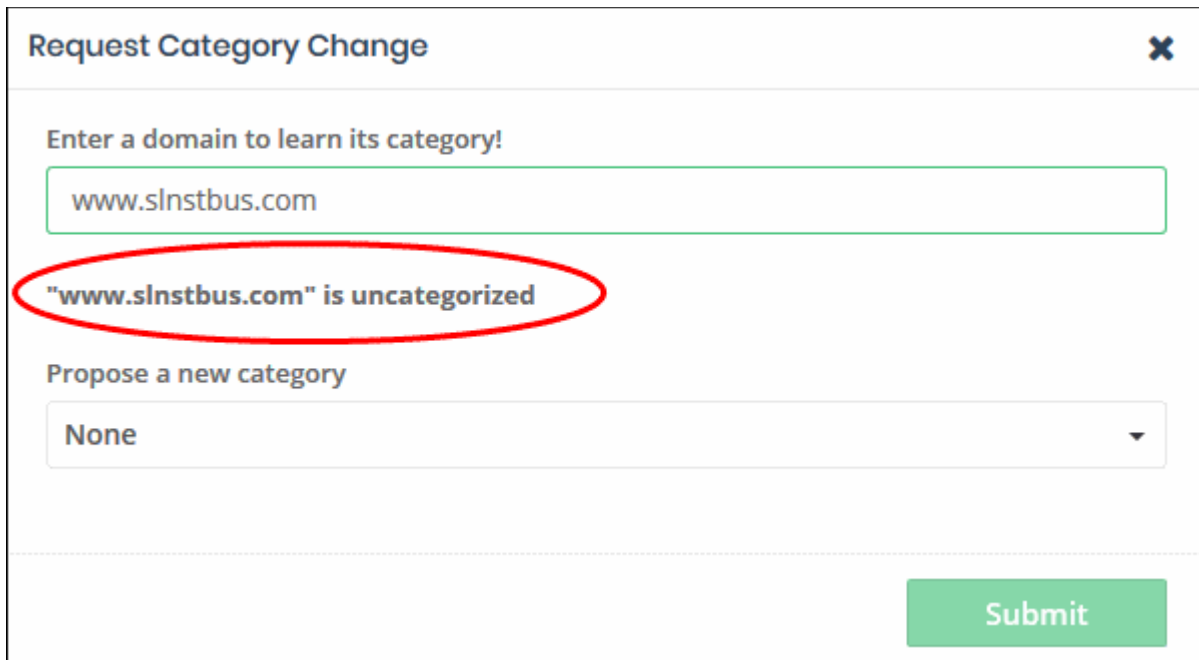
None

- Sports
- Travel**
- Travel
- Misc**
- Real Estate
- Technical Information
- Political Issues
- Religion
- Government & Legal

Comodo will analyze the request. If successful, your site will be placed in the category within 48 hours.

New Domain

- Domains that are not in our database are listed as 'Uncategorized':



Request Category Change ✕

Enter a domain to learn its category!

"www.slnstbus.com" is uncategorized

Propose a new category

- **Propose a new category** - Select the category to which you think the domain should belong. Click 'Submit'.

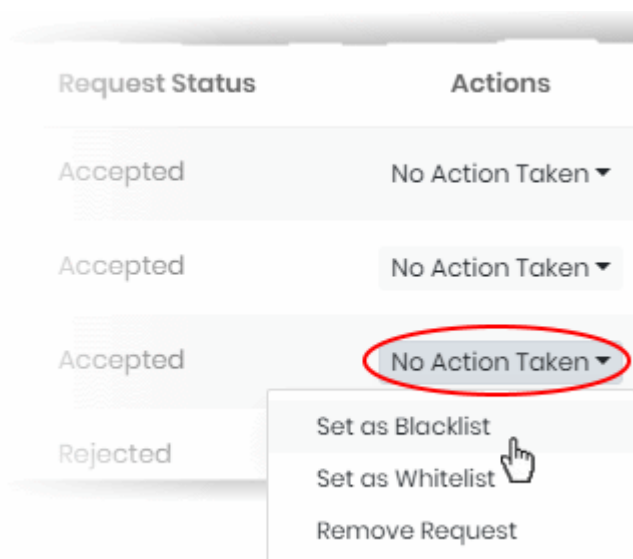
Comodo staff will analyze the request and assign the domain to a category within 48 hours.

Whitelist/Blacklist a Domain

Whitelists and blacklists let you explicitly block or allow access to certain domains. This is useful if you want to create exceptions for sites that are blocked or allowed by a category rule.

General points:

- Whitelist - Access to the domain is allowed, even if it is blocked by a category rule.
- Blacklist - Access to the domain is blocked, even if it is allowed by a category rule.
- There are two places you can set black/whitelists in Secure Internet Gateway:
 - Use the 'Set as Black/Whitelist' action in this interface. These lists apply to ALL your policies.
 - Add a black/whitelist to a specific policy. These lists apply only to the networks/devices covered by the policy.
- Blacklists and whitelists over-rule category rules for a domain.
- Whitelists over-rule blacklists.
- Click the 'Actions' link in the row of the domain



- Select the option from the drop-down
 - **Set as Blacklist** - The domain is added to a master blacklist for your account and blocked on ALL your policies.
 - **Set as Whitelist** - The domain is added to a master whitelist for your account and allowed on ALL your policies.
 - **Remove Request** - The request is withdrawn and deleted from the list. The domain is also removed any list you may have put it on using the 'Set as blacklist' or 'Set as whitelist' links.
 - **Take no action** - Do not whitelist or blacklist the domain. Do not remove the request. The domain continues to be allowed or blocked according to its current category and your policy.
- **Request accepted** - The domain's category changes to your requested category. The domain is allowed or blocked based on this new category. It is removed from any list you may have put it on using the 'Set as blacklist' or 'Set as whitelist' links.
- **Request rejected** - The domain remains in its current category and is allowed or blocked accordingly. It remains on any list you may have put it on using the 'Set as blacklist' or 'Set as whitelist' links.

The following table has some examples of how blacklists and whitelists work together:

www.example.com	Whitelisted in device policy	Whitelisted using 'Set as whitelist' link	Blacklisted in device policy	Blacklisted using 'Set as blacklist' link	Outcome
Case 1	✗	✗	✗	✓	Blocked
Case 2	✗	✗	✓	✗	Blocked
Case 3	✗	✗	✓	✓	Blocked
Case 4	✗	✓	✗	✗	Allowed
Case 5	✗	✓	✓	✗	Allowed
Case 6	✓	✗	✗	✗	Allowed
Case 7	✓	✗	✗	✓	Allowed
Case 8	✗	✓	✓	✓	Allowed

8 View Protection Details by Customer

Details about networks and roaming agents enrolled for an end-customer. This feature is only available for MSP accounts.

- Click 'Configure' > 'MSP Control' > 'Customer' to open the 'Customer' area:

The screenshot shows the 'Configure' menu with 'MSP Control' selected. The 'Customer' table displays the following data:

#	Customer	# of Networks	# of Roaming Devices	# of Mobile Devices	# of Sites	# of Local Resolver
1	l23bom	2	2	1	0	0
2	gozde	3	3	4	0	1
3	gozde-ds	7	2	0	2	1
4	LeBron	0	0	0	1	1
5	name	0	0	0	1	1
6	vtiger	13	4	3	0	0

Customer - Table of Column Descriptions

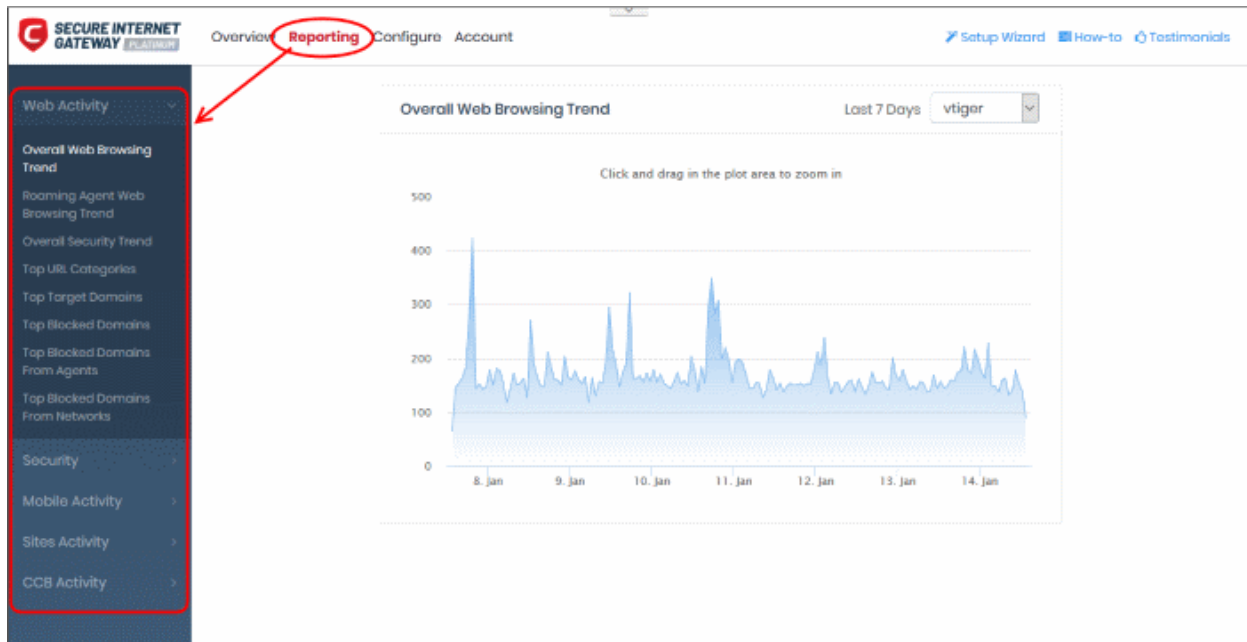
Column Header	Description
Customer	The organization enrolled as your Secure Internet Gateway client
# of Networks	The count of networks enrolled for the customer
# of Roaming Devices	The count of of out-of-network Windows / Mac devices enrolled for the customer.
# of Mobile Devices	The count of Android and iOS mobile devices enrolled for the customer
# of Sites	The count of networks (aka 'sites') which were automatically imported by installing the local resolver on a customer network.
# of Local Resolver	The count of local resolver virtual appliances registered for the customer

You can only view the details and cannot edit or delete the entries.

9 Reports

Reports provide a detailed overview of web and security activity on your networks and endpoints.

- Click 'Reporting' on the top navigation to open the reports area:



- There are five types of reports, 'Web Activity', 'Security', 'Mobile Activity', 'Site Activity' and 'CCB Activity'.
- The charts in each report are larger, easier-to-manipulate-versions of those on the dashboard.
- Click the links below to jump to the relevant section in the dashboard chapter.

Web Activity Reports

- [Overall Web Browsing Trend](#)
- [Roaming Agent Web Browsing Trend](#)
- [Overall Security Trend](#)
- [Top URL Categories](#)
- [Top Target Domains](#)
- [Top Blocked Domains](#)
- [Top Blocked Domains From Agents](#)
- [Top Blocked domains From Networks](#)

Security Reports

- [Overall Advanced Threats](#)
- [Roaming Agent Advanced Threats](#)
- [Most Blocked Mobile Threats](#)
- [Sites - Most Blocked Threats](#)
- [Overall Security Incidents](#)
- [Roaming Agent Security Incidents](#)

Mobile Activity Reports

- [Top Target Domains of Mobile Users](#)
- [Web Traffic of Mobile Users](#)
- [Top Blocked Categories of Mobile Users](#)

Sites Activity Reports

- [Sites - Top Target Domains](#)
- [Sites - Overall Web Browsing Trend](#)

- [Sites - Top Blocked Domains](#)

CCB Activity Report

- [Top Visited Sites](#)
- [Top Opened Sessions](#)
- [File Status](#)

See '[The Dashboard](#)' to find out more about these reports.

10 Read Testimonials

- The 'Testimonials' page contains reviews, comments and feedback about Secure Internet Gateway from our customers.
- Click 'Testimonials' at the top right
- You will be taken to <https://cdome.comodo.com/dns-internet-security.php>

The screenshot shows the admin interface with a navigation bar containing 'Setup Wizard', 'How-to', and 'Testimonials'. The 'Testimonials' link is circled in red. Below the navigation bar, there are filters for 'ACME Ammunitions' and '12 Hours'. The main content area displays three testimonial cards:

- Social Telecoms CIC**: Social Telecoms CIC using Dome Shield for Keeping Internet Safe for Customers. Learn how Social Telecoms CIC are using Dome Shield for making internet a safer place for their customers by applying a Default Internet Browsing Filter. *We have managing security and IT services for more than 500 locations across the UK and Europe.
- Meshoppen Stone Inc**: Meshoppen Stone Inc. using Dome Shield to boost workplace productivity and enhance customer experience. Learn how Meshoppen Stone Inc is using Comodo Dome Shield to boost workplace productivity and enhance customer experience.
- FORE MACHINE COMPANY**: Fore Machine using Dome Shield for NIST Cybersecurity Framework. Learn how Fore Machine Company, an aerospace industry supplier of machine parts is using Dome Shield for keeping web-borne attacks off their IT network and satisfy the NIST (National Institute of Standards and Technology) Cybersecurity Framework.

- You can peruse the views and experiences of our Secure Internet Gateway customers.

11 View Account Details

- The 'Account Info' page shows user information, total DNS requests for the month, and licenses associated with your account.
- You can also upgrade to a Platinum license. See [Compare Secure Internet Gateway Packages](#) to see what features come with each license.
- Click 'Account' to open the account info page:

The screenshot shows the 'Account' page in the Comodo Secure Internet Gateway Admin Panel. The 'Account' tab is circled in red. The page displays the following information:

- ACCOUNT INFO** (indicated by a red arrow)
- User Info**
 - Username / Email: ✓
 - User Type:
 - Joining Date:
- Total DNS Requests (January)**: 38k
- Licenses**

License Type	Retrieval Date	Expiration Date	Status	# of Endpoints	Quantity
GOLD	2018-07-30	N/A	Inactive	N/A	5
PLATINUM	2018-10-31	N/A	Active	25000-10000000	35000
- Upgrade to Secure Internet Gateway PLATINUM** for no DNS requests limit and for more features! [BUY](#)
SALES: +1(888)551-1531
- Secure Internet Gateway Platinum-only Features:**
 - ✓ Local DNS Resolver Virtual Appliances
 - ✓ Internal IP based Visibility & Control
 - ✓ Bypass Domains to Existing Internal DNS
 - ✓ Encrypt Network-wide DNS Traffic
 - ✓ Manage by Sites and DNS Egress Points
- [RATE US!](#) [REPORT ISSUE](#)

- **Username / Email** - Address that was used to sign-up for the account. System notifications are sent to this address.
- **User Type** - Kind of account - MSP or Enterprise
- **Joining Date** - Date you subscribed to Secure Internet Gateway

Total DNS Requests

- Shows the number of requests received by Secure Internet Gateway from the enrolled devices for the current month.
- The number of requests you can make depends on your license type:
 - **Platinum license**
 - Unlimited DNS requests

- **Gold license**
 - DNS requests are capped at 300 K per month for the account. Account = requests from all your endpoints/networks.
 - The request limit is reset to 0 (zero) at the beginning of each month
 - DNS requests are mainly used up by first-time requests to external websites. Subsequent requests for the same site are handled by the local cache until TTL expires.
 - Requests to the Secure Internet Gateway Portal are *not* included in the 300 K limit.

Licenses

- License Type - CSIG subscription type
- Retrieval Date - Date of subscription. For Gold, this is the day you signed up. For Platinum, it is the day you purchased the license.
- Expiration Date - Subscription end date.
- Status - Whether or not the license is active
- # of Endpoints - Endpoint selection range for the license
- Quantity - Number of endpoints subscribed

Enterprise/Gold license holders can upgrade to a Platinum license by clicking the 'Buy' button.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit [comodo.com](https://www.comodo.com) or our [blog](#). You can also follow us on [Twitter](#) (@ComodoDesktop) or [LinkedIn](#).

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: EnterpriseSolutions@Comodo.com