Comodo Secure Internet Gateway

Software Version 2.13

Quick Start Guide

Guide Version 2.13.100620

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Comodo Secure Internet Gateway - Quick Start Guide

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 lets you create location-specific policies.

This document explains how to purchase licenses, add networks/devices, apply policies and generate reports:

Step 1 - Purchase a License and Login to Secure Internet Gateway

Two types of license are available:

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

Click here to compare packages.

There are two ways to to obtain a license:

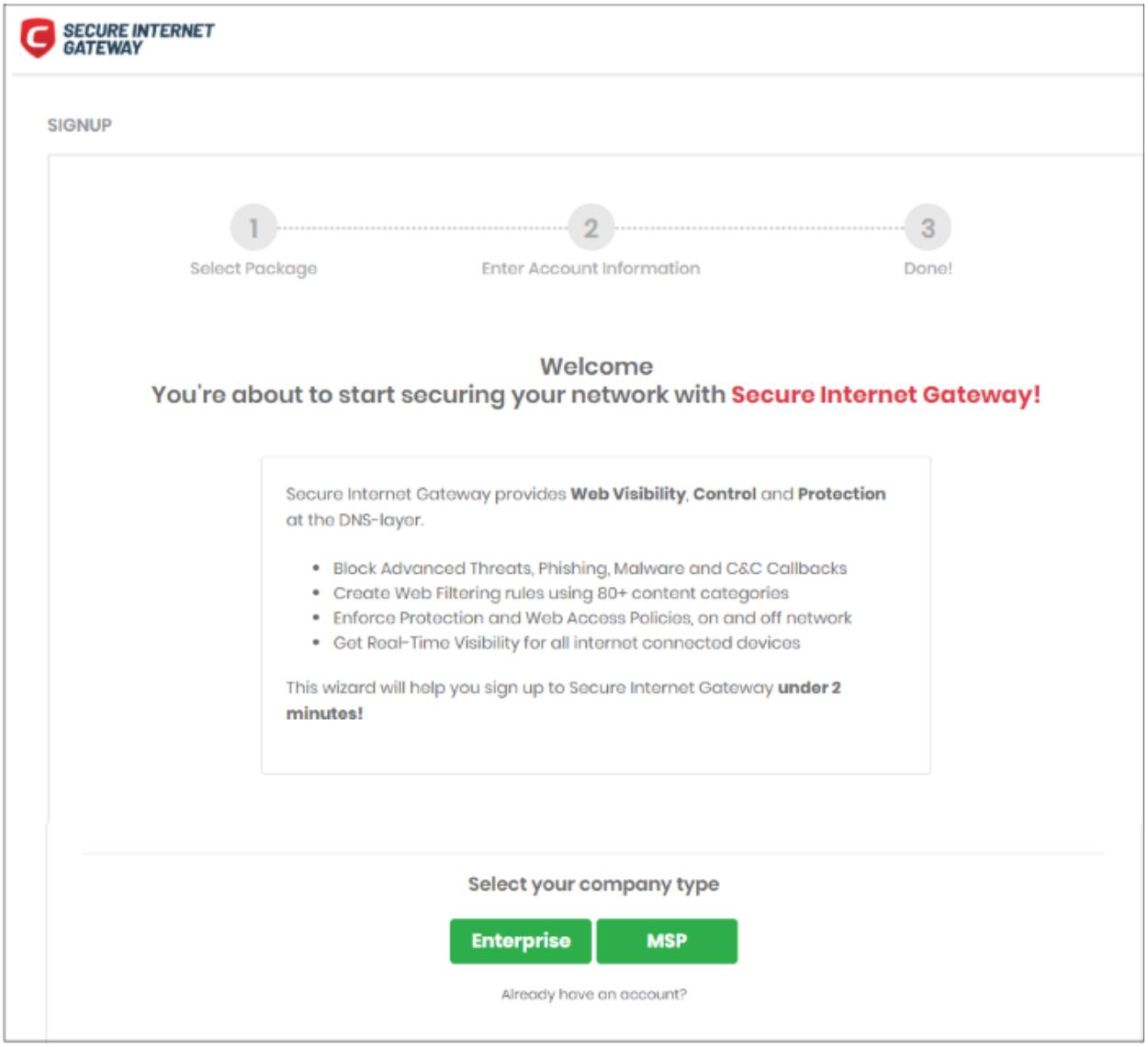
- **Stand-alone customers** - Sign-up for a free license at **https://cdome.comodo.com/dns-internet-security.php**.
- **Comodo One / Itarian / Dragon customers** (enterprise and MSP licenses) - Secure Internet Gateway is automatically activated in your account.

Stand-alone Customers:

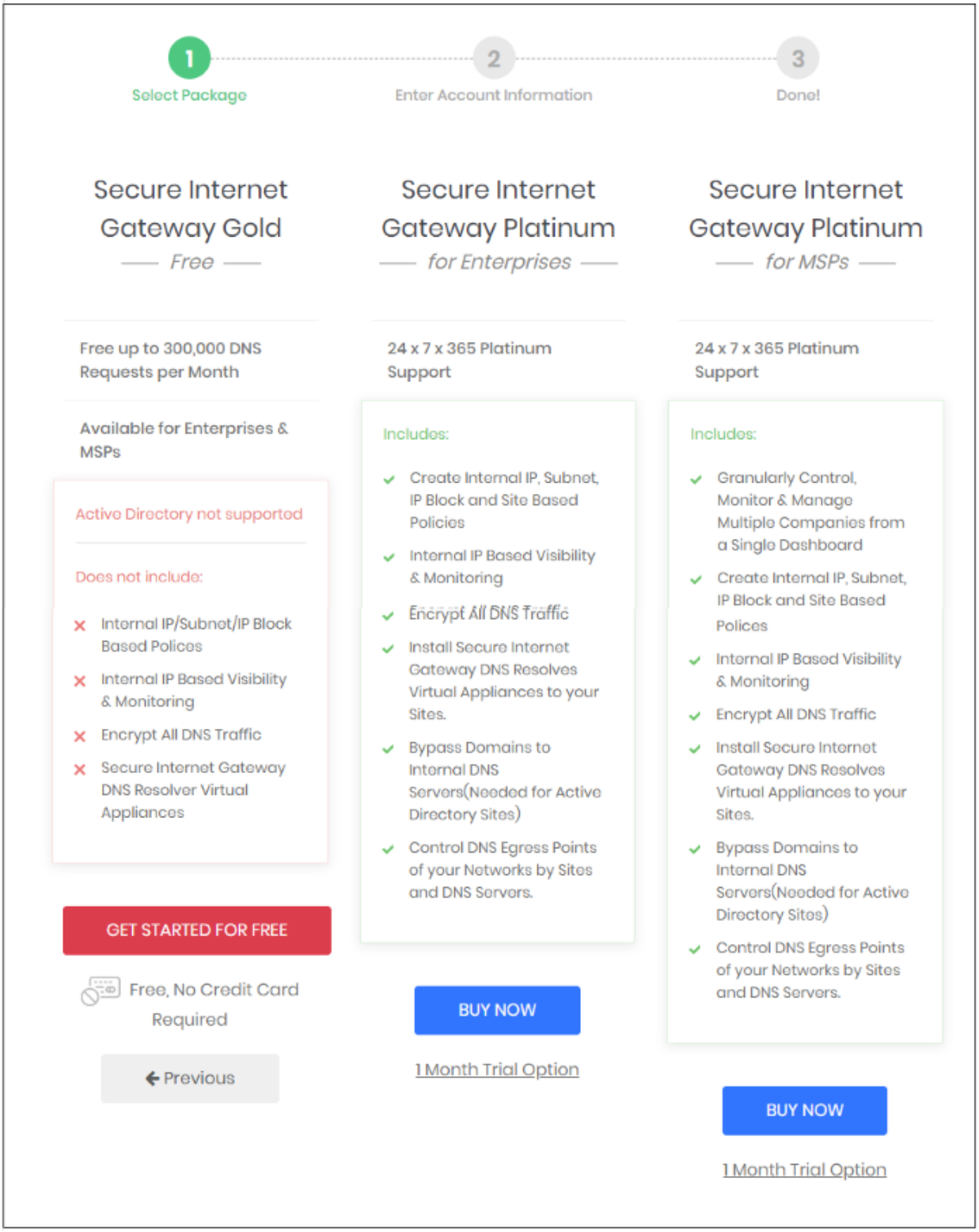
Sign up for a Gold license

- Visit **https://cdome.comodo.com/dns-internet-security.php**.

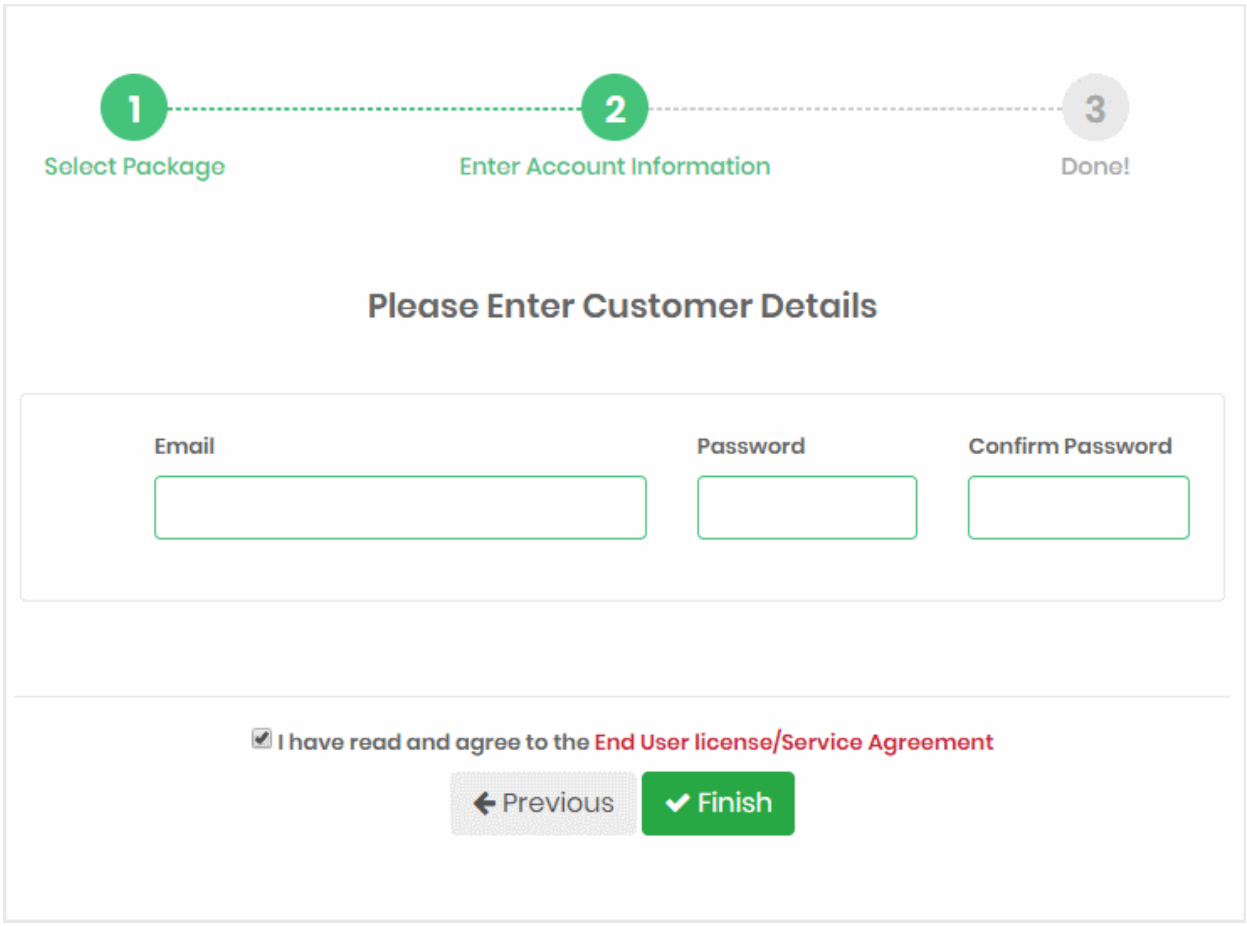
- Click 'Start Now'
- You are taken to the sign-up page:



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



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

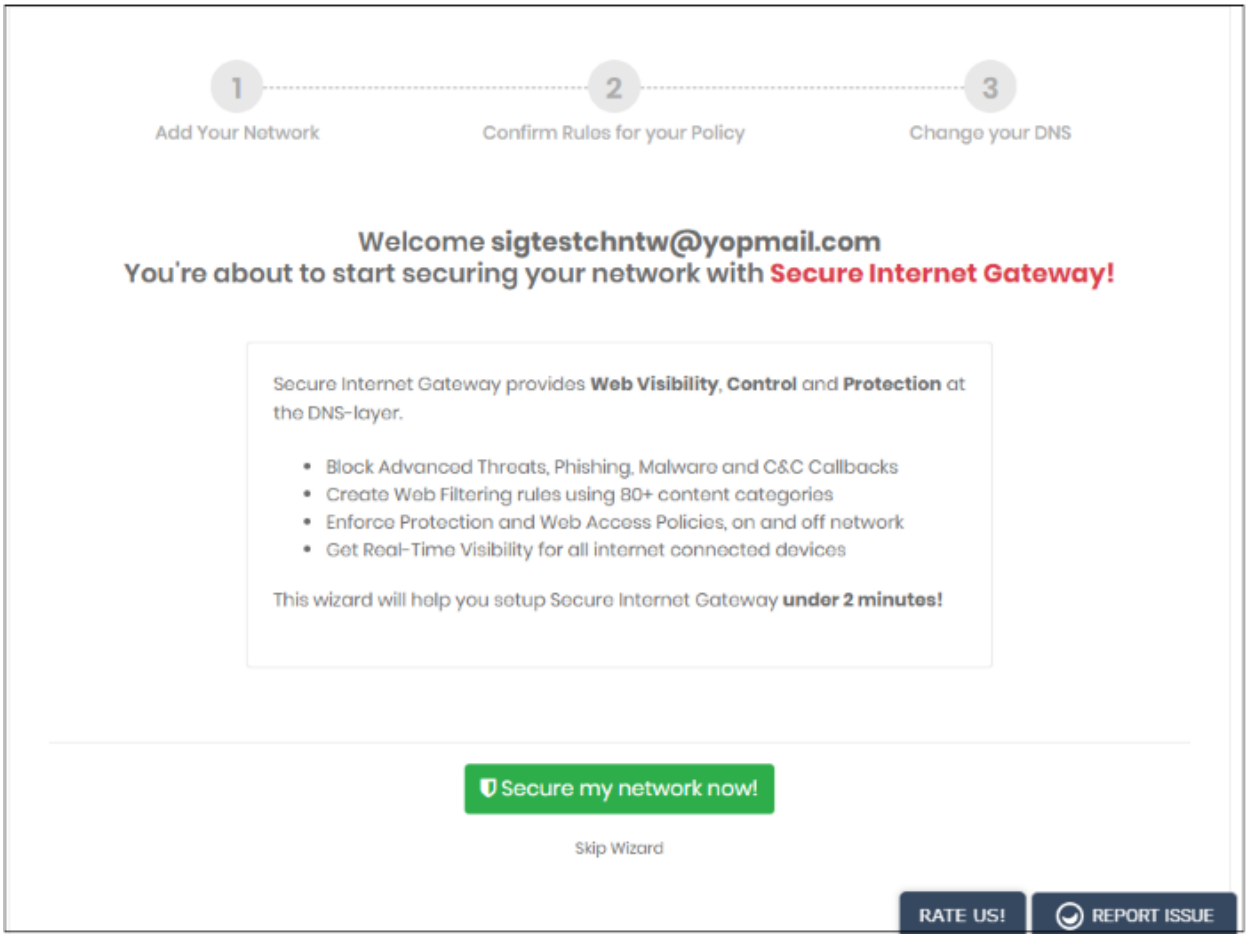


- **Email** – Enter your contact mail address. Order confirmations and license keys are sent to this address. This address doubles up as your Secure Internet Gateway username.
- **Password** and **Confirm Password** - Create a passphrase to login to Secure Internet Gateway. Please use at least 8 characters, and a mix of upper and lower letters, numbers, and special characters.
- **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 **Step 2 - Add your network** for help with this.



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

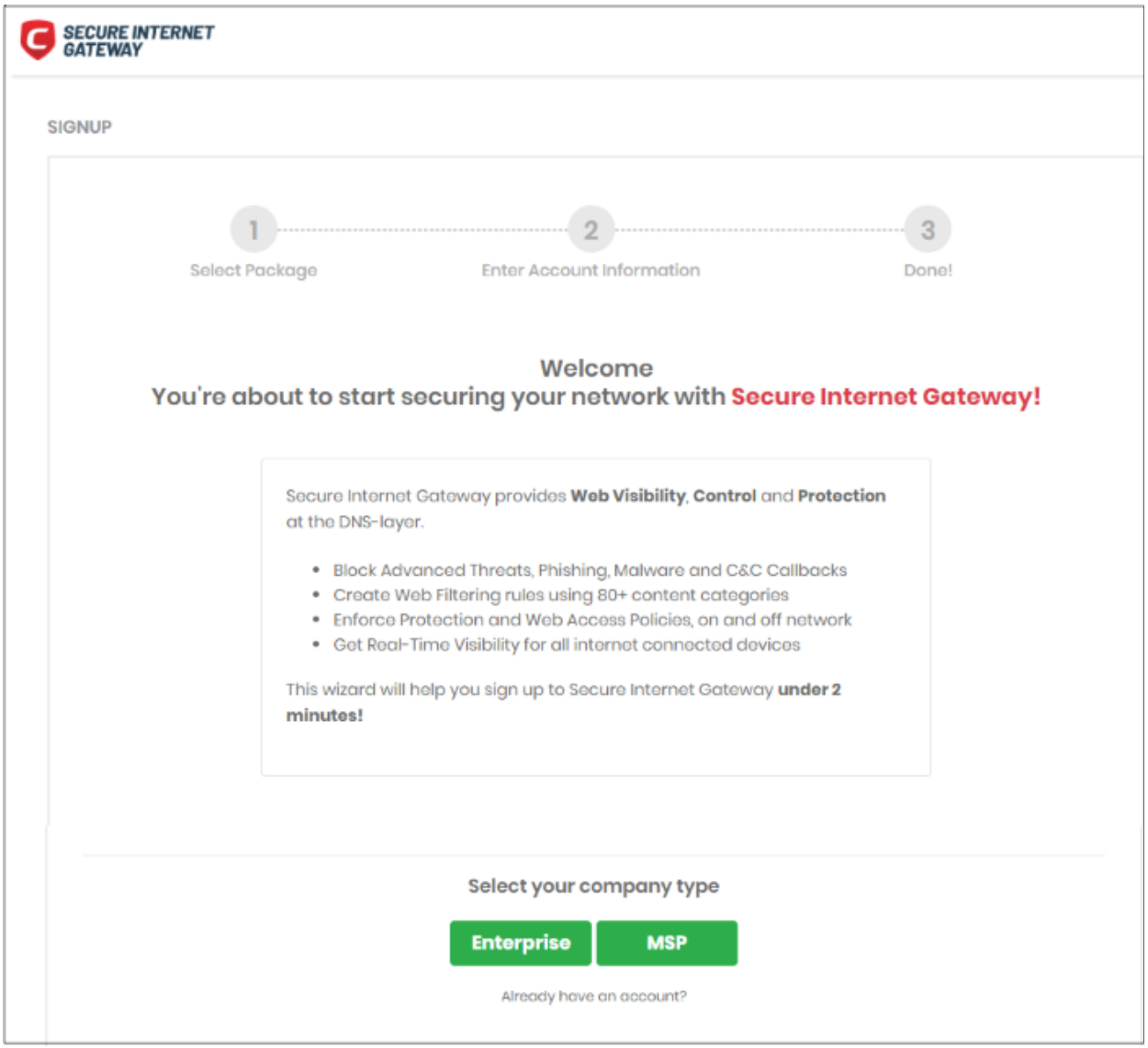
Purchase a Platinum package

There are two ways to get a platinum license:

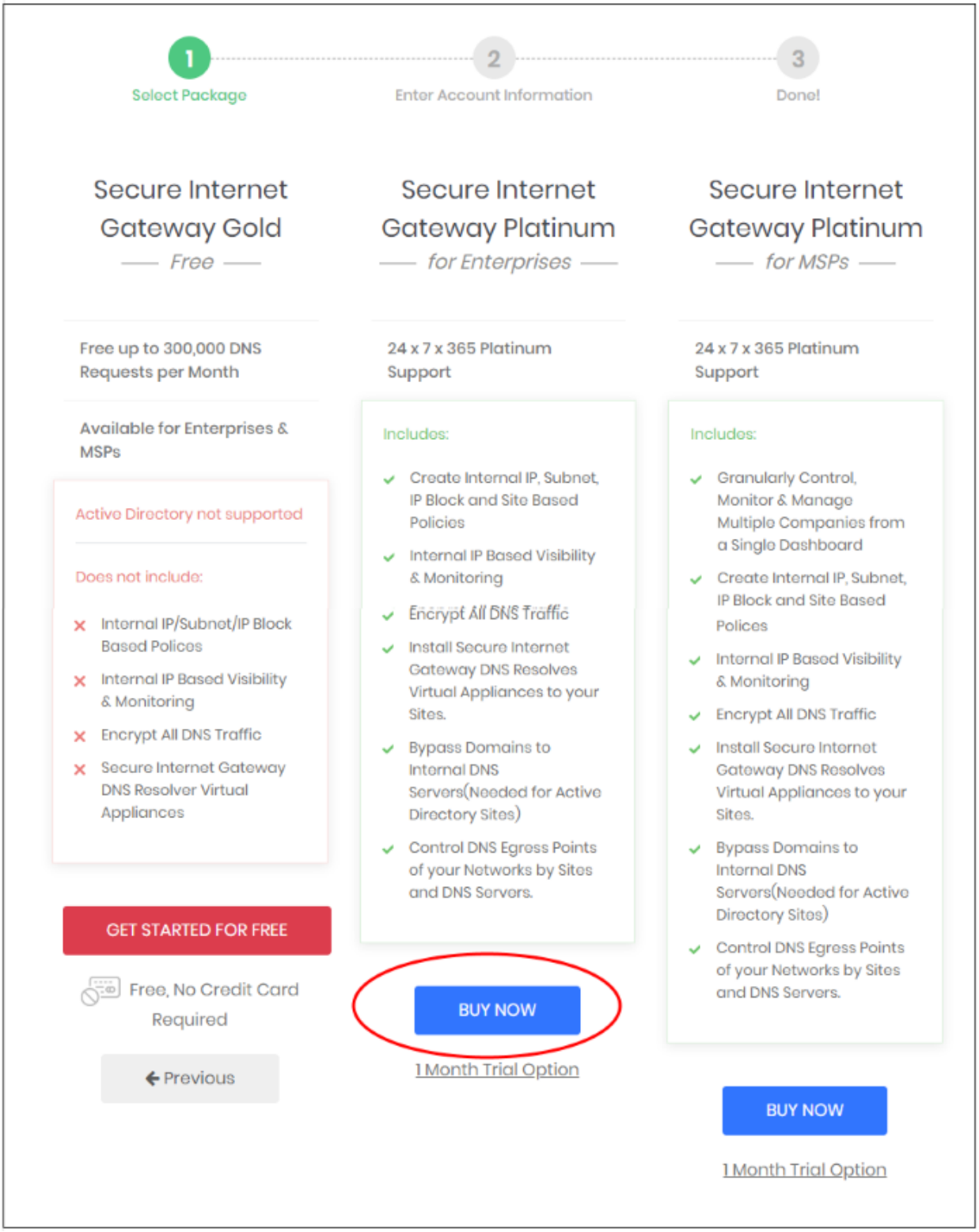
- Signup for a new license
- Upgrade a Gold license - Existing customers can upgrade their license from the CSIG interface. Open Secure Internet Gateway > Click 'Account' > Click 'Buy'

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

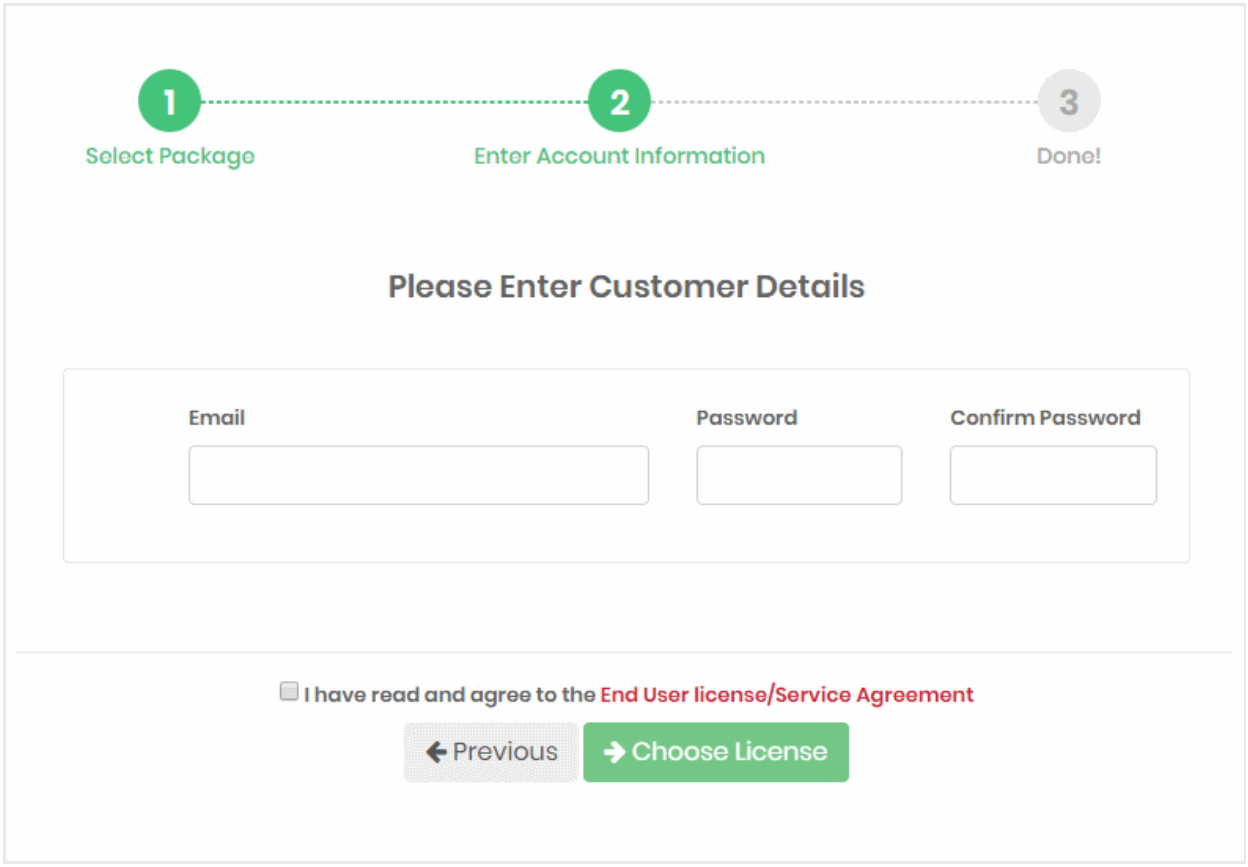
- Visit **https://cdome.comodo.com/dns-internet-security.php**.
- Click 'Start Now'
- You are taken to the sign-up page:



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



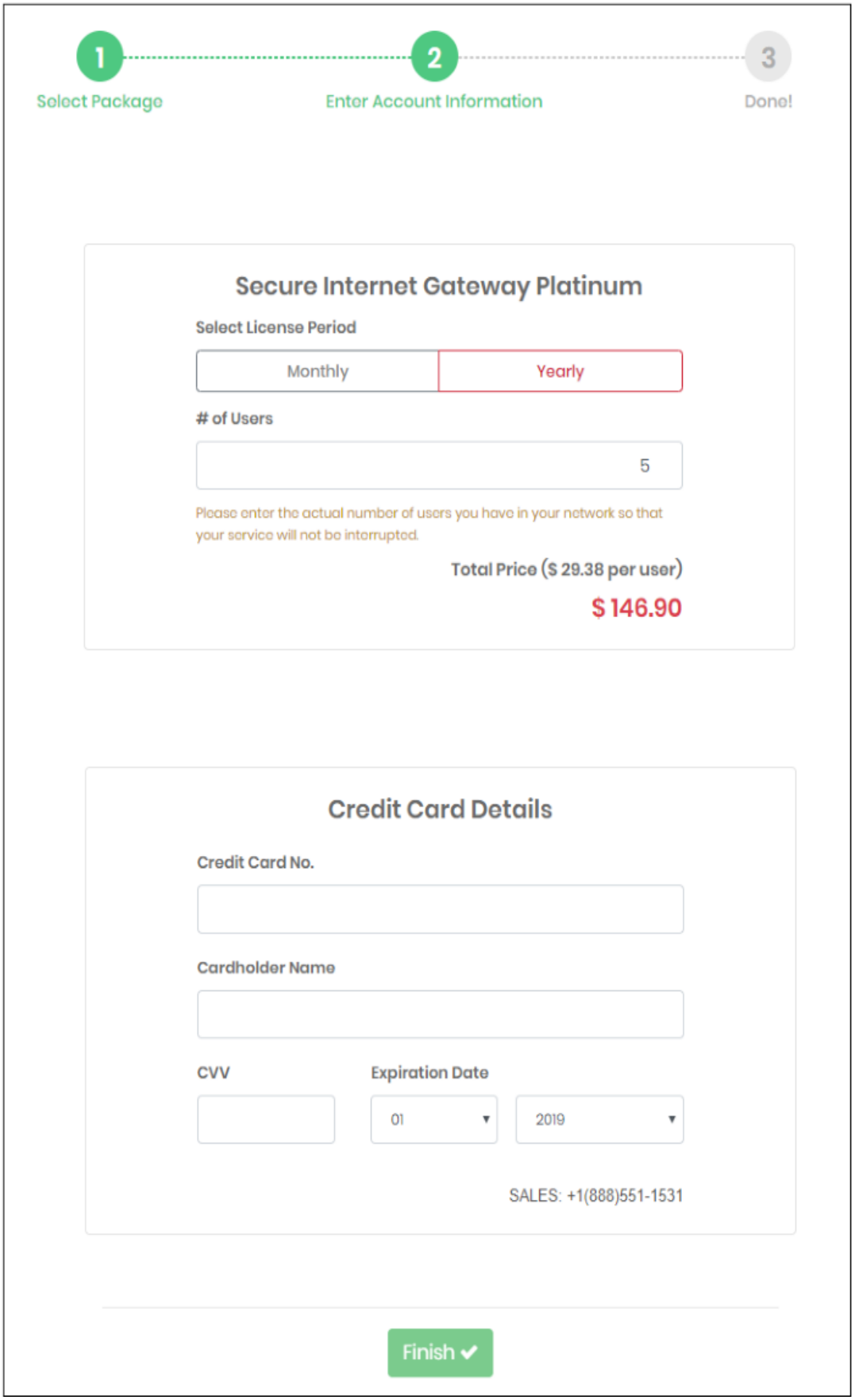
- Click 'Buy Now' under 'Secure Internet Gateway Platinum for Enterprises'
- The next step is to provide your account details and accept the end user license agreement.



- **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. Please use at least 8 characters, and a mix of upper and lower letters, numbers, and special characters. This also serves as your password for your Comodo account (**accounts.comodo.com**)
- **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:



- **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**.

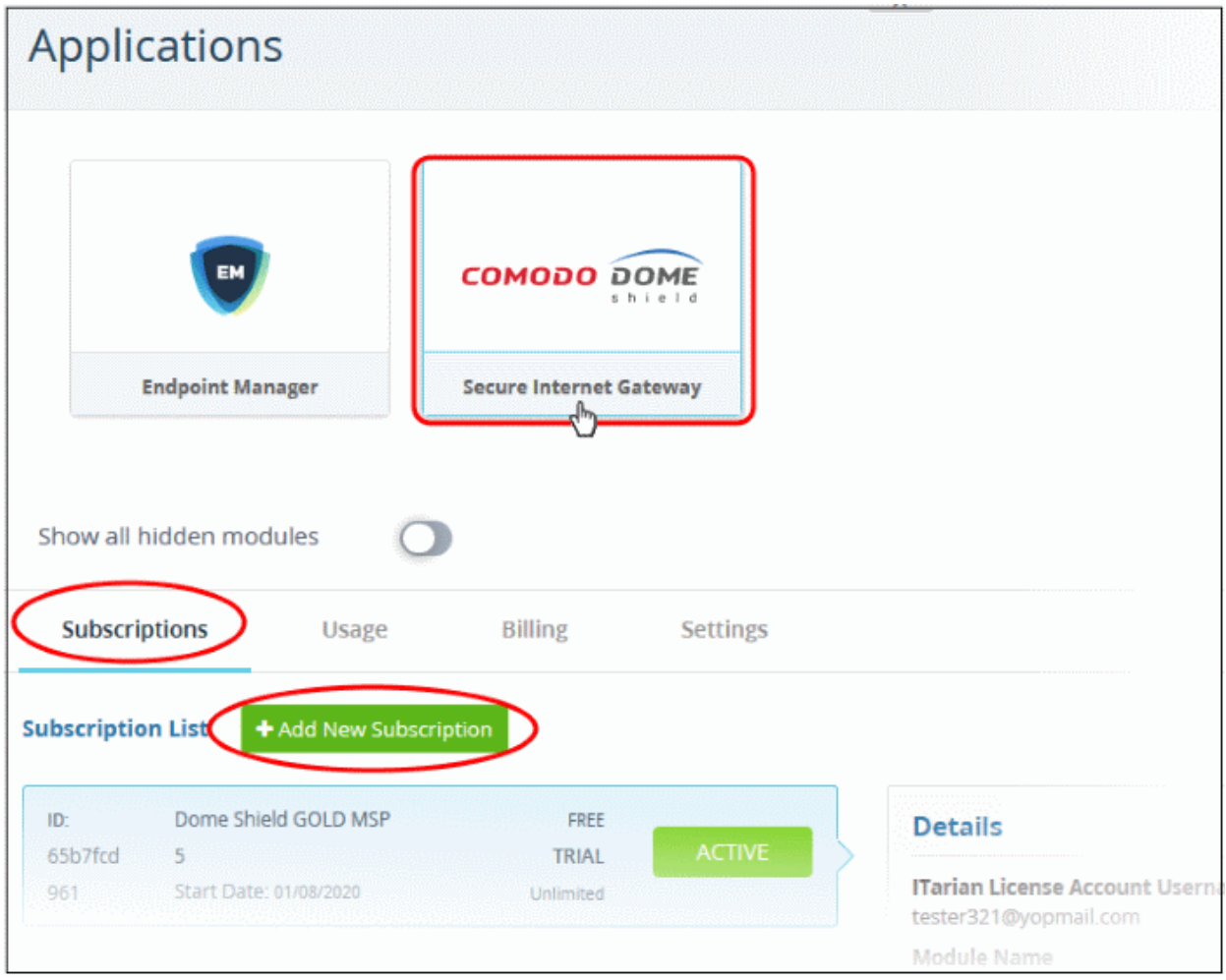
Comodo One / Dragon and ITarian Customers

- 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 enroll for a C1 / Dragon / ITarian account.

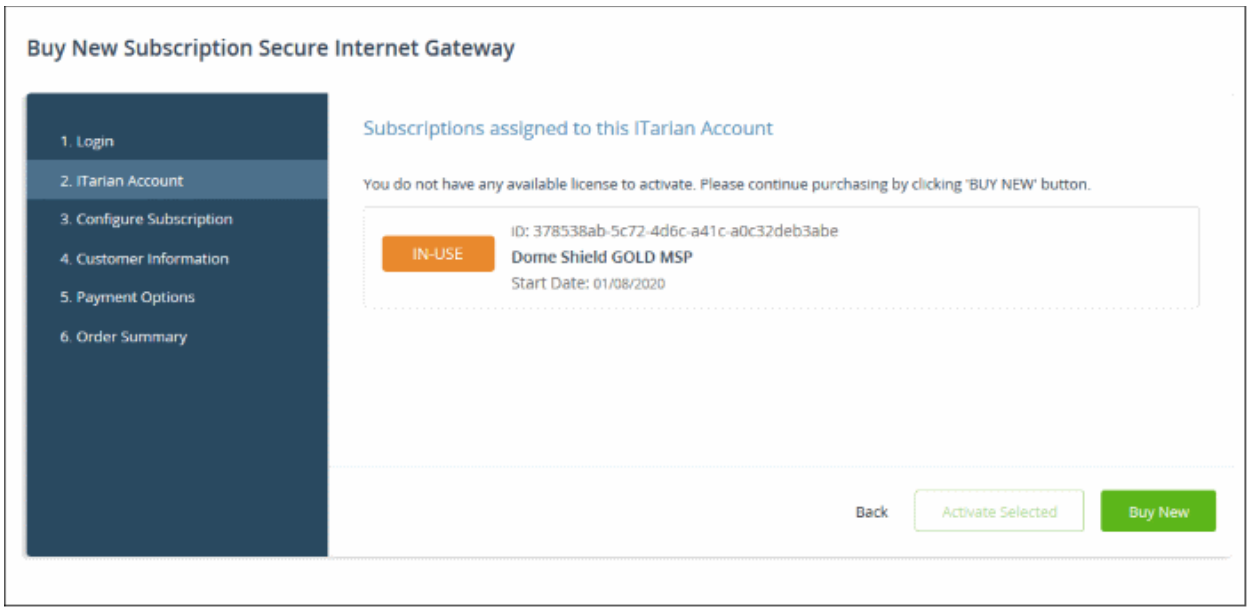
Upgrade to a Platinum license

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

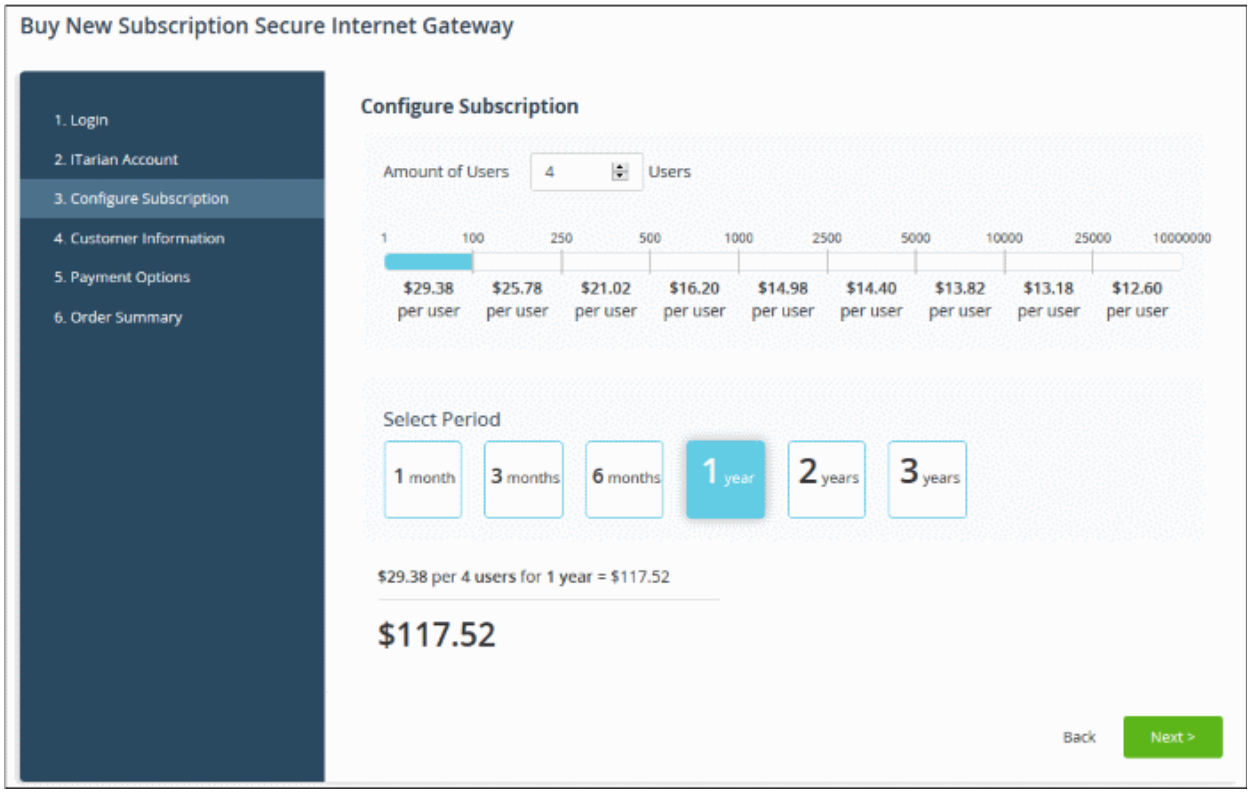


- The account username is pre-populated.
- Enter your C1 / Dragon / ITarian password then click 'Login'

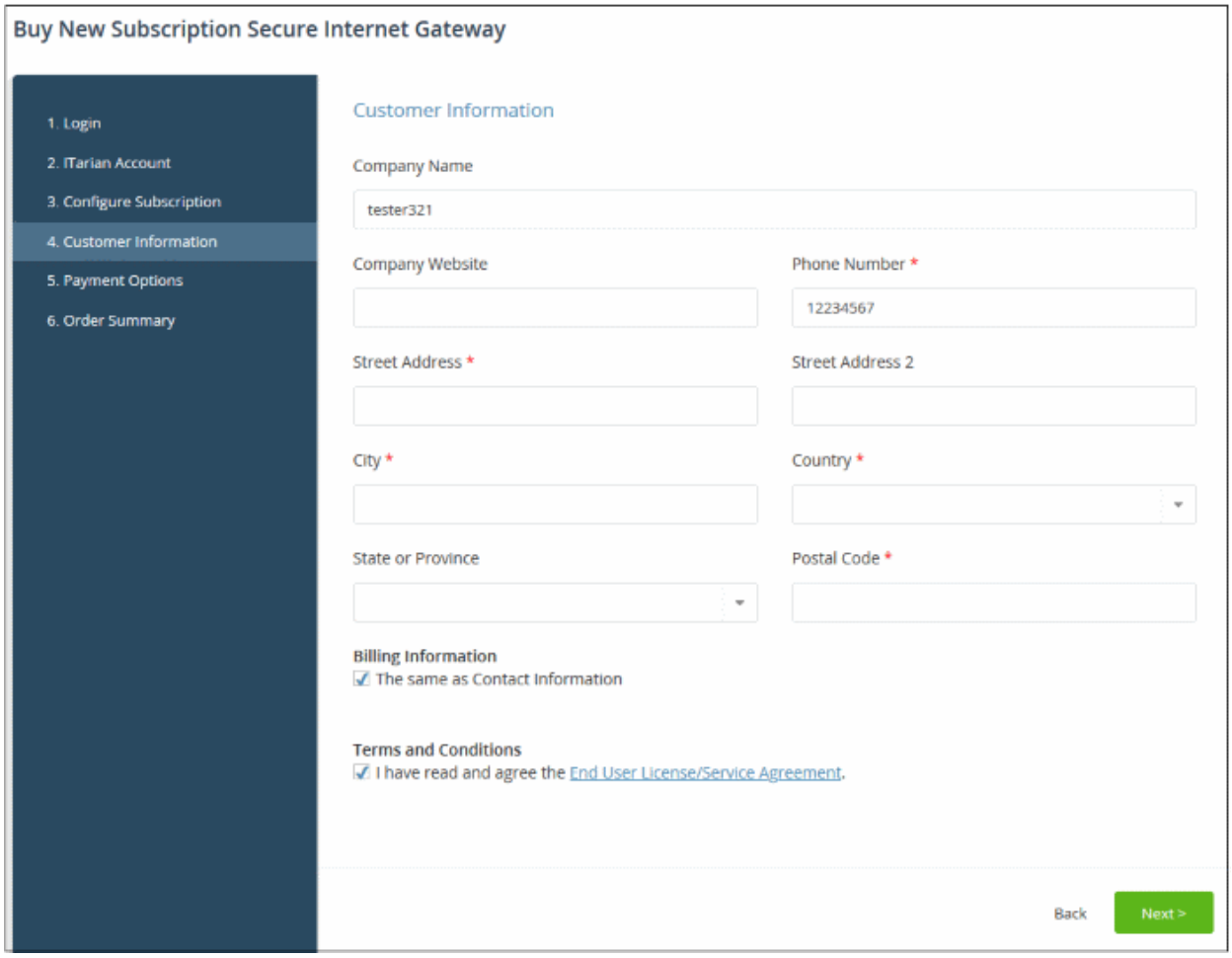
- **Activate Selected** – Activate Platinum licenses that you have purchased via your Comodo Accounts Manager (CAM) account. Activation will allow you to access CSIG via the C1 / ITarian / Dragon interface.
- **Buy New** - Purchase a new Platinum license.



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

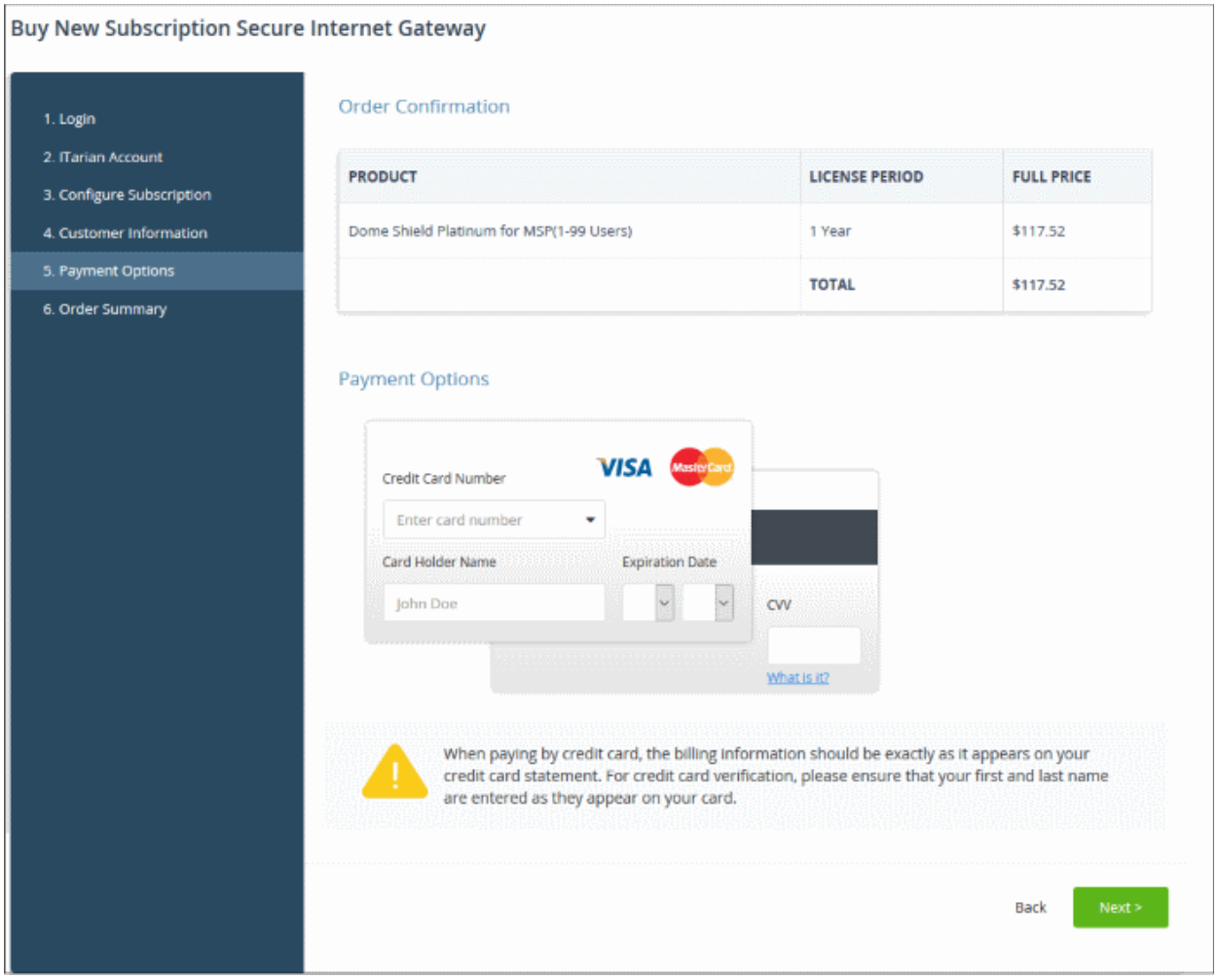


- Click 'Next' and complete the customer information form.



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

- Complete your payment details



- Click 'Next' to place your order. Your license will be added to your account.
- Next, activate the license as follows:
  - 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 interface will show all your purchased CSIG licenses.
  - Select the new license and click 'Activate Selected'.

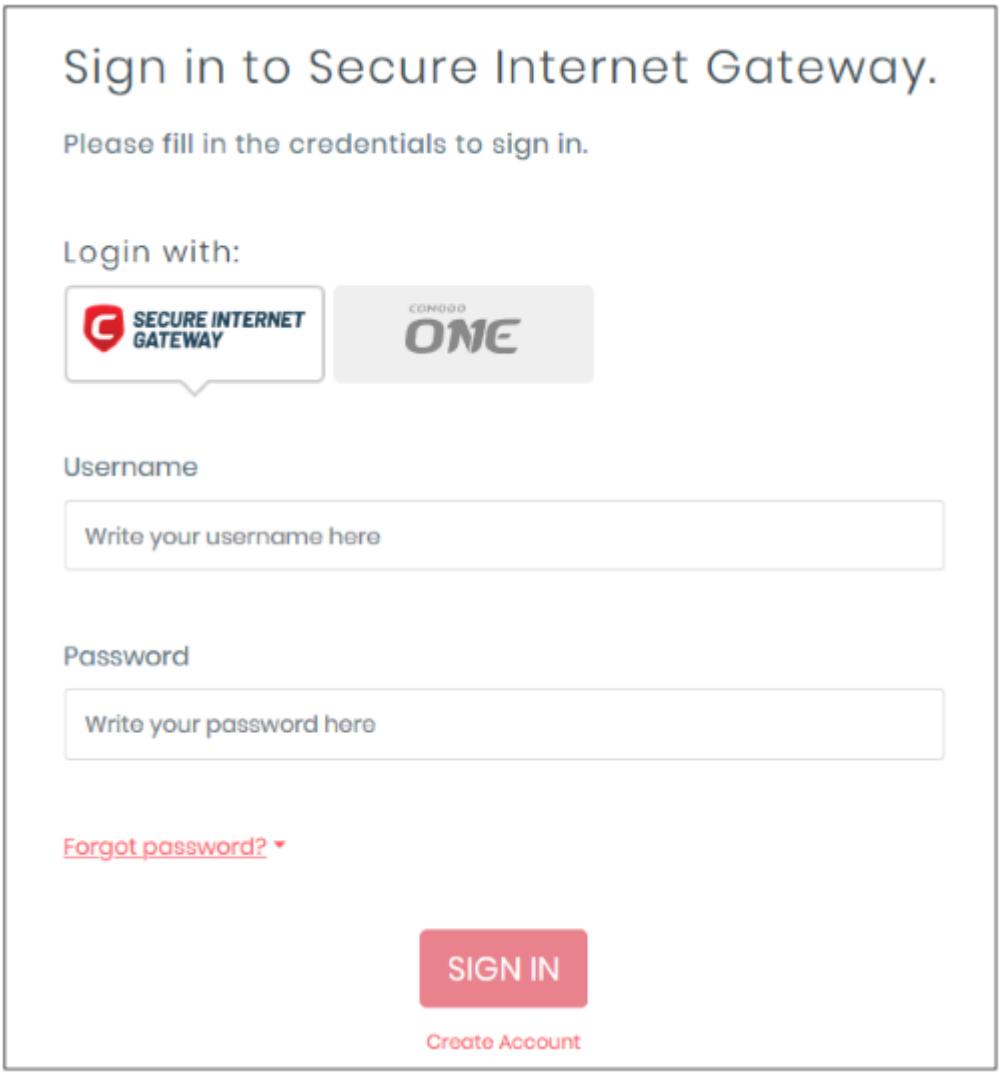
Login to Secure Internet Gateway

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/**.

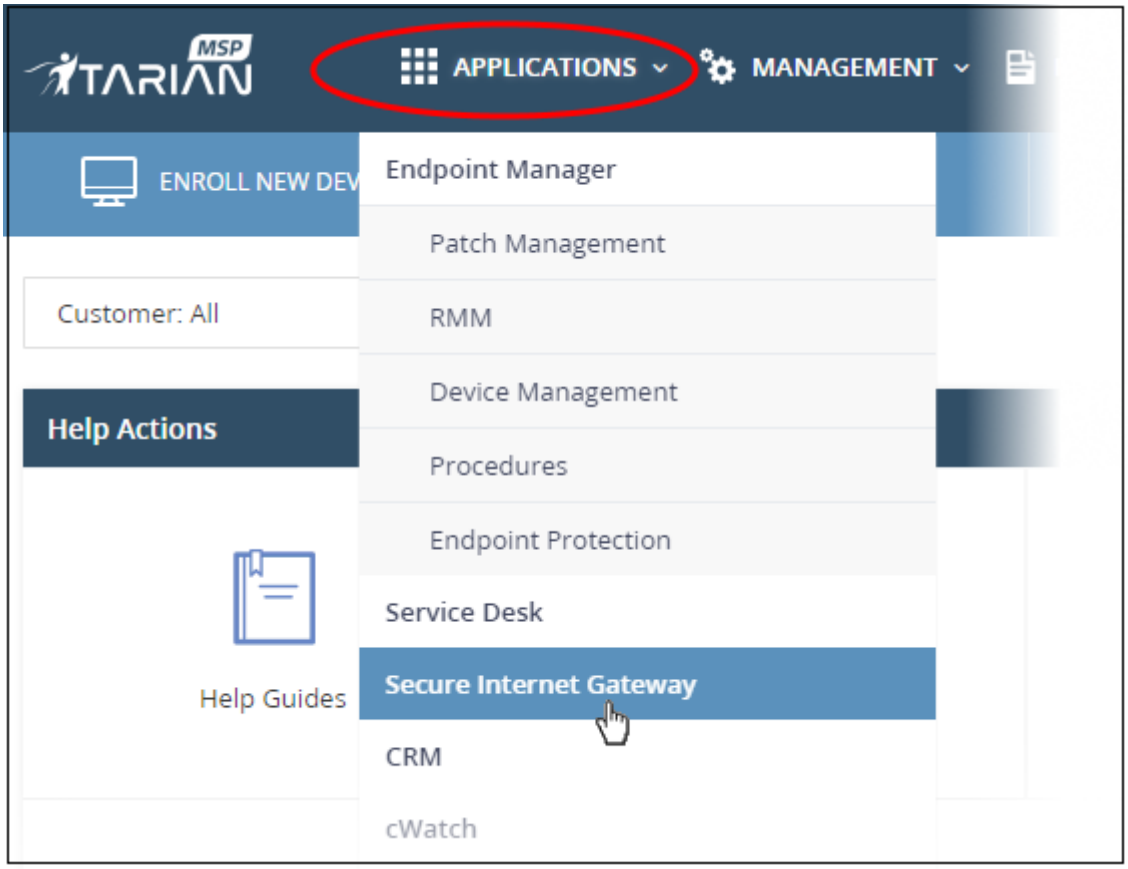
- Login at **https://shield.dome.comodo.com/login** and select 'Secure Internet Gateway'



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

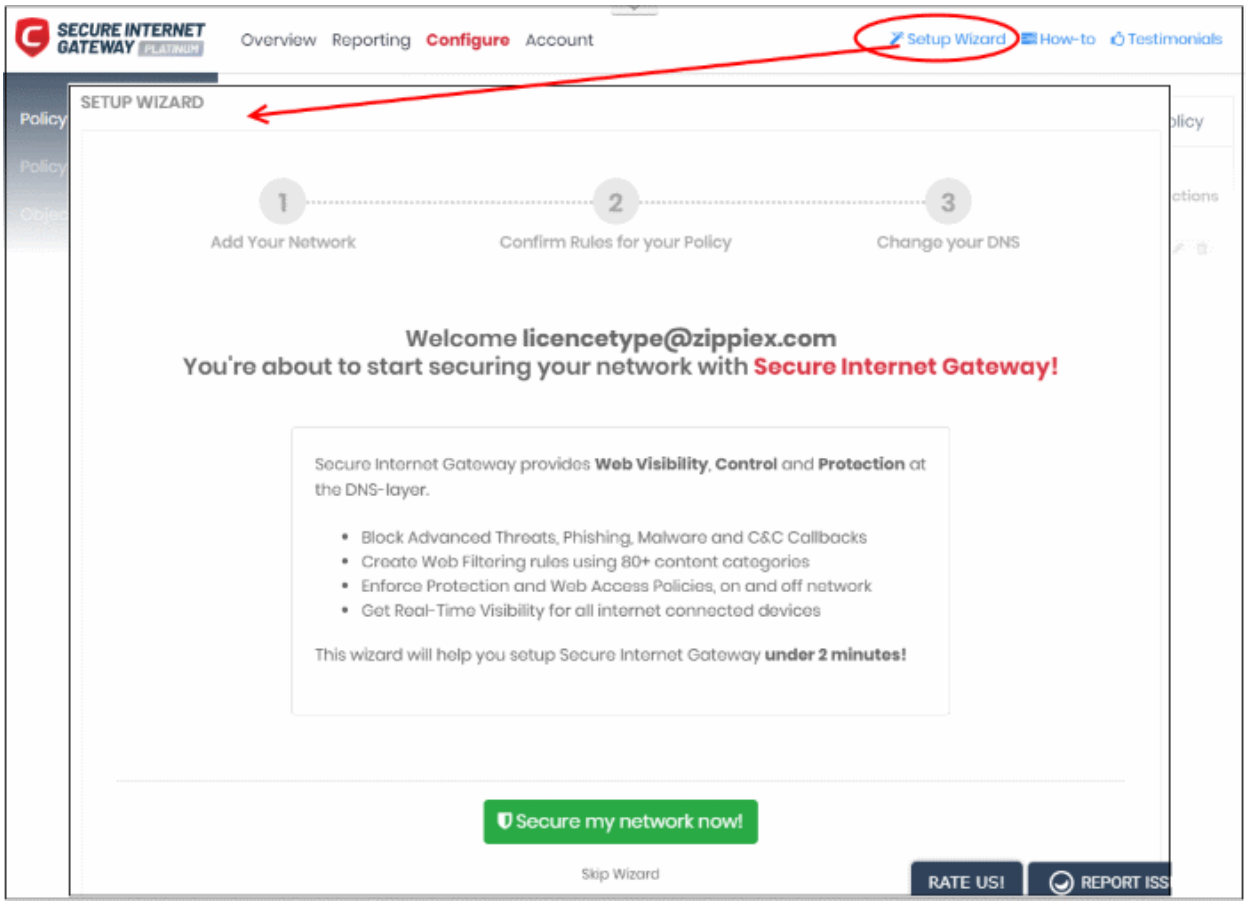
Comodo One / Dragon / ITarian Portal

- 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.



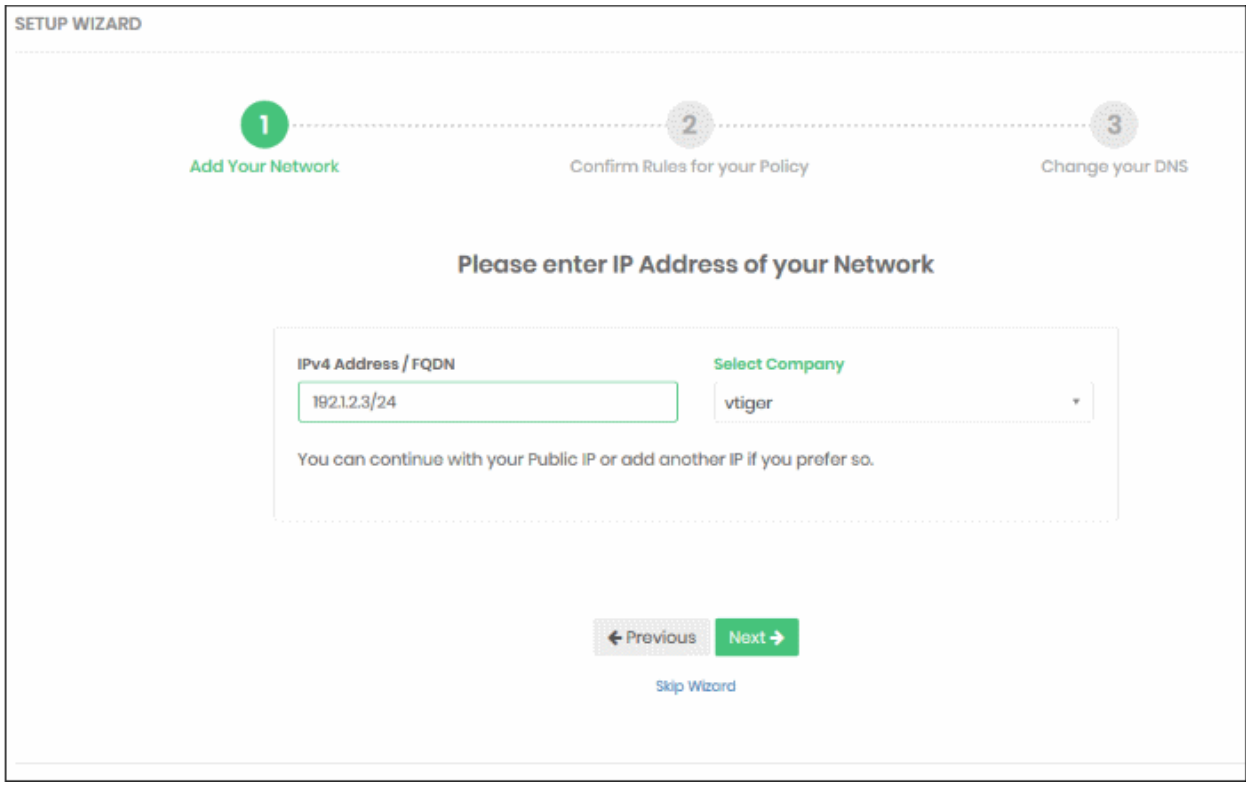
Step 2 - Add Your Network

- 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.

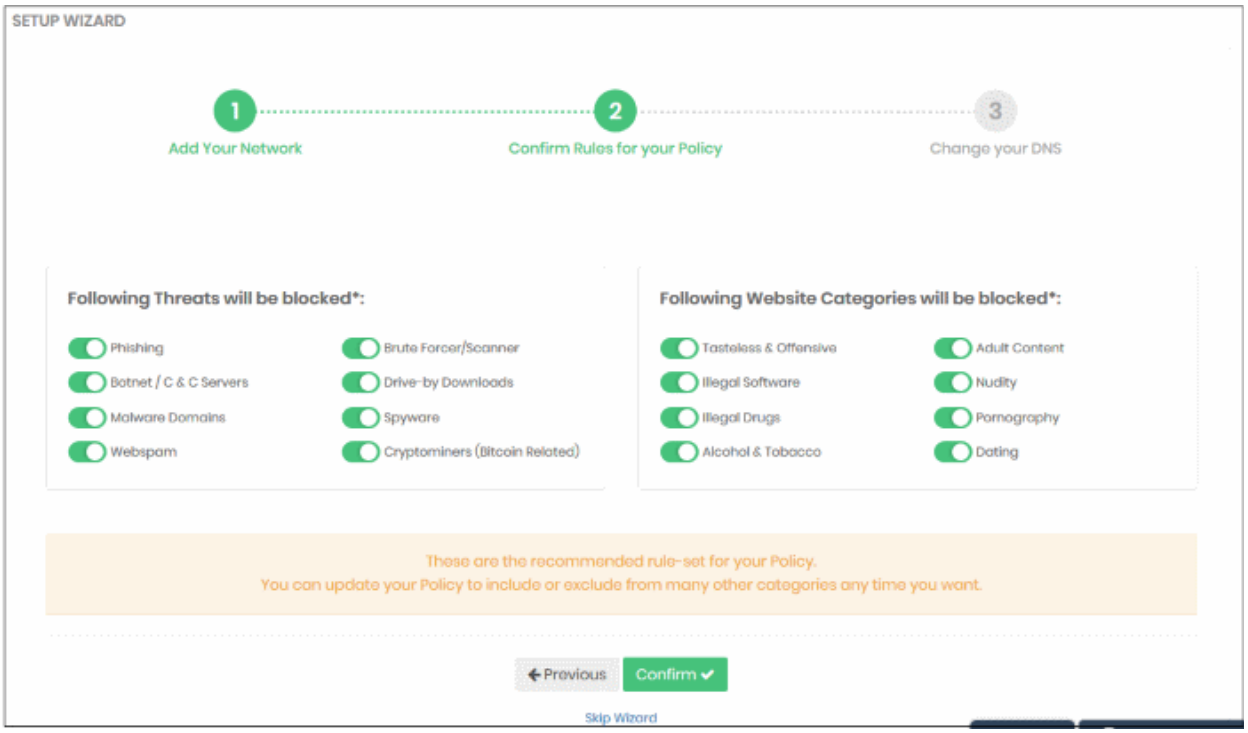
- If required, you can change this to the IP of a different network you want to protect. Enter the fully qualified domain name or the network IP address in CIDR format. Secure Internet Gateway accepts prefixes from /24 to /32.
- Any IP you add here is automatically activated for protection. You need to change the network's DNS settings to Secure Internet Gateway, as explained in '**Change your DNS Settings**'
- 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. Choose the customer organization for which you want to enroll the network.

Click 'Next' to configure rules for the policy.

Step 2 - Configure Rules for your Policy

This steps explains how to set up security and website category rules for your policy. These rules will be applied to your network on enrollment.



- All rules are enabled by default. You can enable / disable rules as required.
- If you are unsure, then a good rule of thumb is to just leave everything enabled. This gives you maximum protection, and you can always modify the rule later if there are issues.
    - You can modify the policy later by clicking 'Policy Settings' in the left menu. See '**Manage Security Rules**' and '**Manage Category Rules**' if you need help with these areas.

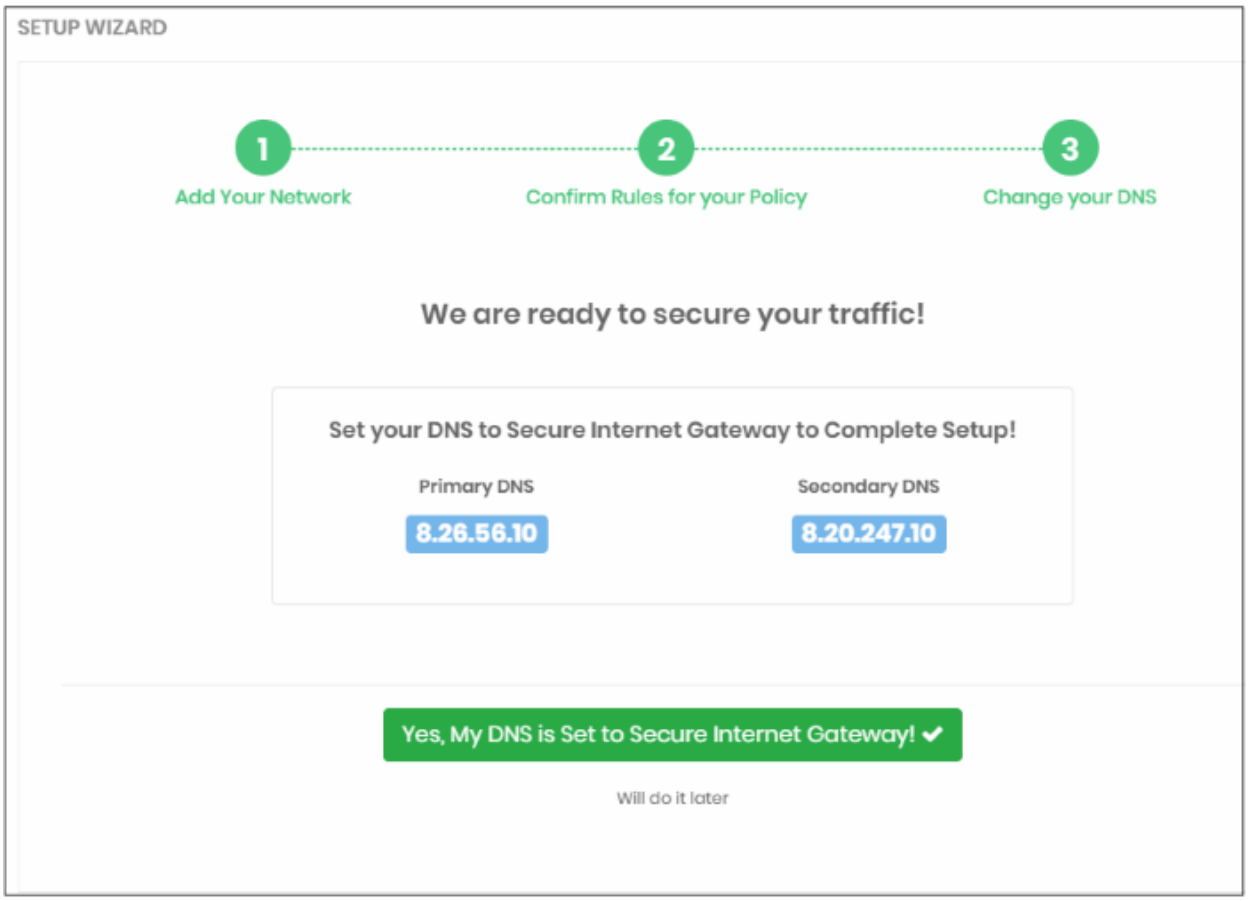
Click 'Confirm' to apply your policy.

Step 3 - Change your DNS Settings

You need to point the network's DNS settings to the following CSIG servers:

- 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:



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

- Networks added via the wizard above are labeled 'My Network', with the date appended to the label.
- Click 'Configure' > 'Objects' > 'Networks' to see all networks that you have added.
- You can also skip the setup wizard and add networks, roaming and mobile devices manually later on. See **Step 3**.
- 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.

Step 3 – (Optional) Enroll Additional Networks and Devices

You can enroll multiple fixed networks and mobile/roaming devices to Secure Internet Gateway.

The following sections explain how to:

- **Enroll additional networks**
- **Enroll roaming devices**
- **Enroll mobile devices**

Enroll Additional Networks

The IP of the network from which you are connecting was added during initial setup (see **Step 2**). This network should already be active.

There are three ways you can enroll additional networks:

1. **Use the setup wizard:**

   - Click 'Setup Wizard' at the top-right of the interface.
   - Follow the steps to add your networks.
   - See **Step 2** for help with the wizard.

2. **Manually add a network:**

   - You can add networks with static IP addresses by specifying their IP address in CIDR notation.
   - You can add networks with dynamic IP addresses by installing our IP updater agent on the network.
   - See **Add Networks Manually** for help with both these methods.

3. **Deploy local resolvers to import a network:**

   - Install a local resolver (LR) as a virtual appliance on the network.
   - Once deployed, the network is automatically imported to Secure Internet Gateway.
   - See **Import networks by deploying local resolvers** for help to setup the local resolvers.

Add Networks Manually

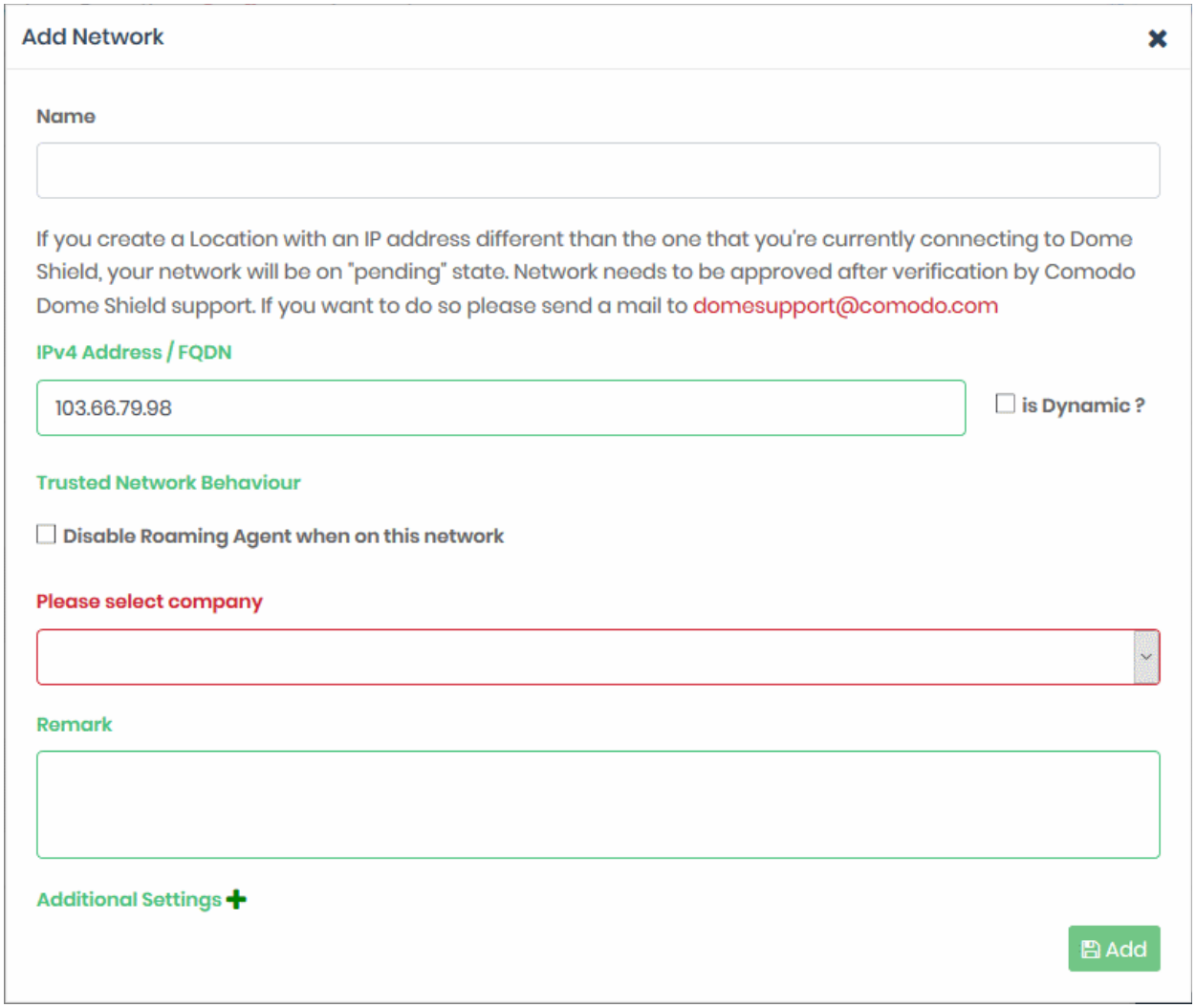
Networks you add manually have a 'pending' status until the IP/FQDN has been approved by Comodo. Please contact your Comodo account manager or **domesupport@comodo.com** if you have questions on this.

Click the links below for help

- **Add Networks with Static IP Addresses**
- **Add Networks with Dynamic IP Addresses**

Add Networks with Static IP Addresses

- Click 'Configure' > 'Objects' > 'Networks'
- Click 'Add New Network'
- Complete the new network form:



Field	Description
Name	Create a label for the network
IP Address / FQDN	Type the IP or fully qualified domain name of the network you want to add. • Enter the IP address in CIDR (Classless Inter-Domain Routing) notation. • Secure Internet Gateway can accept network prefixes from /24 to /32. Any new network you add will have a 'pending' status until approved by Comodo. Dynamic - Select if you want to add a network with dynamic IP addresses. See **Add Networks with Dynamic IP addresses**
Trusted Network Behavior	**Disable Roaming Agent when on this network** – Decide whether or not the network policy is applied to roaming devices when inside the network. • Enabled - The agent is deactivated on roaming devices when they are inside the network. The network policy applies to the device. • Disabled - The agent is not deactivated. The roaming device's policy remains active even when inside the network.
Please select company	MSPs only • Select the customer organization for which you want to enroll the network.

Remark	Enter any notes, comments or advice about the network.
Additional Settings - These settings only apply to roaming devices which have the CSIG agent installed. • 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 roaming devices to reach internal domains. These settings are automatically deployed to the device's host file. • See '**Enroll Roaming Devices**' for more on CSIG agents.	
Host File Configuration	Enter the name and IP address of your host in the respective fields. Click the '+' button to add more host entries.

- Click 'Add' when done.

The network is saved and shown in the list. Next:

Configure your network DNS to forward queries to CSIG DNS

You need to change the network's DNS to forward queries to CSIG DNS. This ensures all endpoints are protected.

Change your DNS addresses to the following:

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

General Notes:

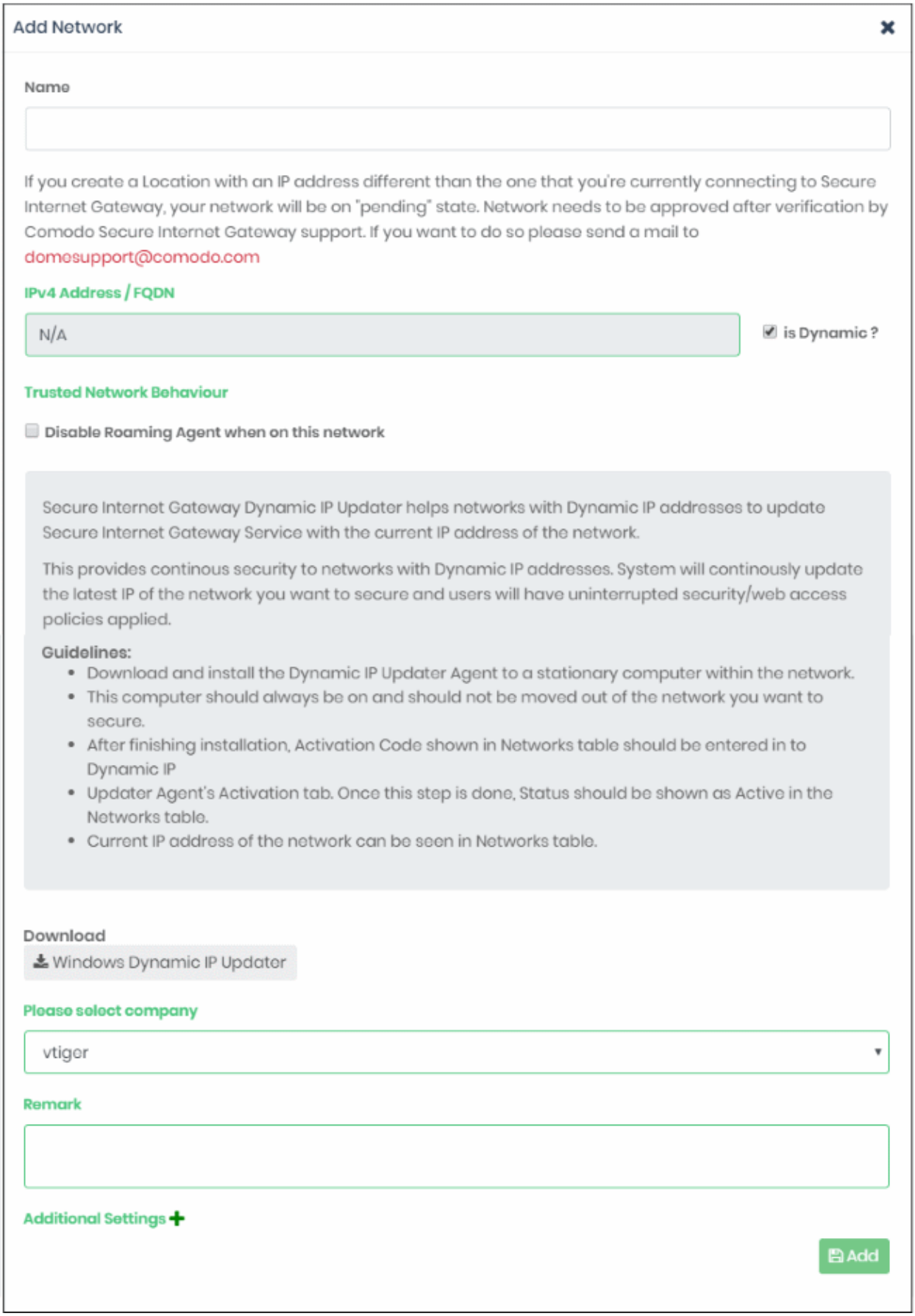
- You need to add internal domains to the host files of endpoints inside the network. This is because CSIG DNS cannot resolve internal domains.
- For roaming endpoints with the CSIG agent, internal domains can be configured in 'Add/Update Network' > '**Additional Settings**' > 'Host File Configuration' field
- Any additional networks you add need to be approved by Comodo before you can manage them.
- By default, no rules are applied to new networks. You need to apply a policy to them. See '**Step 5 - Create and Apply Security Policies**' for help with 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':



Field	Description
Name	Create a label for the network

IP Address / FQDN / Dynamic	Enable 'Is Dynamic?' to enroll a network with dynamic IP addresses. A message box opens with help to enroll the network. • Click 'Windows Dynamic IP Updater' in the message box and save the agent setup file.
Trusted Network Behavior	**Disable Roaming Agent when on this network** - Decide whether or not the network policy is applied to roaming devices when inside the network. • Enabled - The agent is deactivated on roaming devices when they are inside the network. The network policy applies to the device. • Disabled - The agent is not deactivated. The roaming device's policy remains active even when inside the network.
Please select company	MSPs only • Select the customer organization for which you want to enroll the network.
Remark	Enter any notes, comments or advice about the network.
Additional Settings - These settings only apply to roaming devices which have the CSIG agent installed. • Roaming devices cannot connect to internal hosts when inside the office network. This is because CSIG DNS is an external DNS which can't resolve internal domains. • Configure the 'Host File' fields to allow roaming devices to reach internal domains. These settings are automatically deployed to the device's host file. • See '**Enroll Roaming Devices**' for more on CSIG agents.	
Host File Configuration	Enter the name and IP address of your host in the respective fields. Click the '+' button to add more host entries.

- Click 'Add' once you have completed the form.

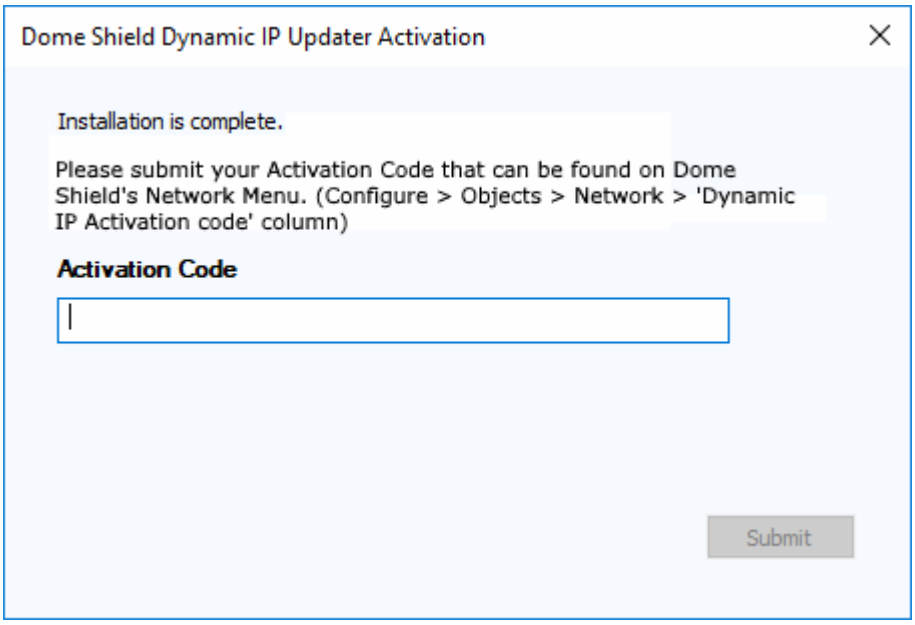
The network is added to CSIG with a status of 'Pending'. An activation code is also created for the network:

- Copy the agent setup files to an endpoint in the target network
- Install the agent on the target endpoint.

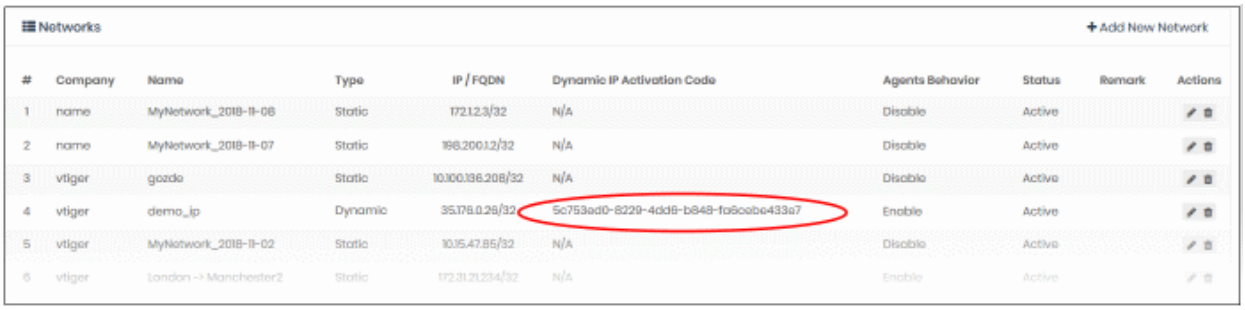
Note: Choose an endpoint which is always powered on and connected to the network. This lets the agent monitor IP address changes and send updates to Secure Internet Gateway.

Step 2 - Activate the agent

After installing the agent, you need to enter the network's activation code to enable protection:



- Click 'Configure' > 'Objects' > 'Networks' to get the code:



- Paste the code and click submit

The network is now activated.

Note – No security policy is applied to new networks by default – you need to create/apply your own policy. See **Step 5 - Create and Apply Security Policies** for help with this.

Import networks by deploying local resolvers

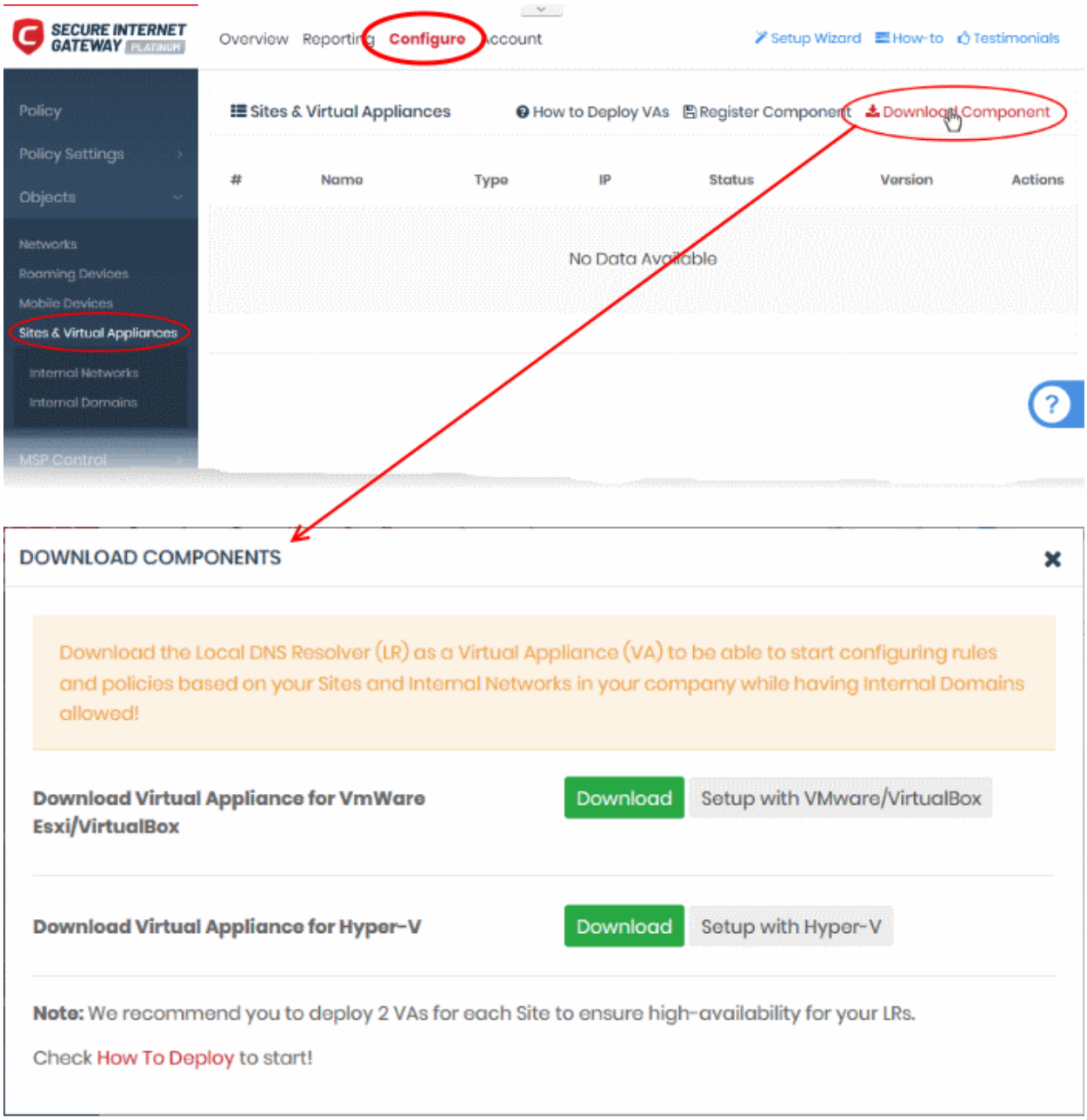
- The local resolver virtual machine (VM) is an alternative way to import networks. The feature is only available with Platinum licenses.
- The resolver is deployed as a VM on your network and will forward public DNS queries to CSIG DNS servers.
- The network is automatically imported to CSIG after you deploy the resolver.
- The resolver method offers some key advantages over 'direct' enrollment:
  - 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, giving you insight into the browsing patterns of endpoint users.
  - You can apply different policies to internal IP addresses and sub-nets, giving you granular control over the network.
  - 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 IP address.
  - Local resolver VMs require minimal hardware (only one CPU and 1GB of RAM) to process millions of DNS queries.

Follow the steps below to install the LR VA and import a network:

- **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

- Click 'Configure' > 'Objects' > 'Sites & Virtual Appliances'
- Click 'Download Component' at top-right



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

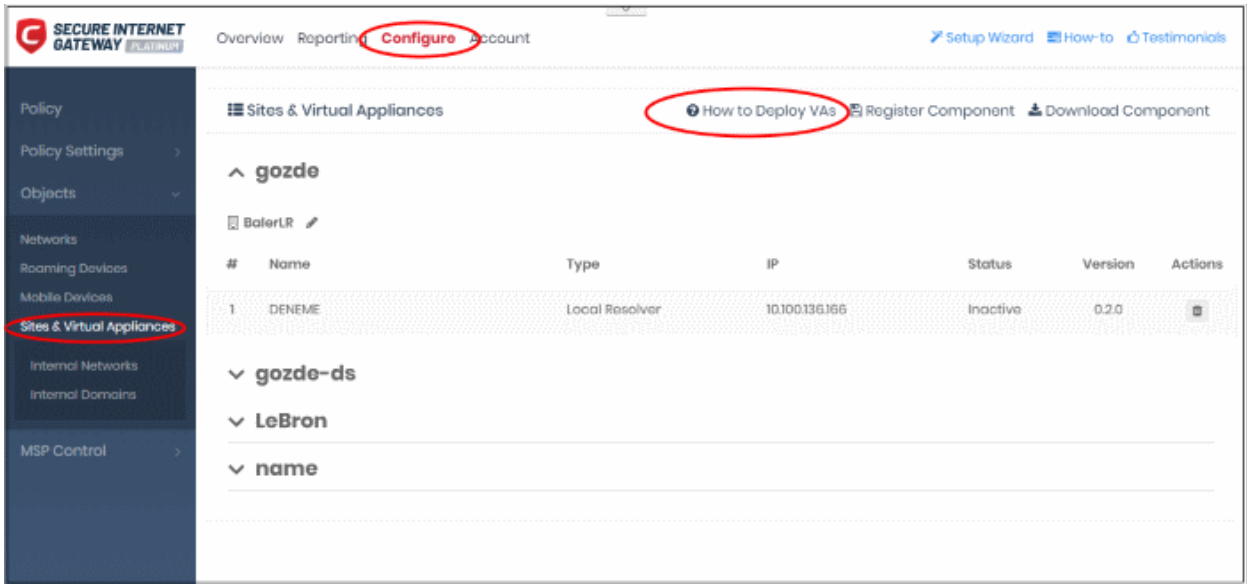
- Click the 'Download' button beside the VM application you want to use
- The setup package contains an OVA or HYPER-V file depending on the VM you chose. The package also contains a text file with login credentials to access the appliance.

Step 2 - Setup the Master Virtual appliance

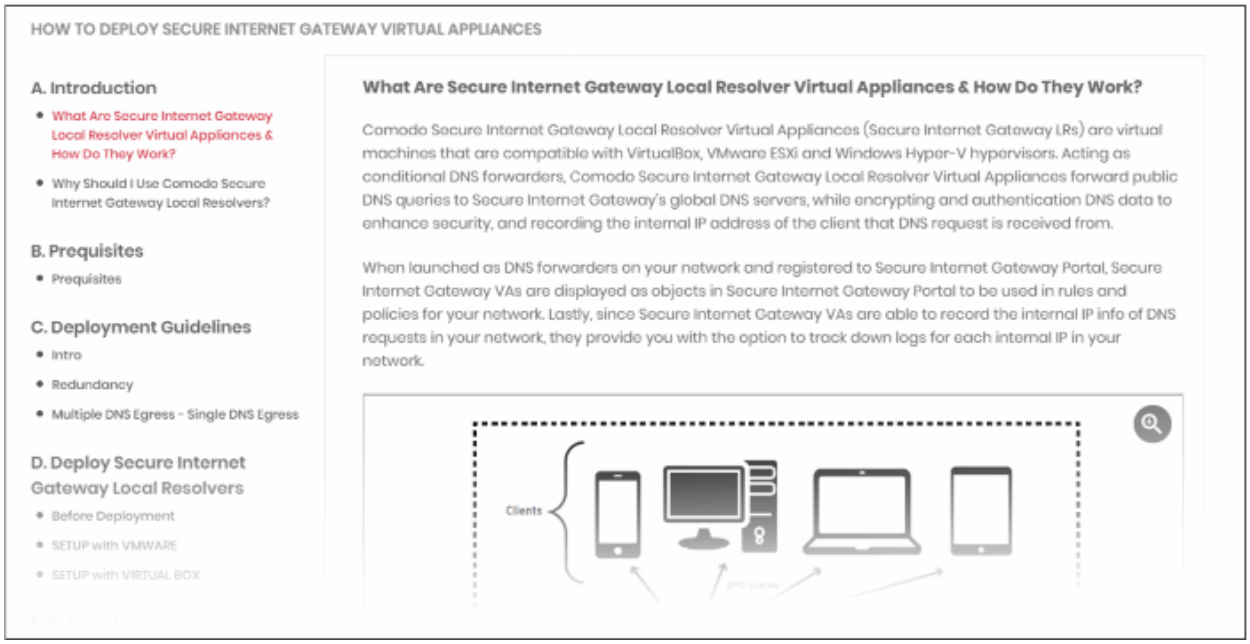
- Copy the package to the hosts on which you want to setup the appliance.
- Extract the package.
- Install the virtual appliance.

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'

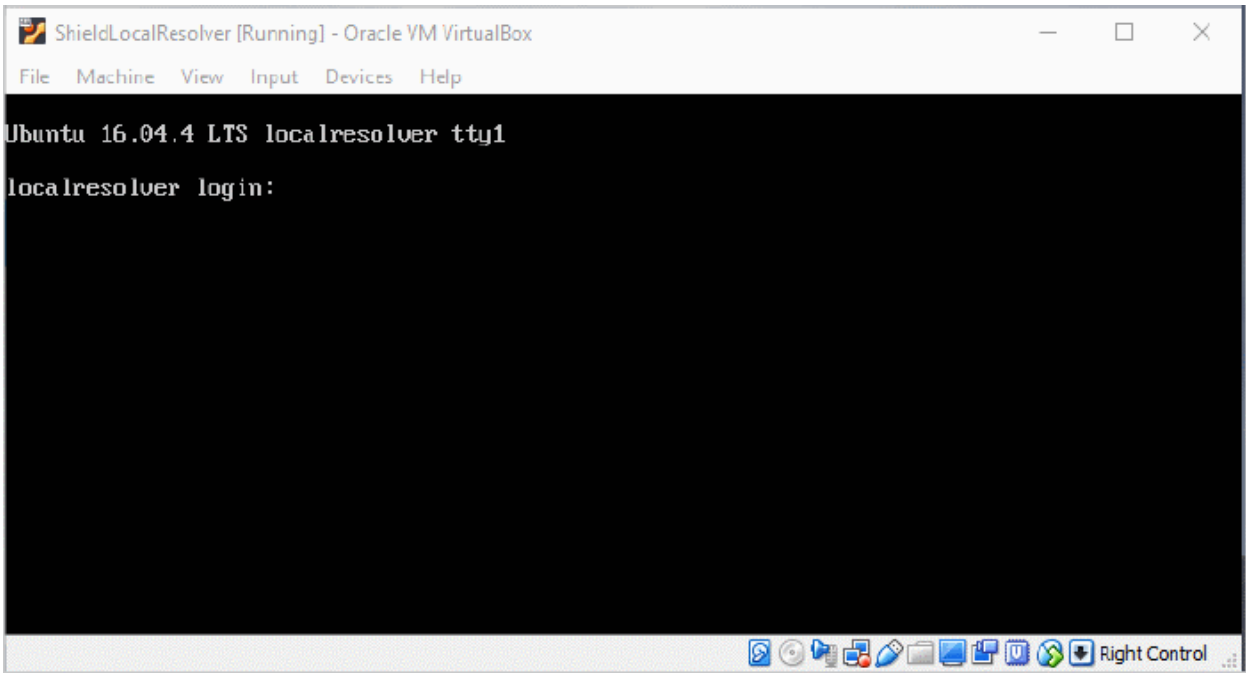


The instructions page explains how to install the VA on VMWare, VirtualBox and Hyper-V:

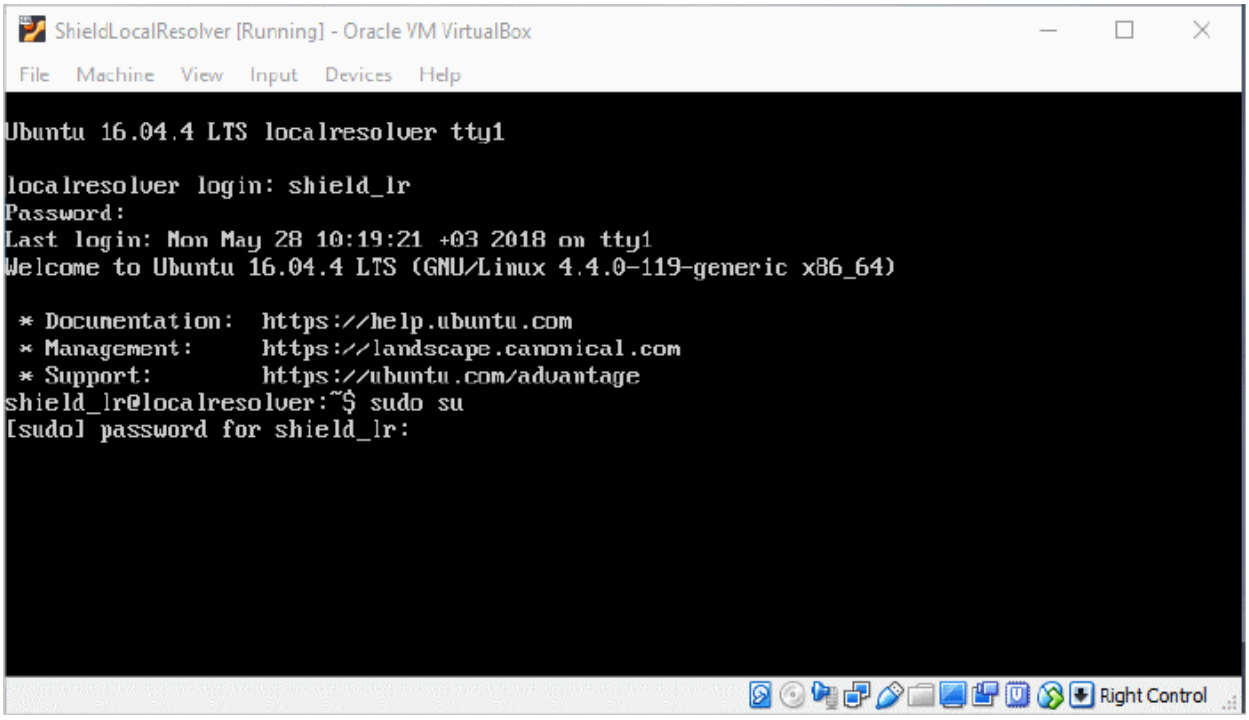


Configure the Local Resolver

- Start up the VA once installation is complete.

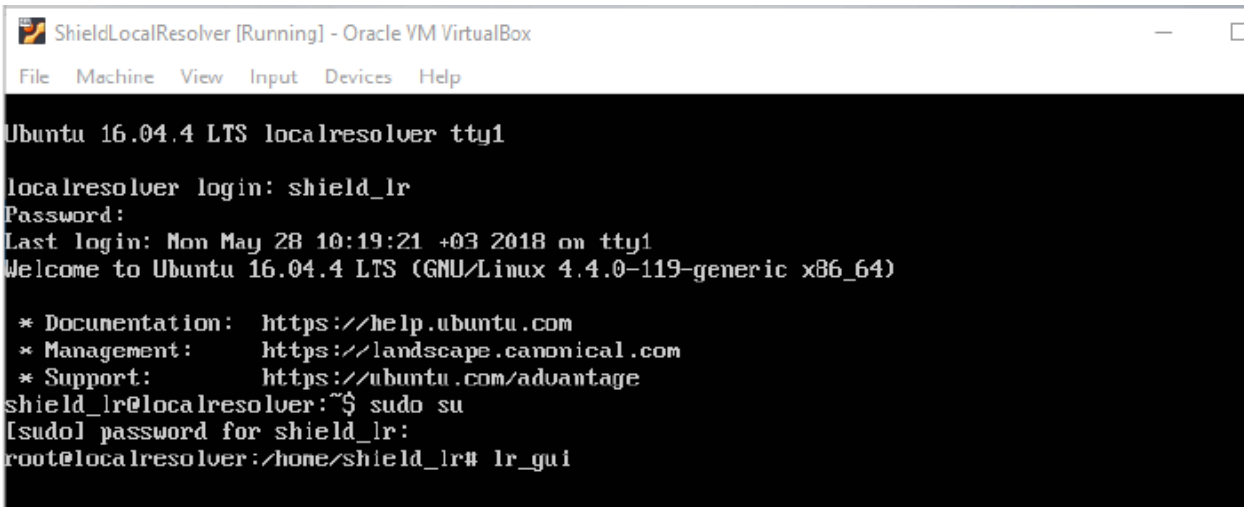


- Login to the appliance with the username and password in 'credentials.txt'. This file is in the VA package you downloaded.

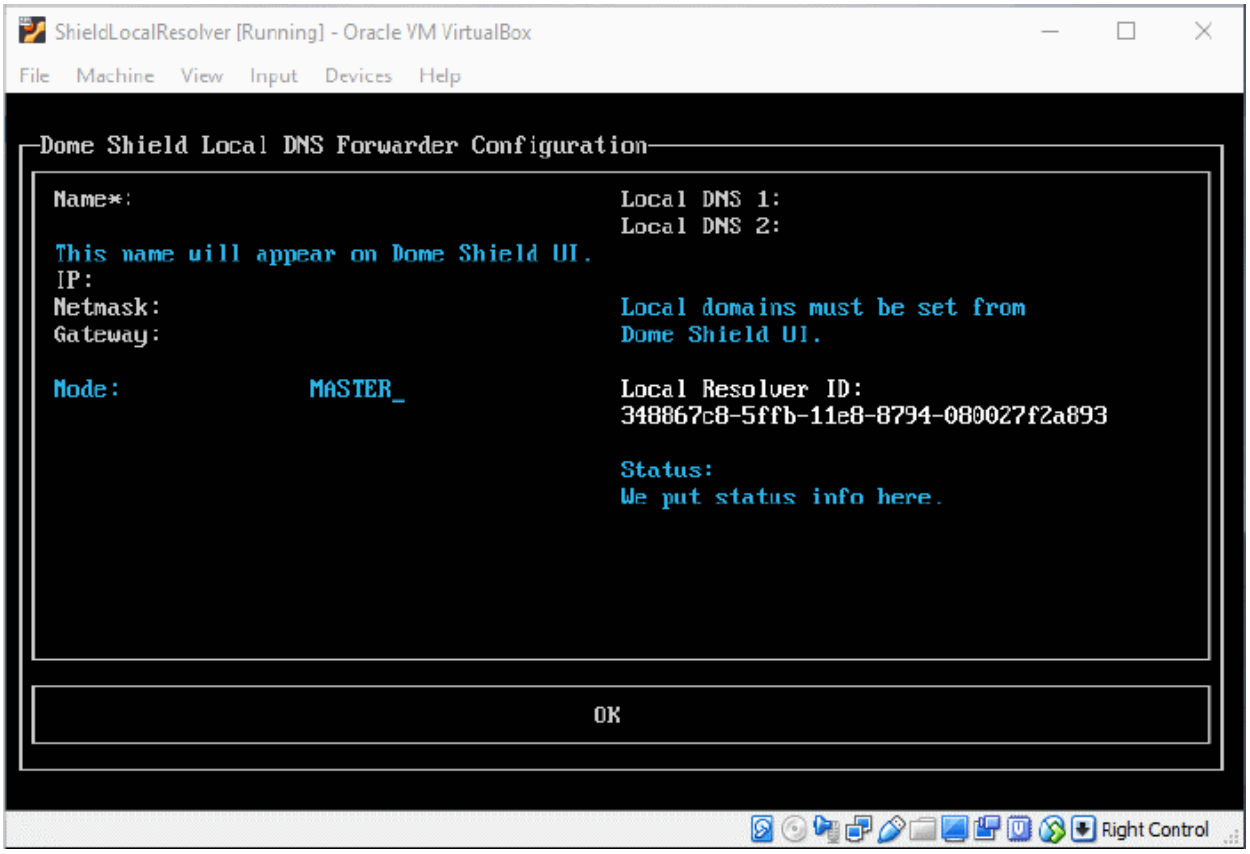


- Run the 'sudo su' command and enter the root password contained in 'credentials.txt'. This gives you root access.

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

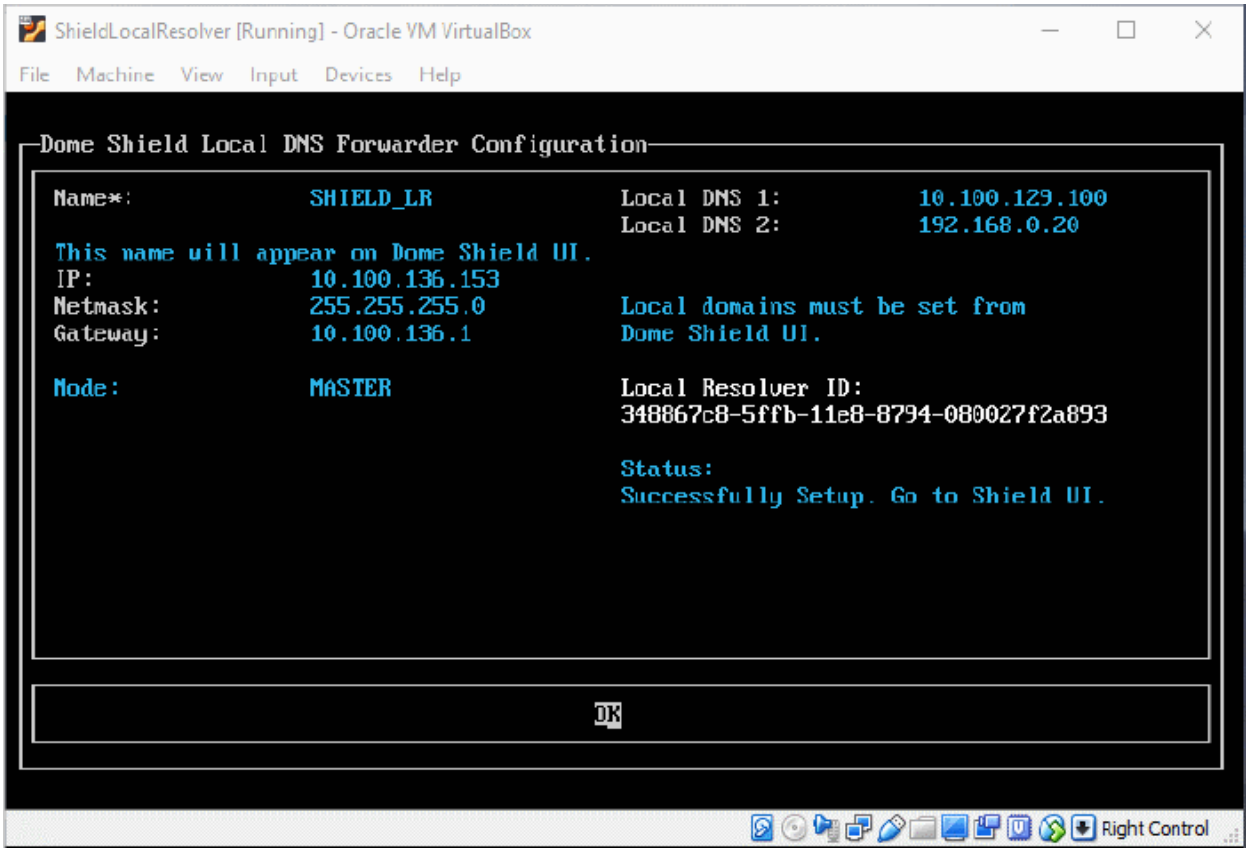


- Complete all fields in the forwarder configuration screen.
- Make sure to copy the 'Local Resolver ID' string. You need this to register the device later.



Field	Description
Name	Type a label to identify the master VA. This name will identify the VA in CSIG 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	**Note this ID string**. You need this to register the resolver in the next step.
Status	Progress of the VA setup process.

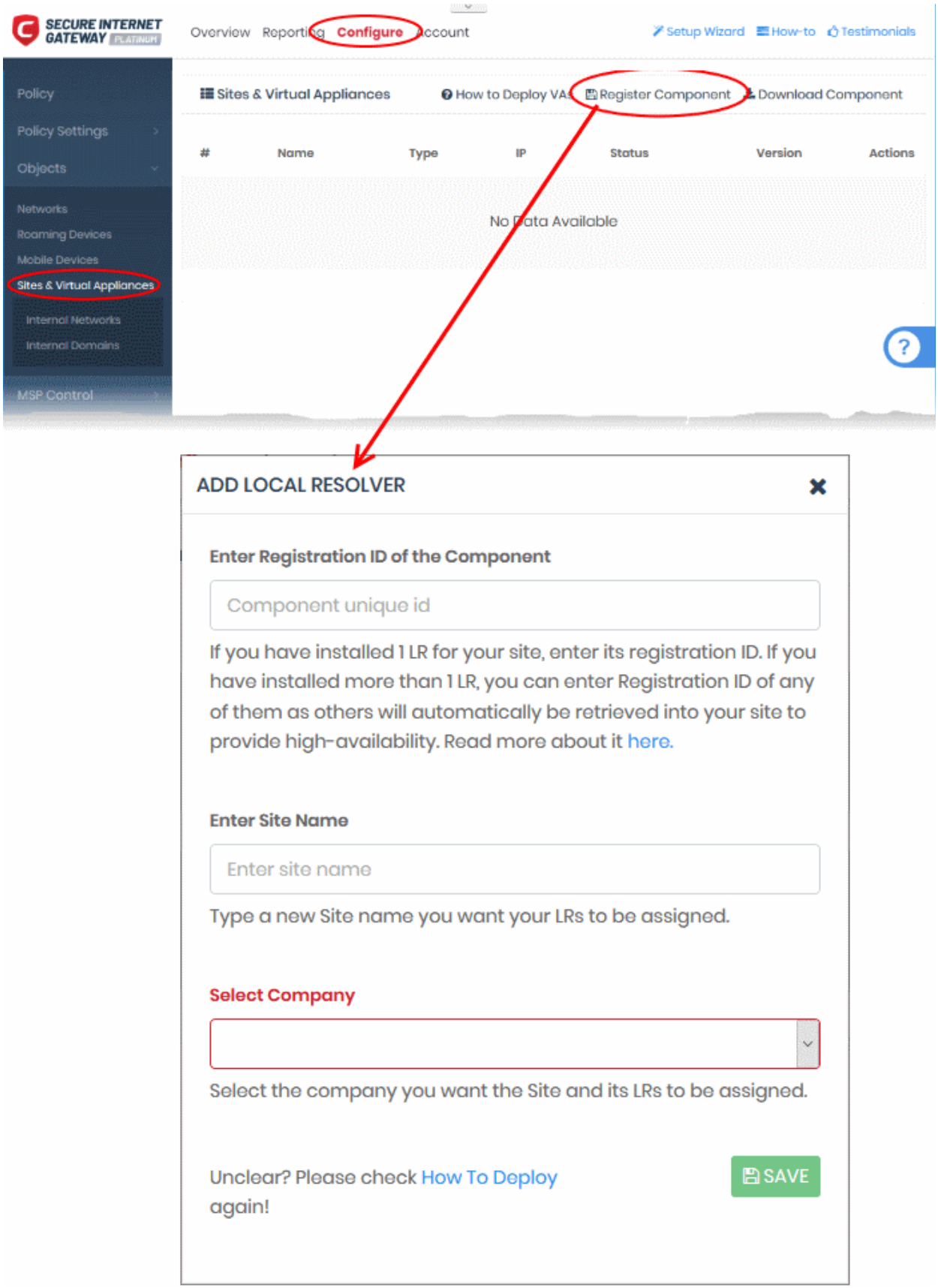
- Select OK then press 'Enter' when finished. Your configuration is saved.



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

Step 3 - Register the Master VA

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


SECURE INTERNET GATEWAY PLATINUM
Overview
Reporting
Configure
Account
Setup Wizard
How-to
Testimonials
Policy
Policy Settings
Objects
Networks
Roaming Devices
Mobile Devices
Sites & Virtual Appliances
Internal Networks
Internal Domains
MSP Control
Sites & Virtual Appliances
How to Deploy VA
Register Component
Download Component
Name Type IP Status Version Actions
No Data Available
ADD LOCAL RESOLVER
Enter Registration ID of the Component
Component unique id
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
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!
SAVE

Form Element	Description
Enter Registration ID of the Component	Paste the local resolver ID from the previous step. See the last screen in **Step 2 - Setup the Master Virtual appliance** if you missed this.
Enter Site Name	Create a label for the network you are about to import. The name is used to identify the network in the CSIG interface.
Select Company	MSPs only. • Choose the customer organization whose network you want to import

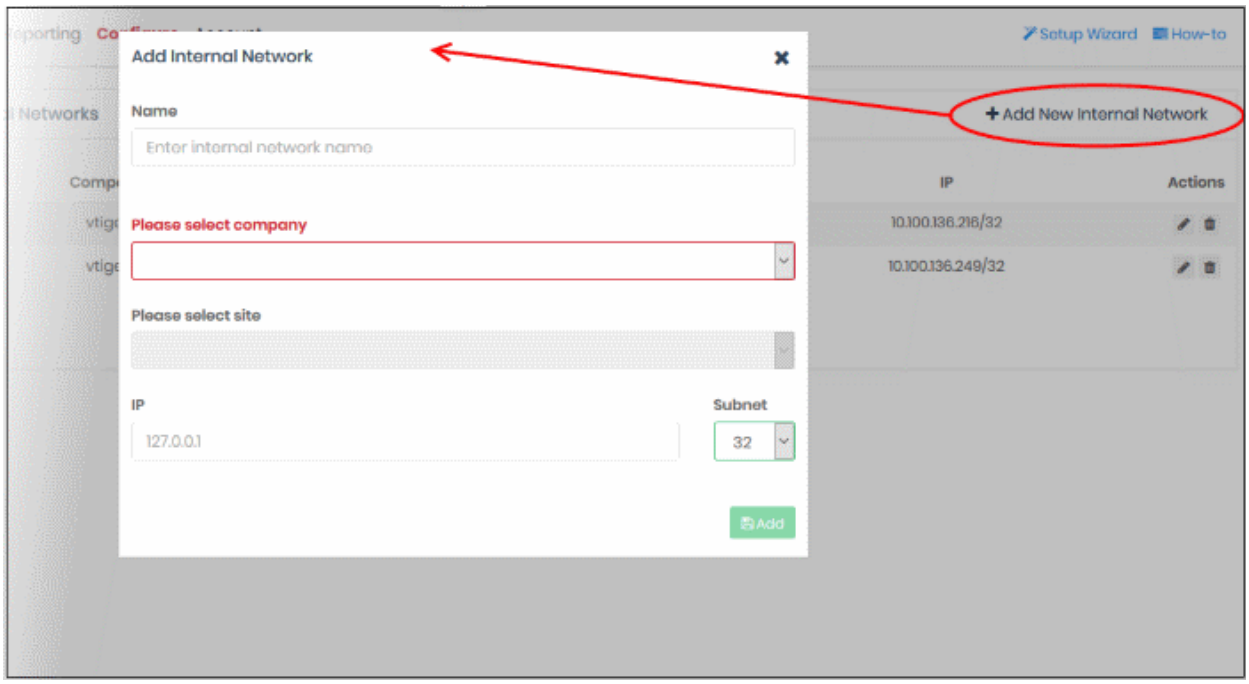
- Click 'Save' to register the local resolver and import the network

The resolver is listed in 'Sites & Virtual Appliances' and the network auto-imported. You can now:

- Apply a policy to the entire network site, or
- Define individual endpoints or sub-nets as objects, and apply policies to them. See 'Add Internal Network Objects', next, for help with this.

Add Internal Network Objects (optional)

- Login to Secure Internet Gateway
- Click 'Configure' > 'Objects' > 'Internal Networks'
- Click 'Add New Internal Network'



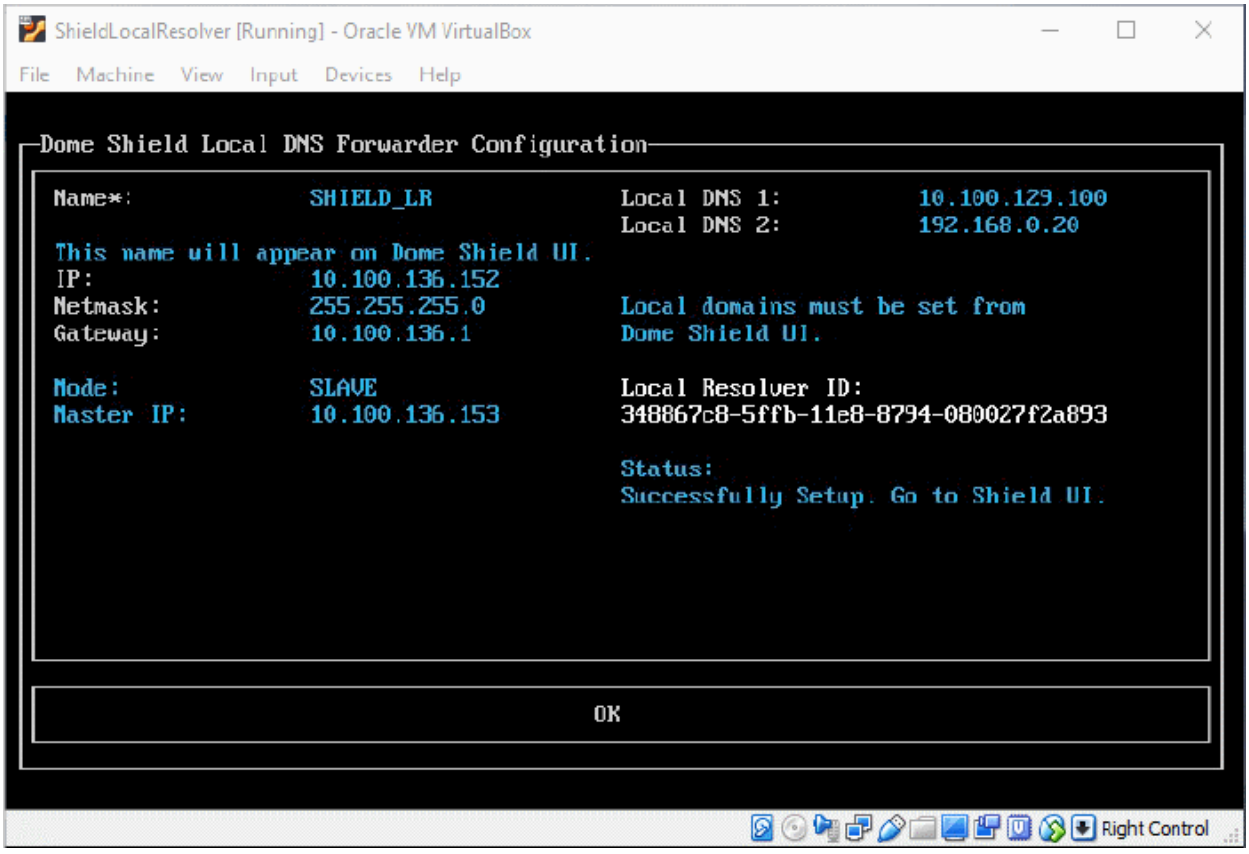
Field	Description
Name	Create a label for the internal object. This name appears in the 'Object' drop-down for the site when you create a policy.
Please select company	MSP customers only. • Choose the company for whom you want to add the network
Please select site	Choose the site to which the internal network belongs

Field	Description
Name	Create a label for the internal object. This name appears in the 'Object' drop-down for the site when you create a policy.
IP	IP address of the internal network in CIDR notation. • 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.
- Repeat the process to define more internal network objects

Step 4 - Setup the Slave VA (Optional)

- For high-availability, we recommend you deploy two local resolvers (LR's) for each network you import. The resolvers can be configured in a master-slave relationship. If the master fails, the slave will continue to forward queries to Secure Internet Gateway DNS.
- You need to install another local resolver VA 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:



Field	Description
Name	Type a label to identify the slave VA. This name will identify the VA in CSIG 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 '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	**Note this ID string**. You need this to register the resolver in CSIG. See Step 3 - Register the Master VA for more help.
Status	Progress of the VA setup process.

- Complete all required fields, select OK, then press 'Enter'. The resolver is registered as 'Slave' to the 'Master'.

Step 5 - Configure DNS Settings on endpoints to point 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

Enroll Roaming Devices

Install the CSIG agent on Windows and Mac devices to protect them when they are outside your network.

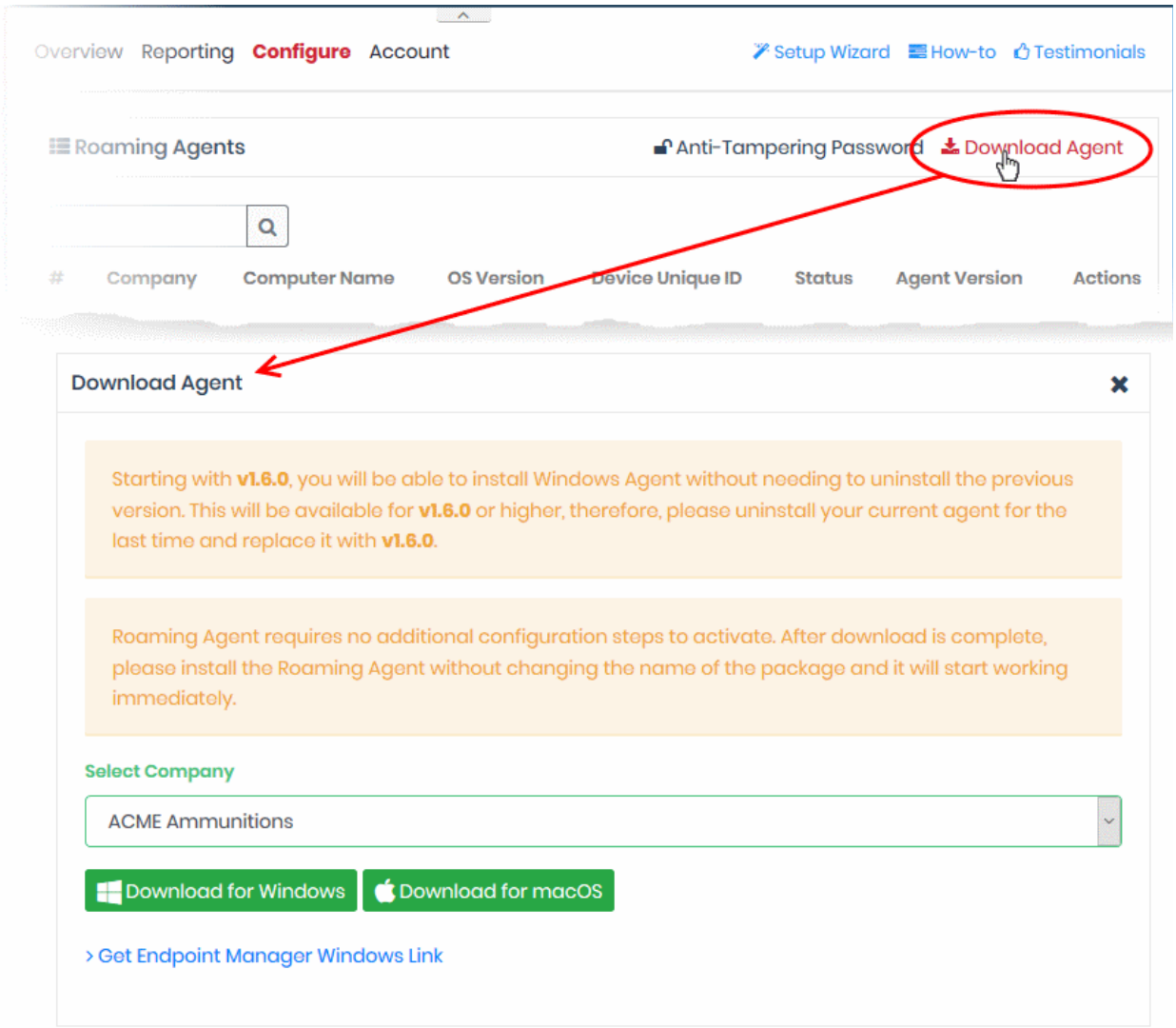
- Click 'Configure' > 'Objects' > 'Roaming Devices' > 'Download Agent'
- You can manually install the agent on devices, or install it remotely through Endpoint Manager.

Once installed, you can deploy policies to 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).

Add new devices:

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



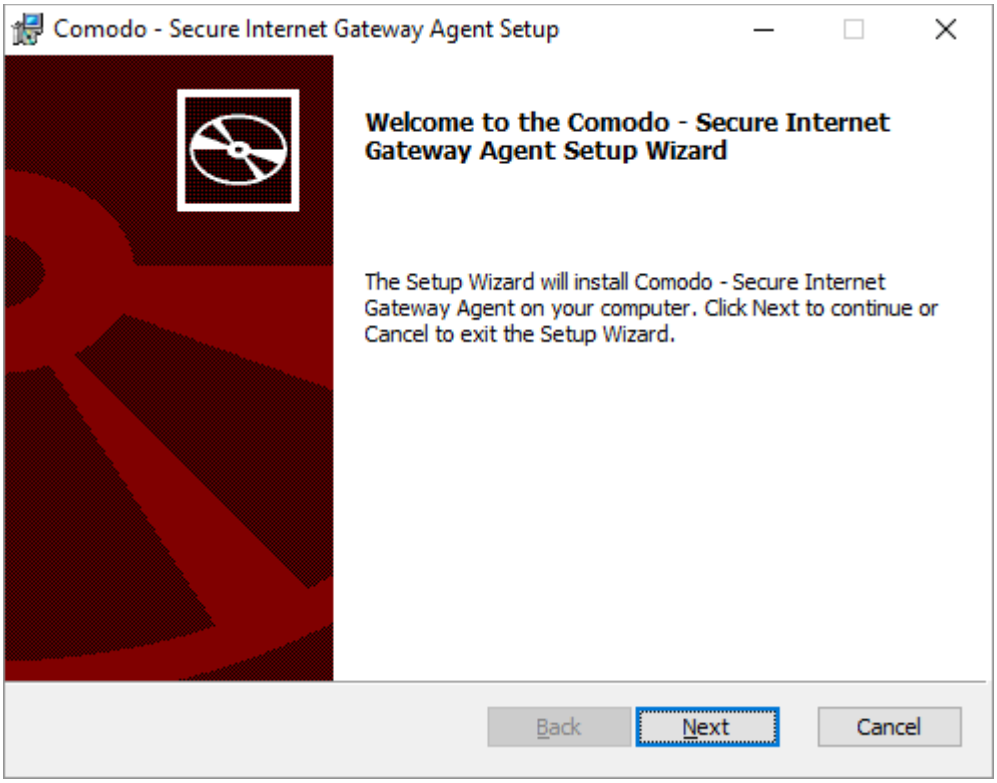
- **Company** - MSPs only. Select the customer organization for which you want to enroll devices.
- **Download for Windows** - The agent setup file for Windows devices. See **Enroll Windows devices** for more details.
- **Download for mac OS** - The agent setup file for Mac devices. See **Enroll Mac OS devices** for more details.
- **Get Endpoint Manager Agent Windows Link** - Allows you to remotely install the agent on endpoints through Endpoint Manager. See **Import Windows Devices from Endpoint Manager (formerly ITSM)**.

Enroll Windows devices

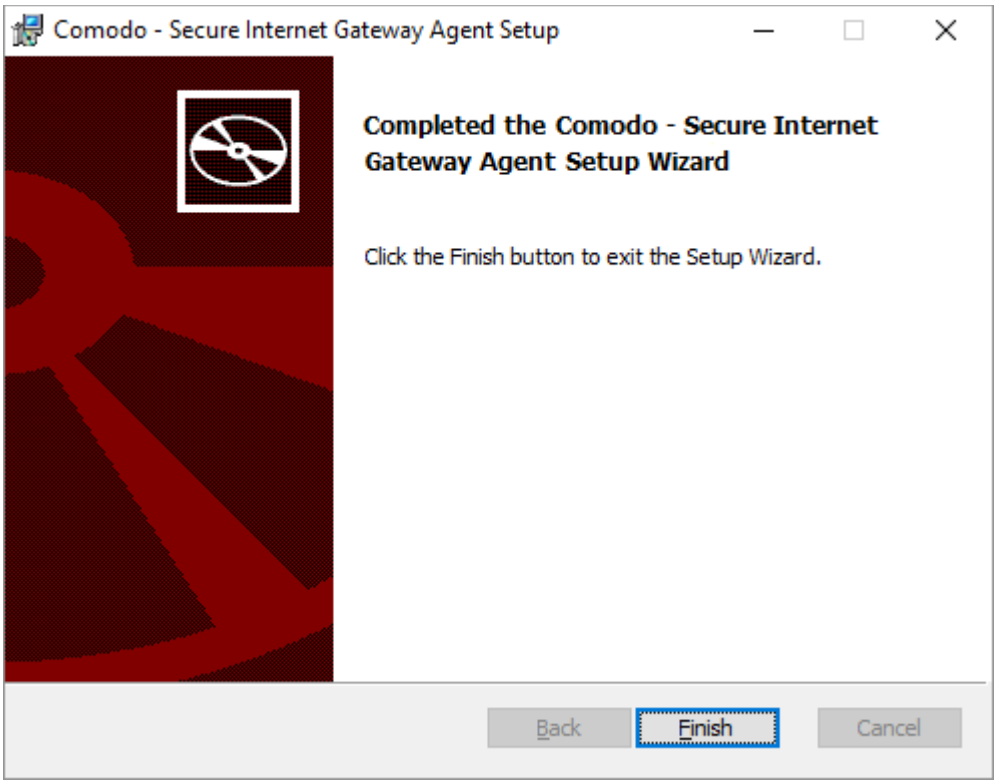
- Click 'Configure' > 'Objects' > 'Roaming Devices'
- Click 'Download Agent' at top-right
- Click 'Download for Windows'.
- Transfer the setup .msi to the Windows devices you want to enroll.

Next, install the agent on the devices.

- Run the setup file to start the installation wizard:



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



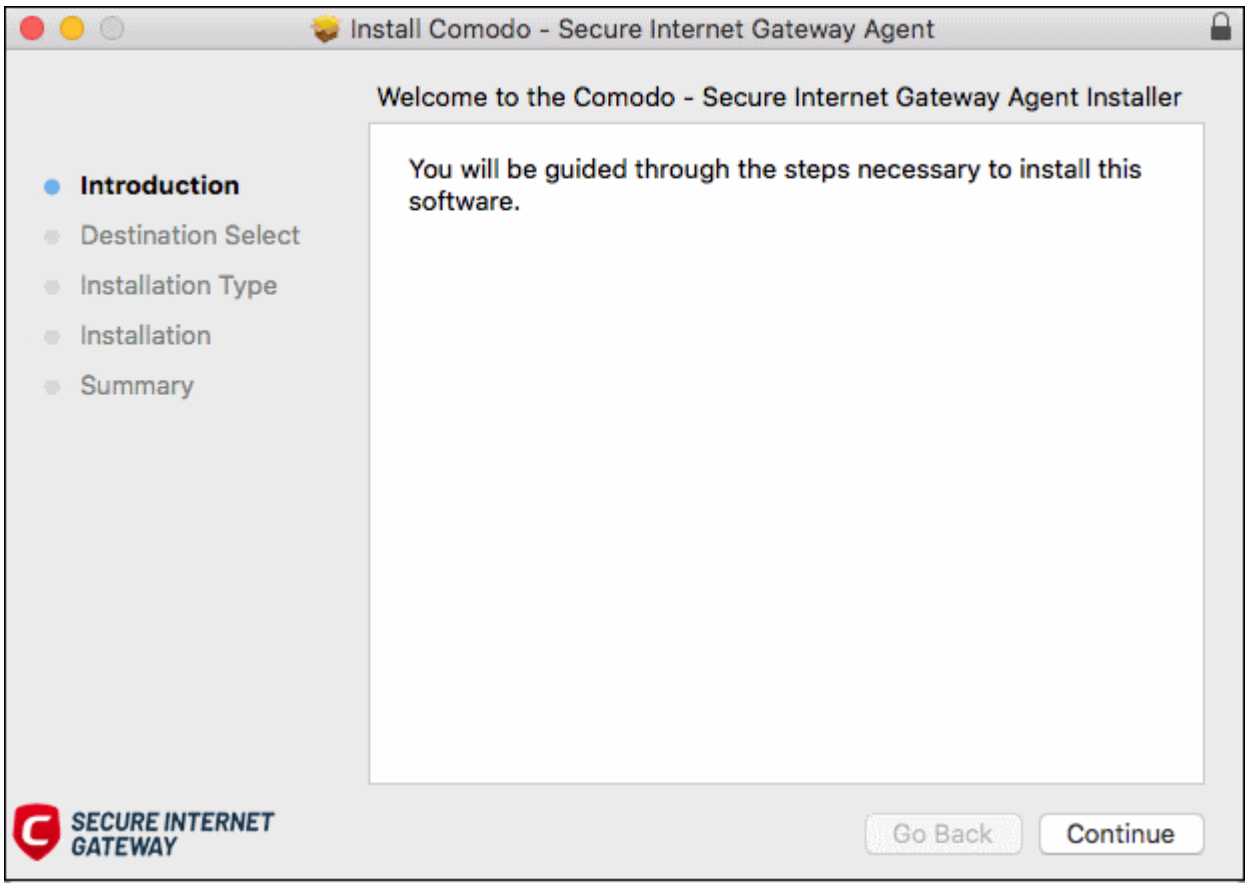
- Click 'Finish'

The device is added and listed in 'Configure' > 'Objects' > 'Roaming Devices'.

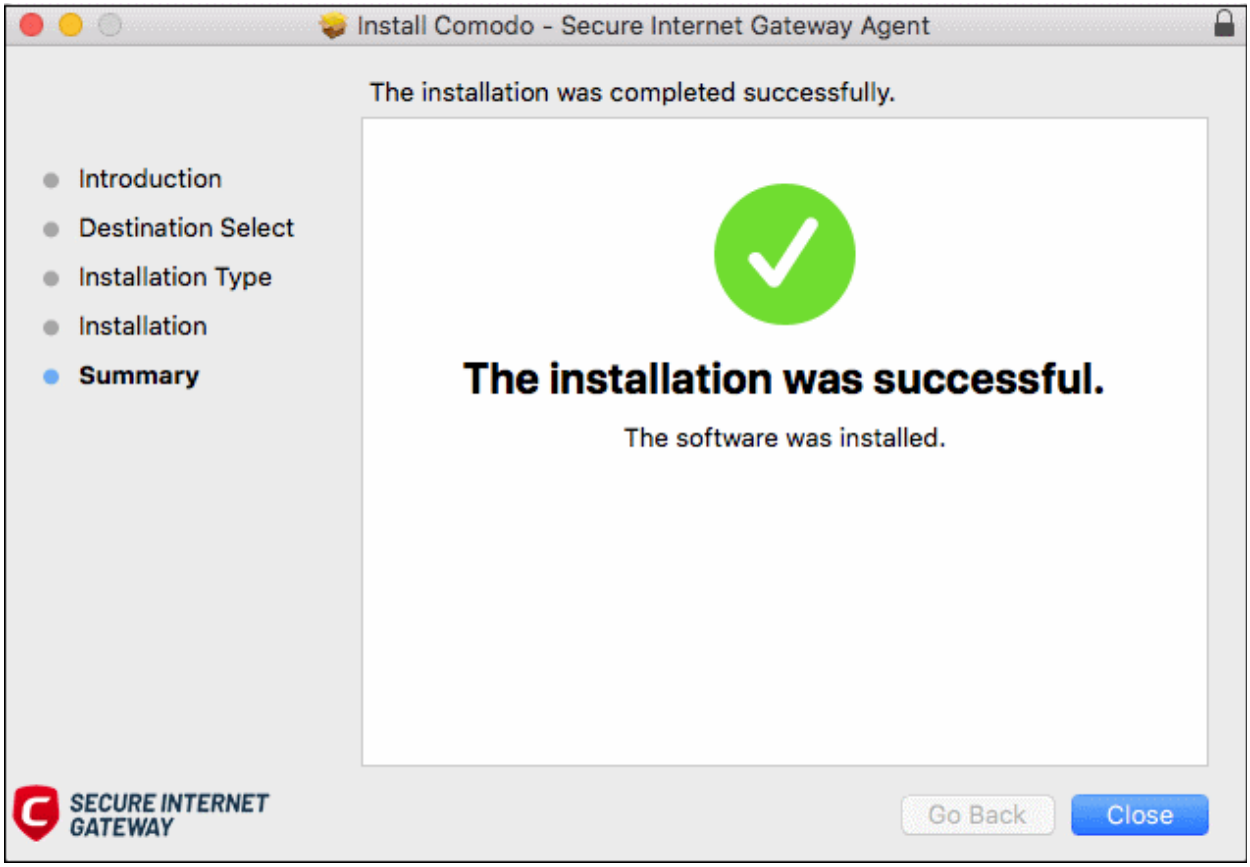
- Note - no security policies are applied to roaming devices by default – you need to create/apply your own.
- See **Step 4** and **Step 5** for help to apply security policies to roaming devices.

Enroll Mac OS devices

- Click the 'Download for Mac OS'.
- Transfer the .pkg file to the Mac devices that you want to enroll..
- Run package to start the installation wizard:



- Click 'Continue' and follow the wizard.
- Click 'Close' to exit the wizard when installation is finished:

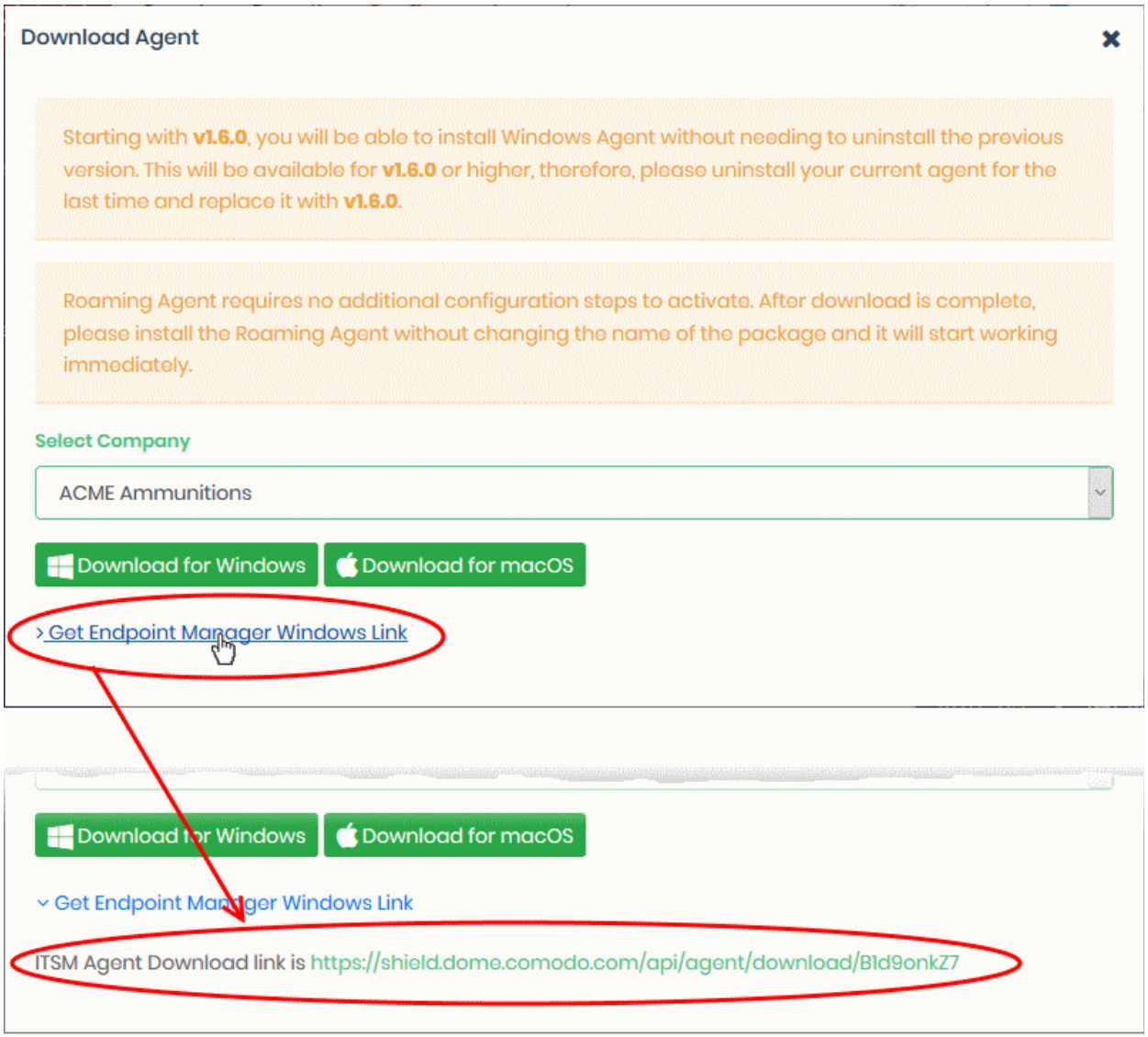


Once installed, the agent starts communicating with the Secure Internet Gateway server. The device is visible in 'Configure' > 'Objects' > 'Roaming Devices'.

- Note - no security policies are applied to roaming devices by default - you need to create/apply your own.
- See **Step 4** and **Step 5** for help to apply security policies to roaming devices.

Import Windows Devices from Endpoint Manager

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



- 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 devices 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 more help to install packages via Endpoint Manager.

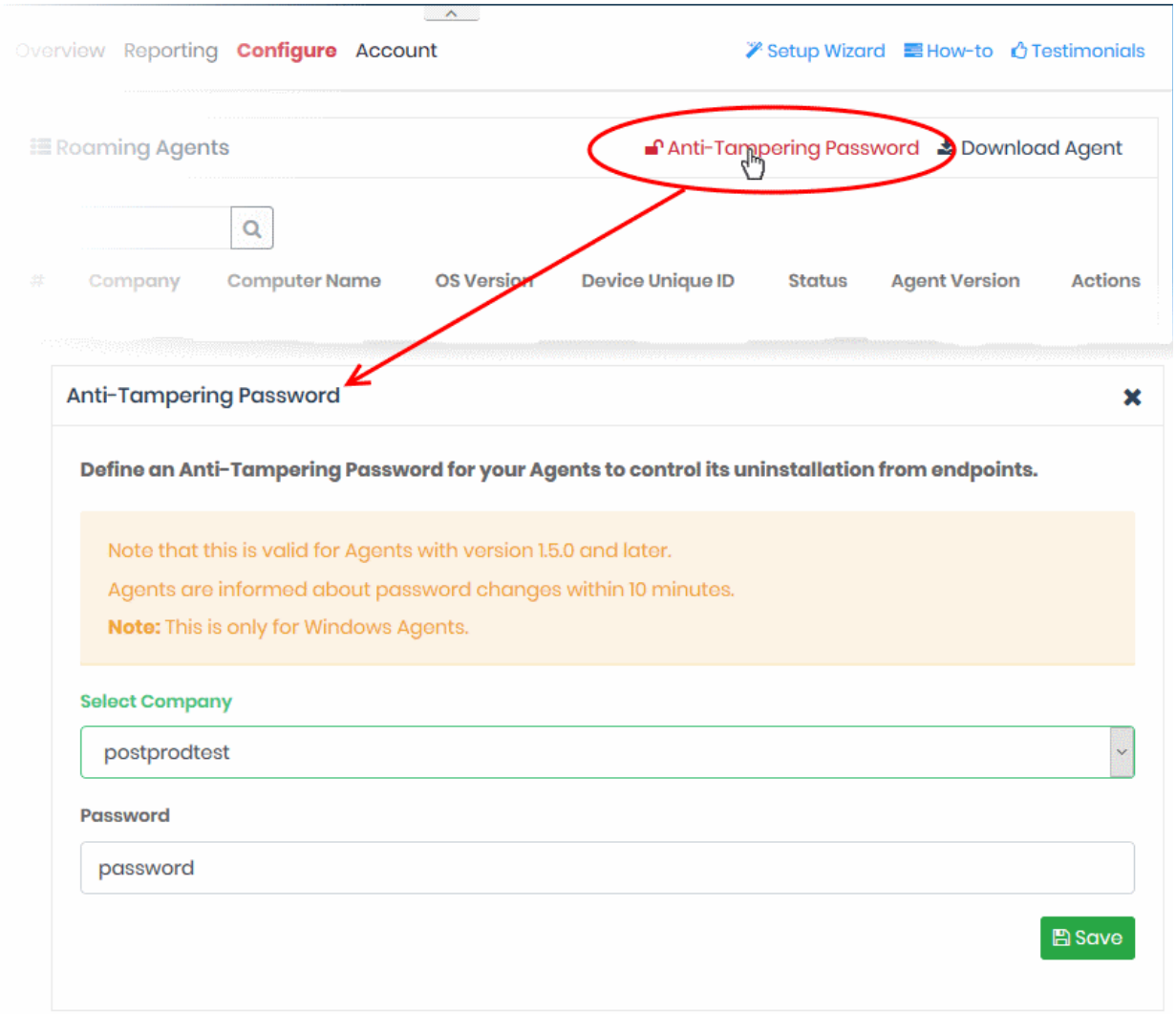
Configure Anti-Tampering Password

- This password helps stop end-users removing the agent from roaming devices.
- Once set, the agent cannot be removed unless the password is provided.
- Password protection is only available for Windows devices.

Set an uninstall password

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

- Click 'Anti-Tampering Password' at top right



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

Note: Password protection is only available for agent version 1.5 and higher.

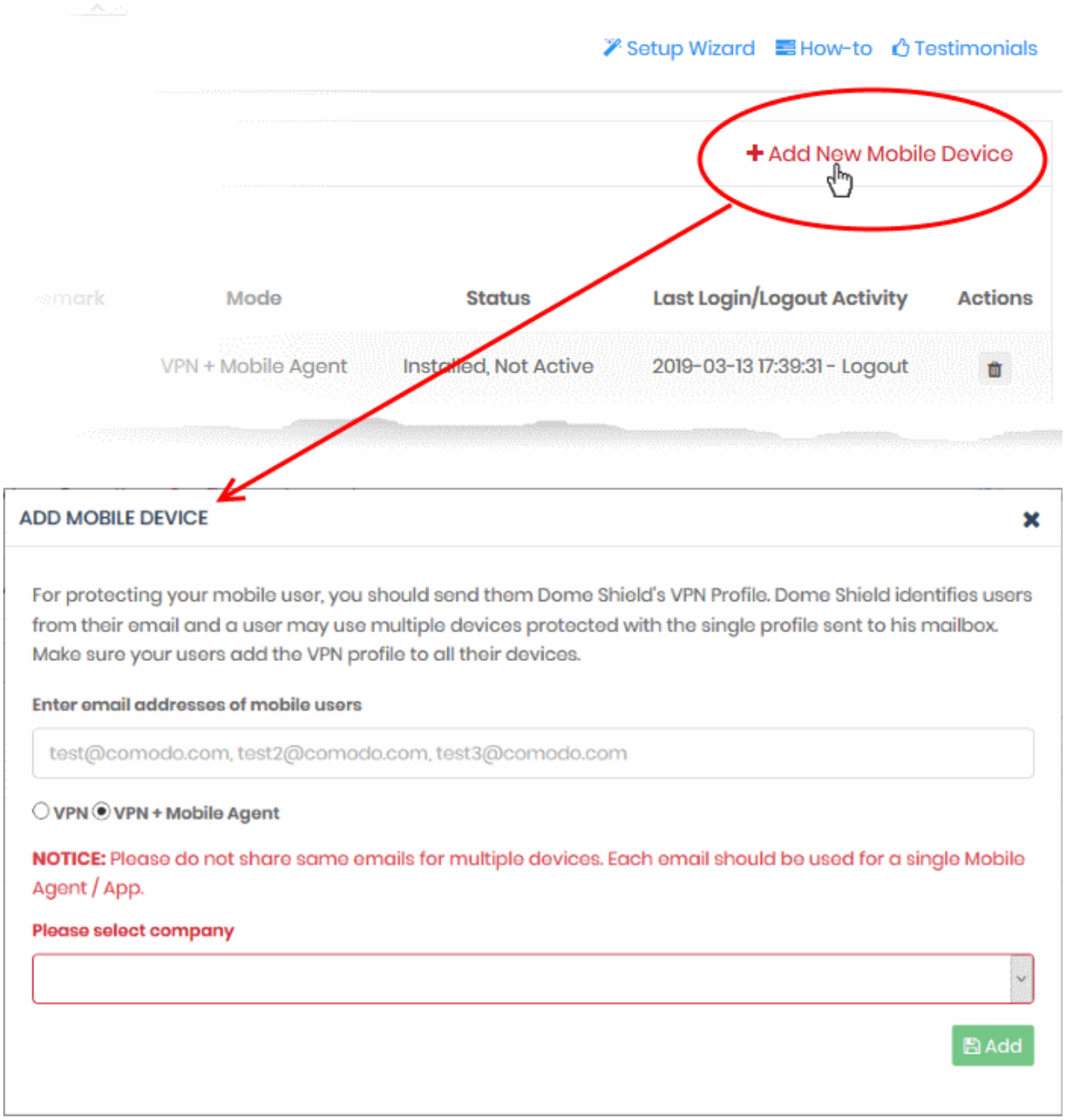
Enroll Mobile Devices

There are two ways to enroll Android and iOS mobile devices:

- **Secure Internet Gateway App** - Includes a VPN client and a VPN profile.
- **VPN Profile** - Contains only the profile. Android users need to install the StrongSwan VPN client.

Enroll mobile devices

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



- **Email addresses of mobile users** - The contact addresses of the users whose devices you want to add. You can enter multiple email addresses. 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

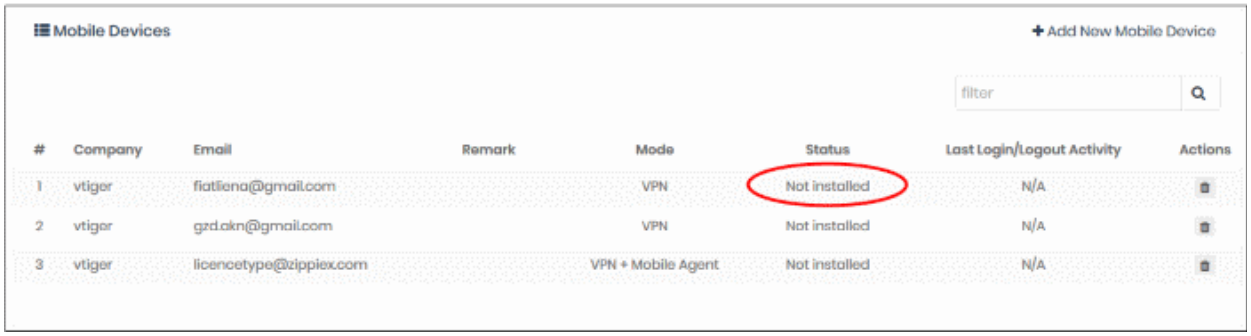
  - **VPN** - This is the profile only. If you select this, Android users must also install the StrongSwan VPN app. StrongSwan is not required for iOS devices.
    - **Click here** to see instructions for this option.
- **Select company** - MSPs only. Choose the customer organization for which you want to enroll mobile devices

- Click 'Add'

VPN

CSIG will send device enrollment mails to all users that you added.

Users are initially added to the list with a device status of 'Not installed':



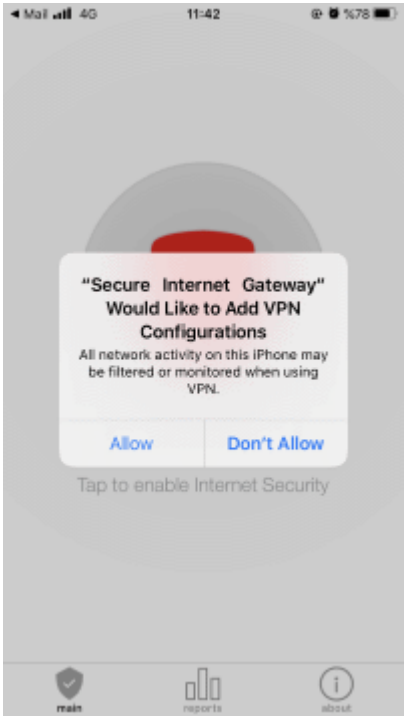
- Users should open the email on the target device.
- The email contains instructions and three attachments:
  - **iOS_VPN_Profile.mobileconfig** - iOS device users should select this.
  - **Android_VPN_Profile.sswan** - Strongswan VPN profile for Android users
  - **Android SSLCert.pem** - This SSL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

iOS instructions

Android instructions

iOS instructions

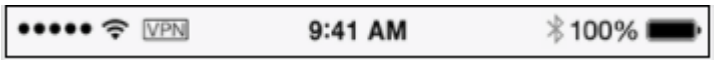
- Tap 'Activate iOS App' in the mail
- Hit 'Allow' to complete the activation:



The VPN profile is now installed on the device.

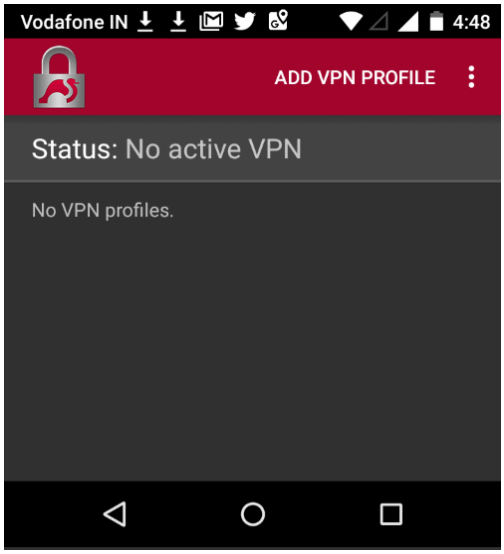
- You also need to trust an SSL certificate in order to view HTTPS pages over the VPN.
- Go to 'Settings' > 'General' > 'About' > 'Certificate Trust Settings' > enable full trust for root certificates.

The VPN icon will appear in the nav bar when you are successfully connected:

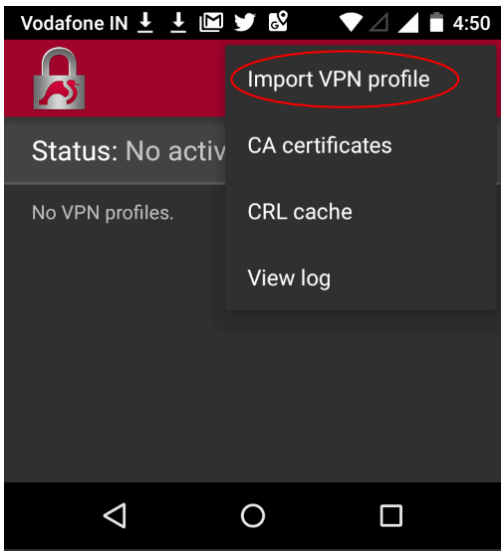


Instructions for Android

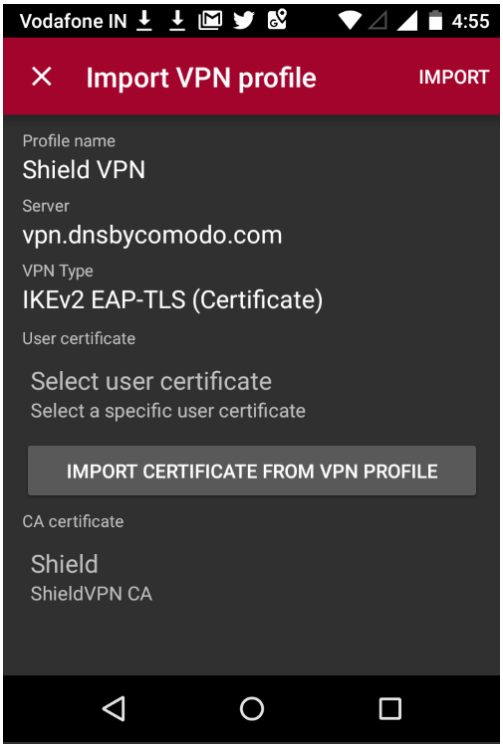
- Open the enrollment mail and select 'Android_VPN_Profile'
- Open the StrongSwan VPN app:



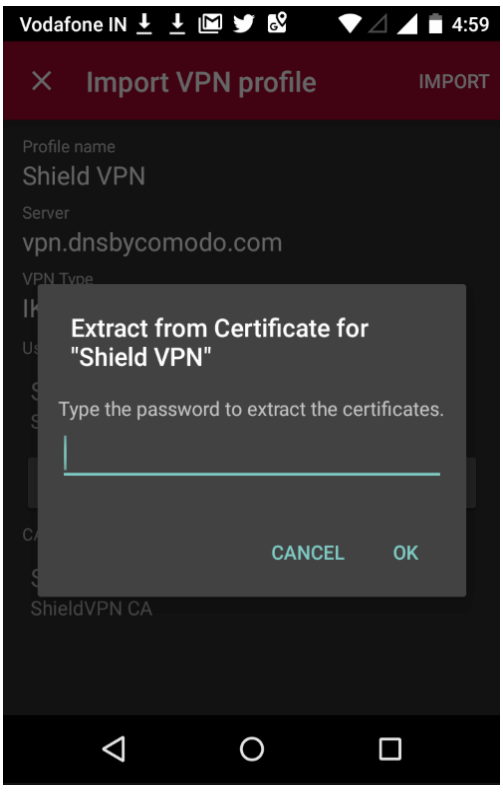
- Select 'Add VPN Profile' > 'Import VPN profile':



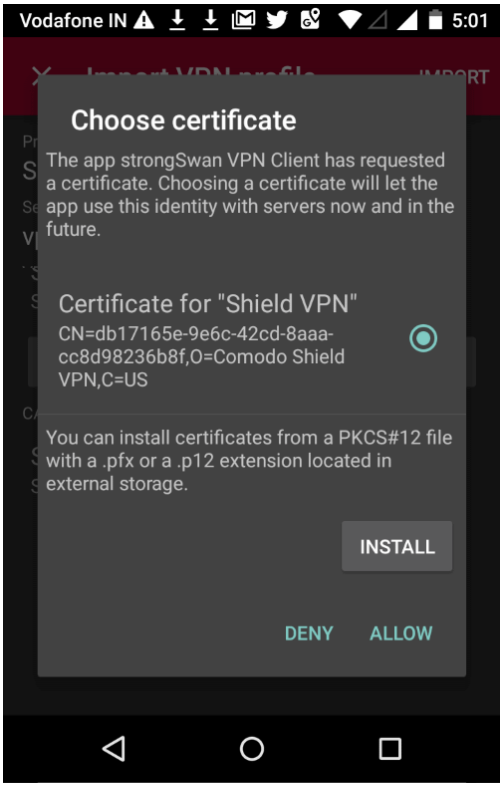
- Open the 'Android_VPN_Profile' that you saved earlier



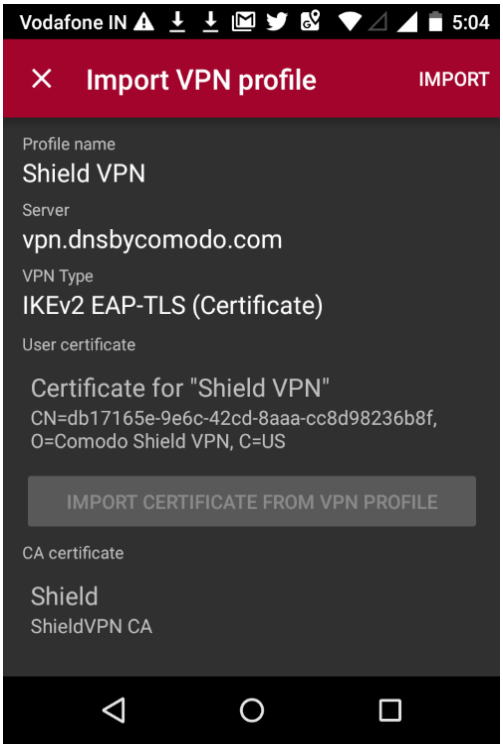
- Select 'Import Certificate from VPN Profile'



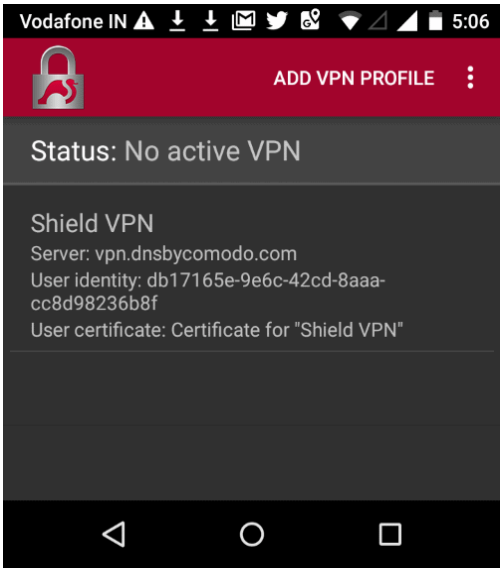
- Enter the password in the email and select 'OK'



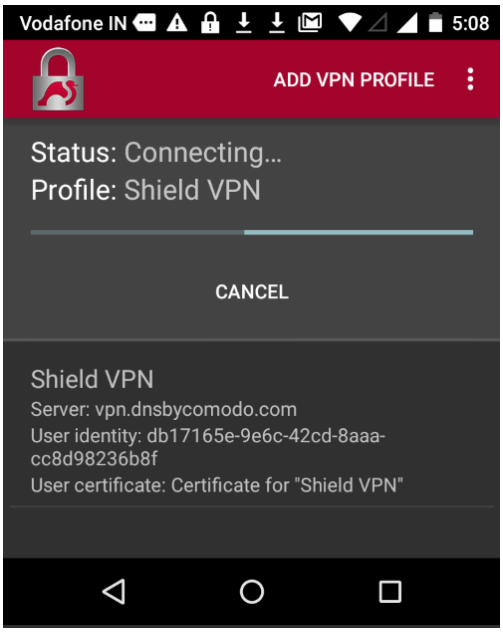
- Tap 'Allow' instead of 'Install'



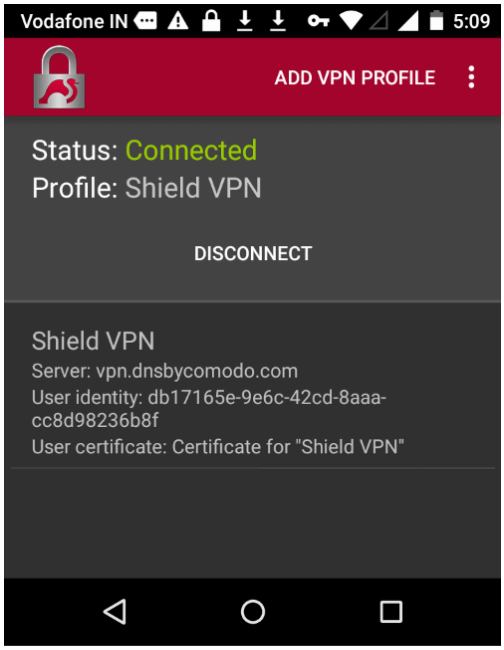
- Select 'Import' at the top-right



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

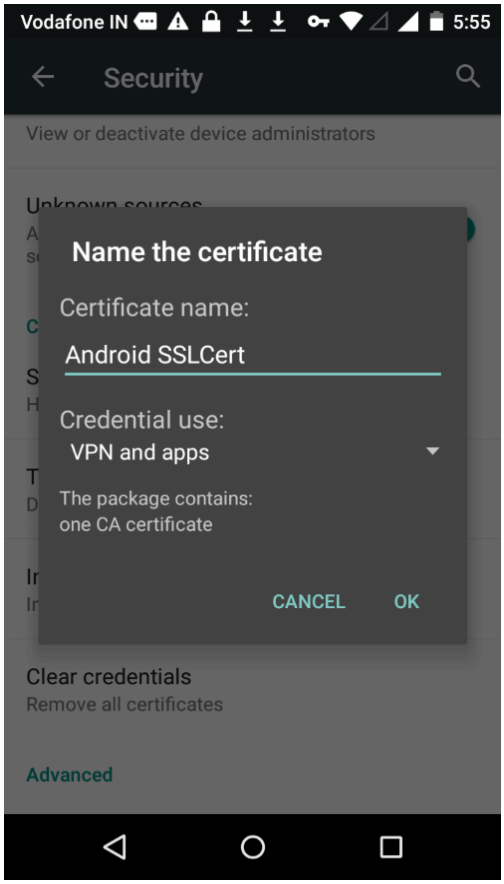


You will see the following screen when connected:



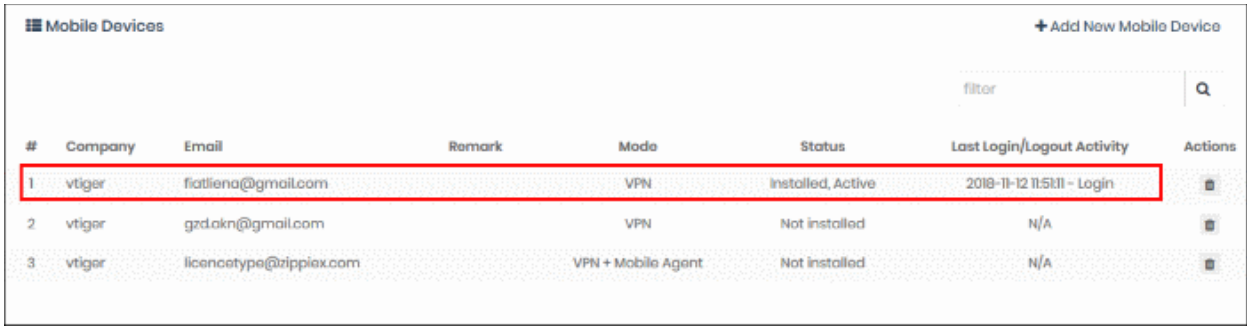
Note: You also need to trust the SSL certificate in order to view HTTPS pages over the VPN.

- Go to 'Settings' > 'Security' > 'Credential Storage' > 'Install from SD card'. 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.

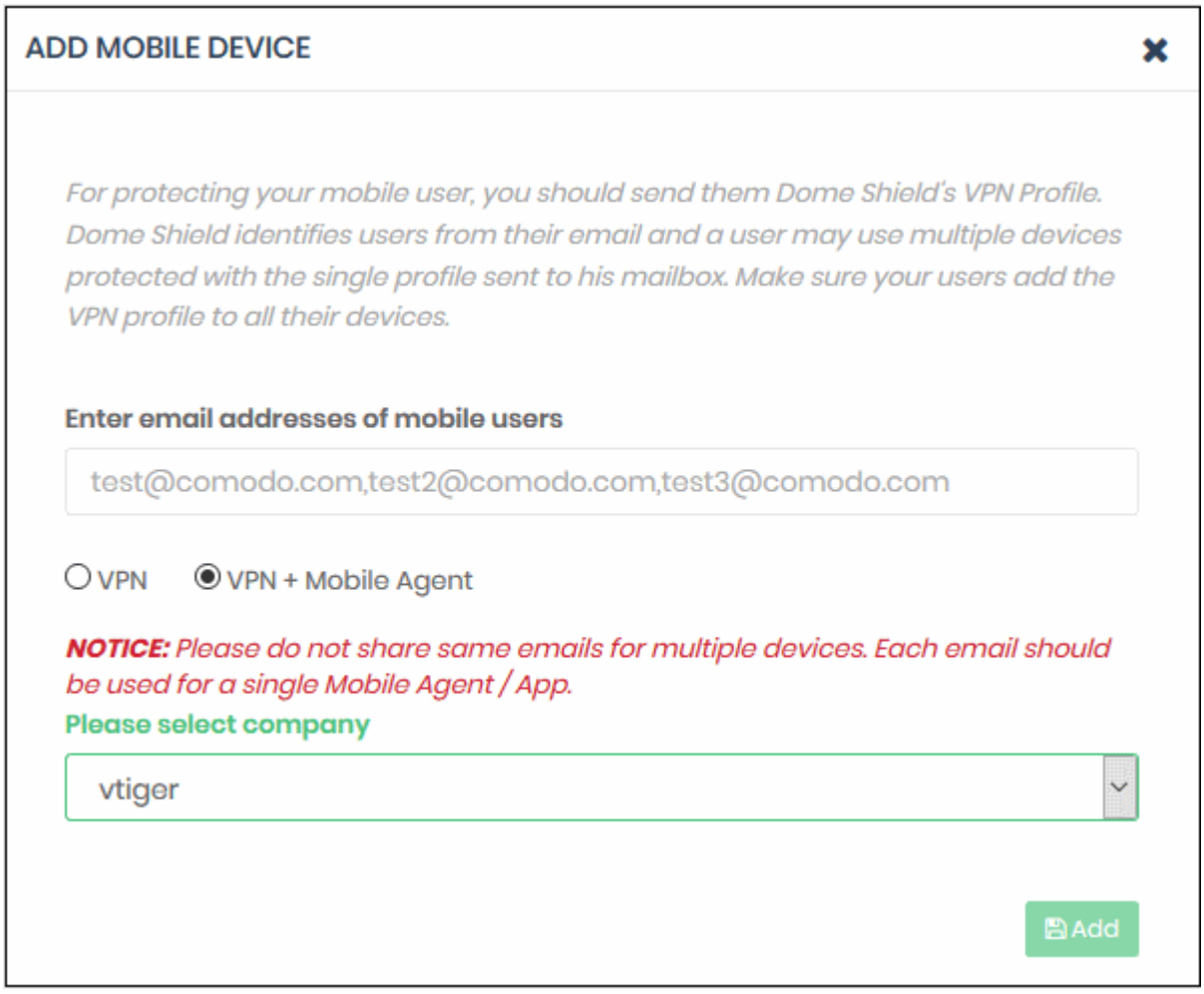
The mobile device will be enrolled and shown as follows:



- No rules are applied to mobile devices by default.
- You can apply device specific policy according to your requirements.
- See **Step 5 - Create and Apply Security Policies** for help to apply security policies to mobile devices.

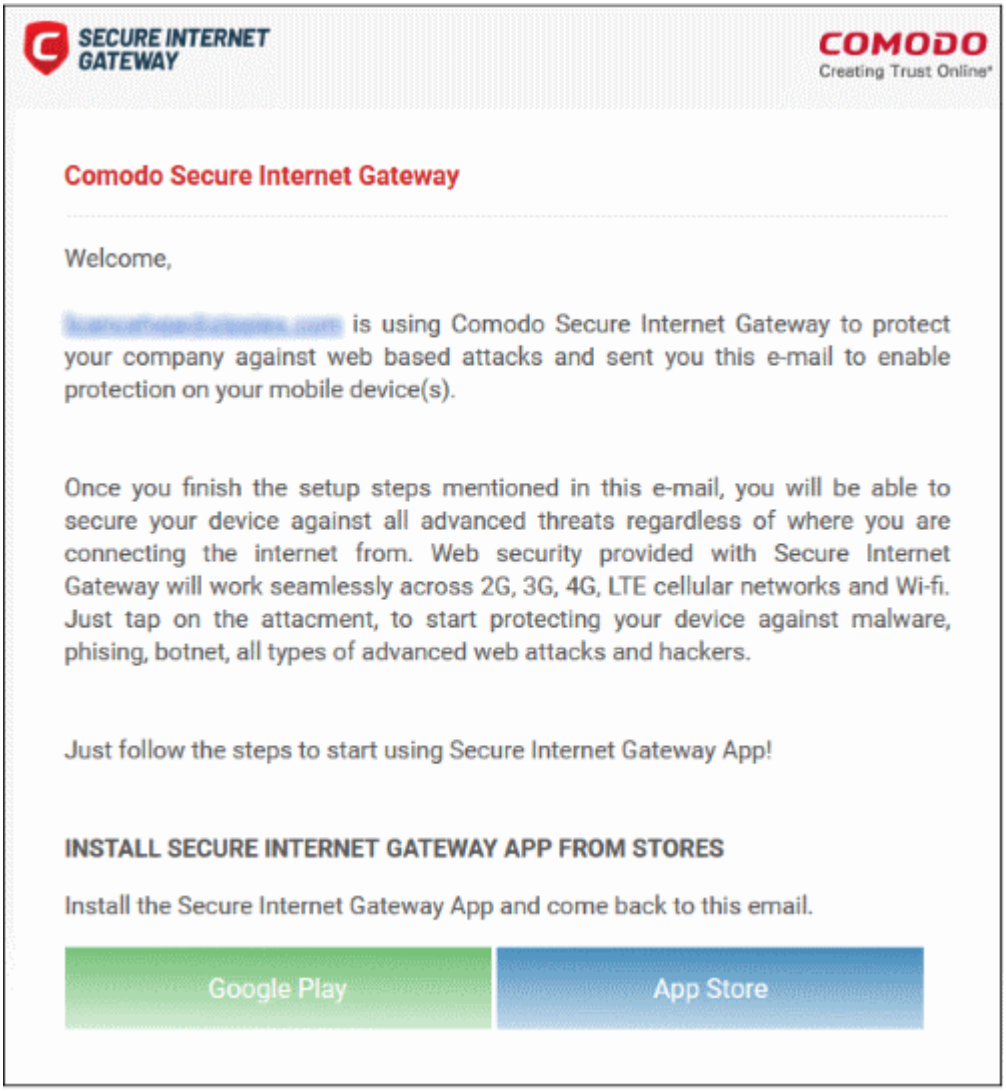
CSIG Mobile App

- Enter the email addresses of device owners as before
- Select 'VPN + Mobile Agent'



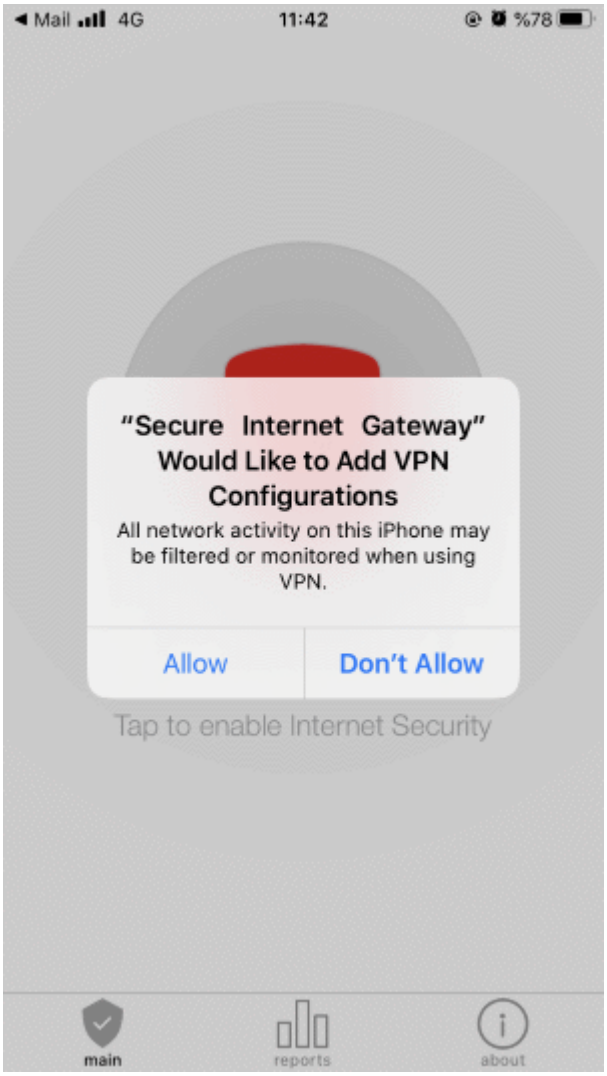
- Select Company - MSPs only. Choose the company to whom the devices belong.
- Click 'Add'
- CSIG will send enrollment emails to all users that you add.
- Users are initially added with a device status of 'Not installed':

- Users should open the enrollment mail on their mobile device. The email contains instructions on how to install the 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:

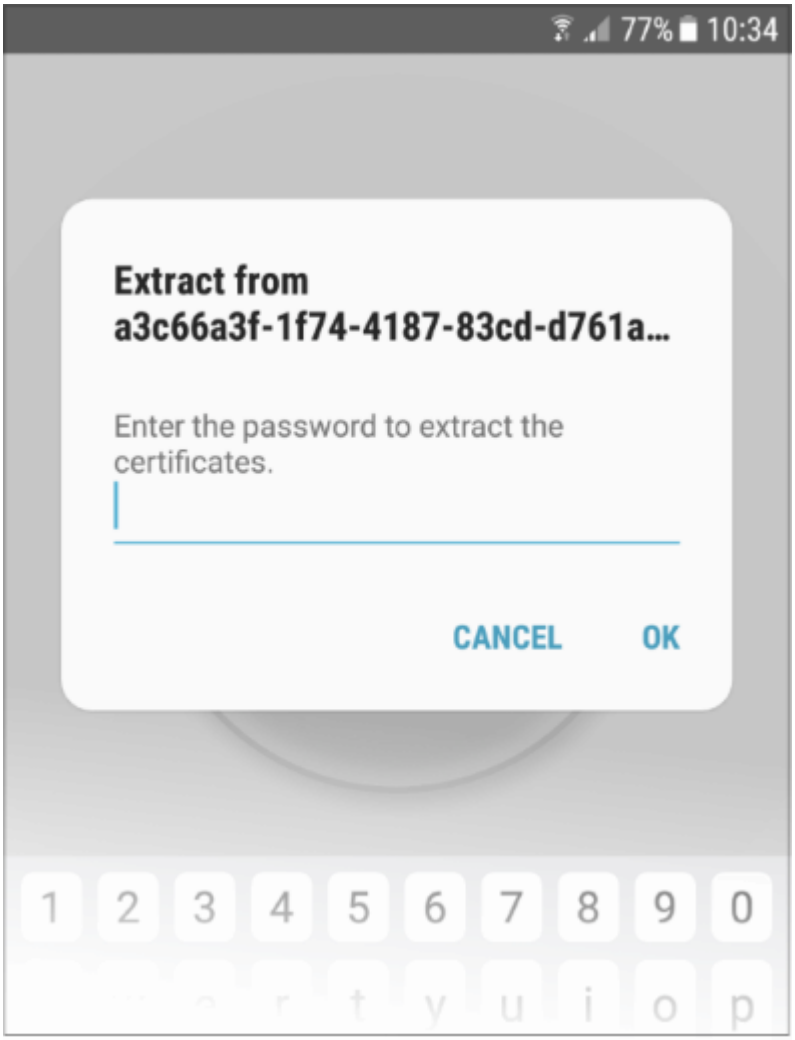
That's it. The iOS device is successfully enrolled to Secure Internet Gateway.

- You also need to trust the SSL certificate 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

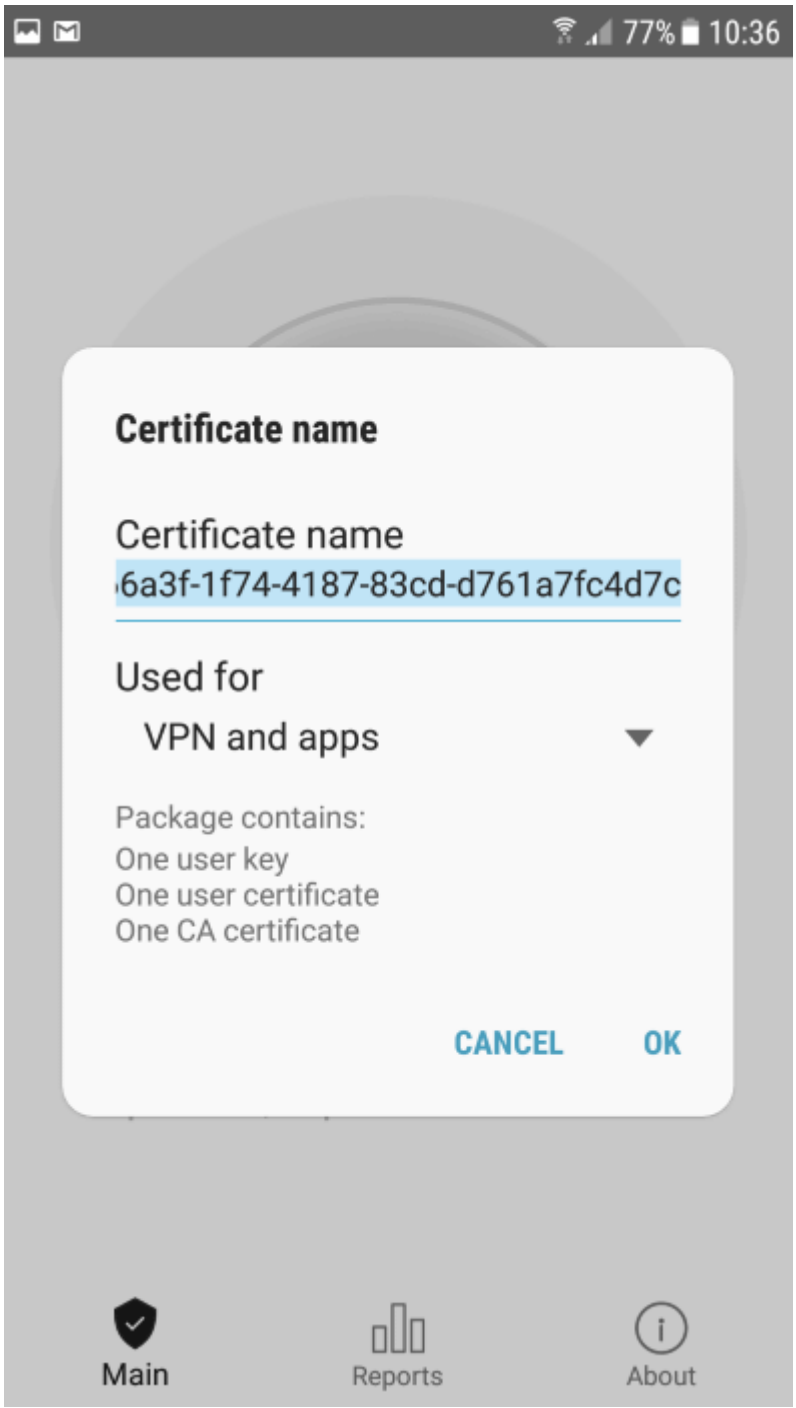
Instructions for Android

- Open the enrollment mail.
- Select 'Google Play' and install the app from the Play Store.
  - The installation screens may differ across Android versions.
- 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:



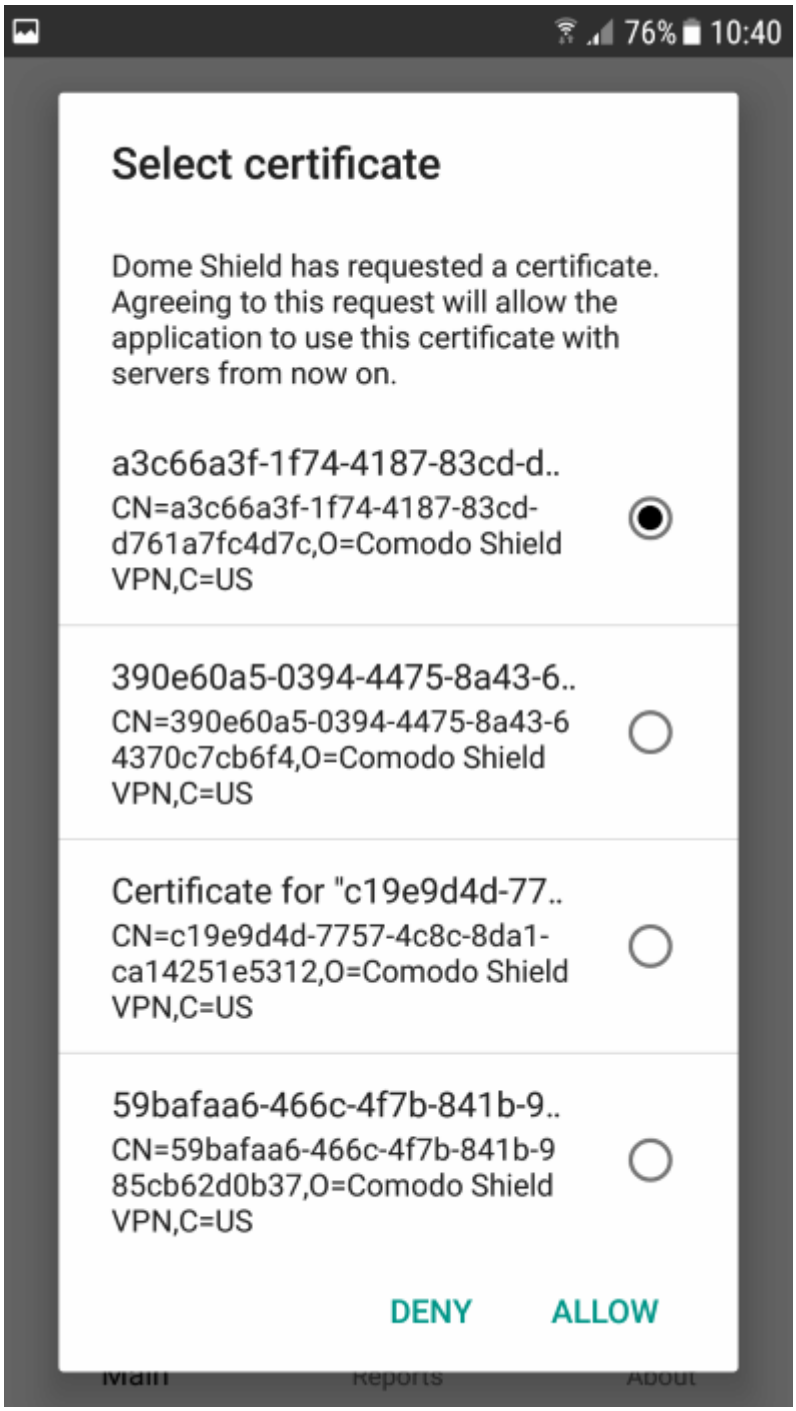
- Long press in the password field and select 'Paste'
- Select 'OK'

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:



- Choose '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.

Step 4 – Configure policy items

Policies are constructed from a series of rules. There are three types of rule:

- **Security Rules** - Block sites known to host specific types of threat. Example threat types include malware, phishing, spyware etc.
- **Category Rules** - Control access to websites by content type. Example categories include social media, gambling, sports etc. Each category contains hundreds or thousands of sites that host a specific content type.
- **Blacklists and Whitelists** – Block or allow access to specific sites. These lists are often used to create exceptions when a site is blocked or allowed by a category rule.

You can also configure the following in a policy:

- **Virtual Browsing** - Specify that websites blocked by a security rule are instead opened inside a virtual environment. Virtual sessions are completely isolated from the host operating system, so any malware downloaded cannot infect the device or network.
- **Block pages** - Create custom block pages which are show when users visit a site that is blocked by one of your policies.

You can create as many policies as you want and apply them to networks and devices as required.

See the following sections for help with each item:

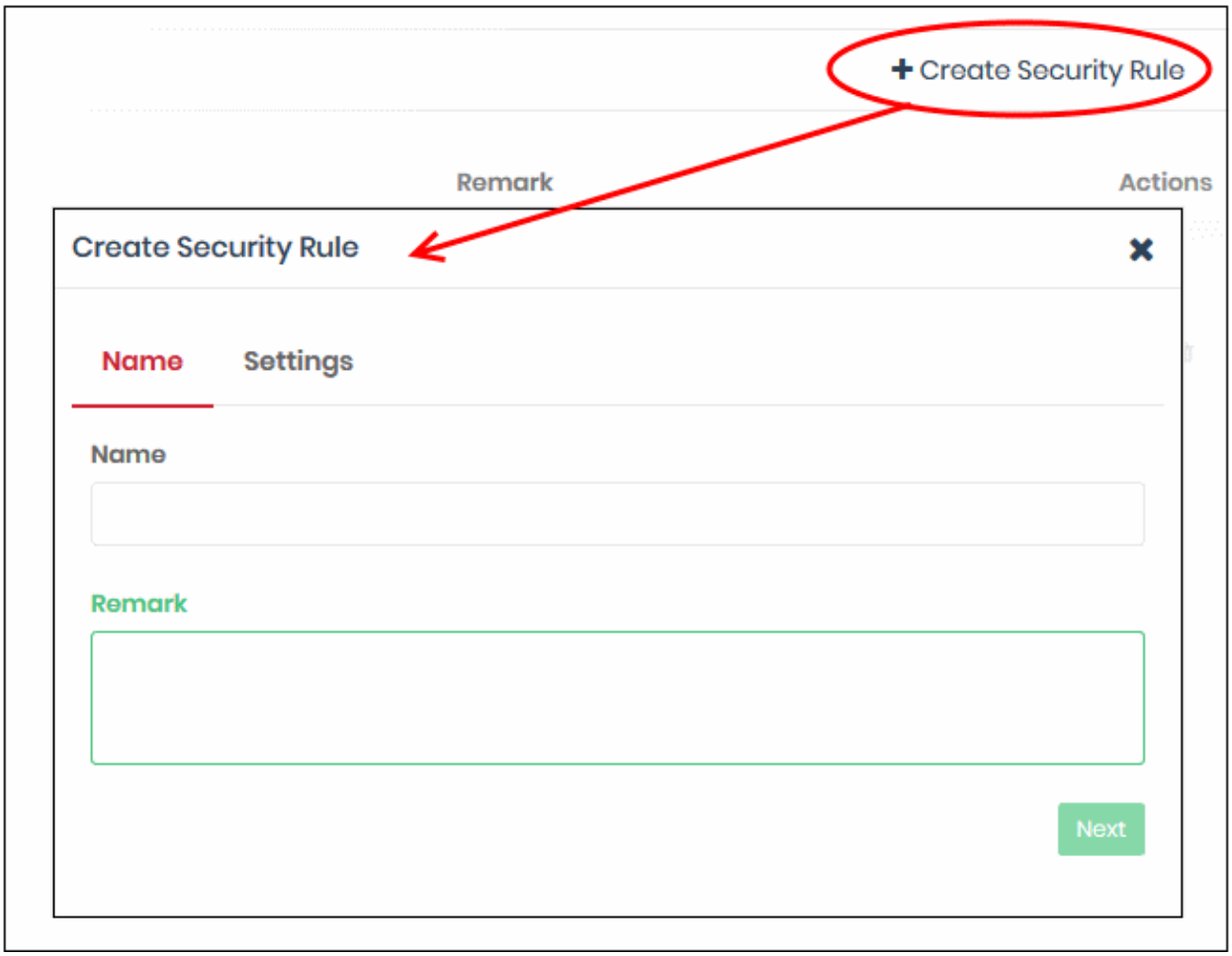
- **Add Security Rules**
- **Add Category Rules**
- **Add Domain Blacklists and Whitelists**
- **Configure Virtual Browsing**
- **Add Block Pages**

Add 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. 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
- CSIG ships with a default security rule that blocks phishing, malware and spyware websites. You can use this rule in a policy, or configure new security rules as required.

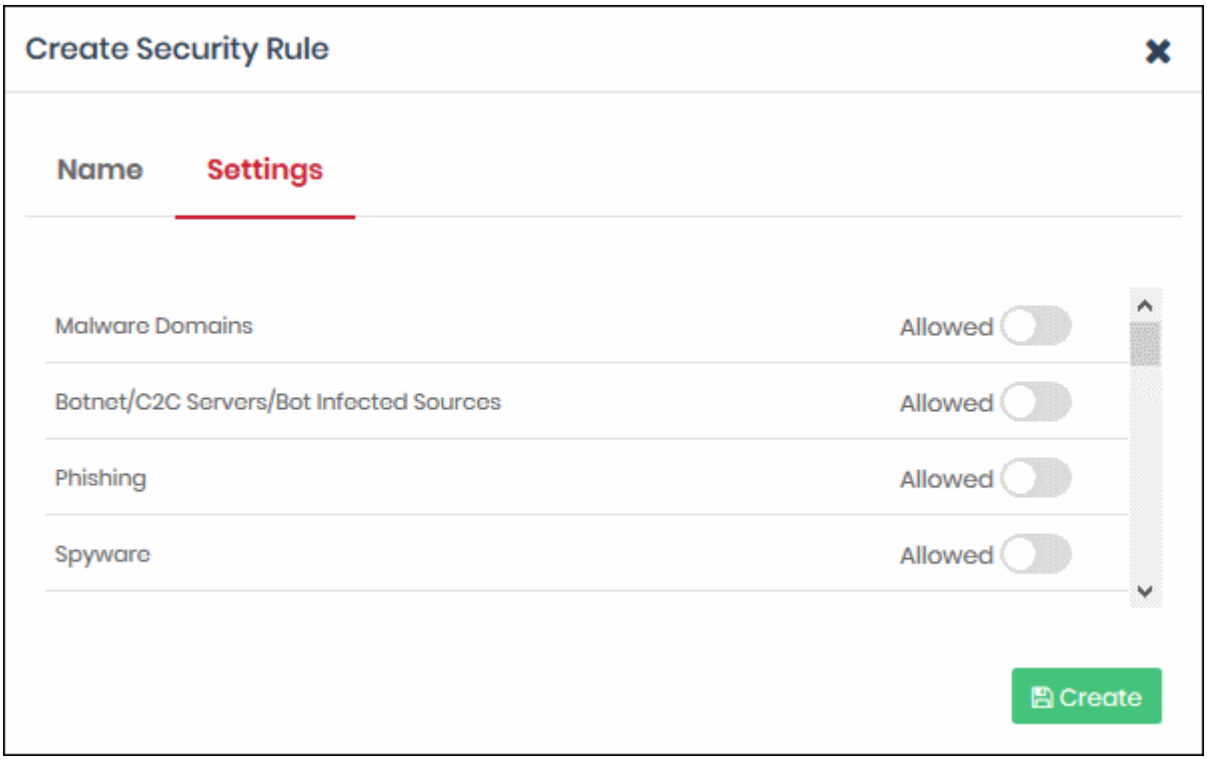
Create a security rule

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



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' or 'Settings' to choose the security categories you want to allow or block:



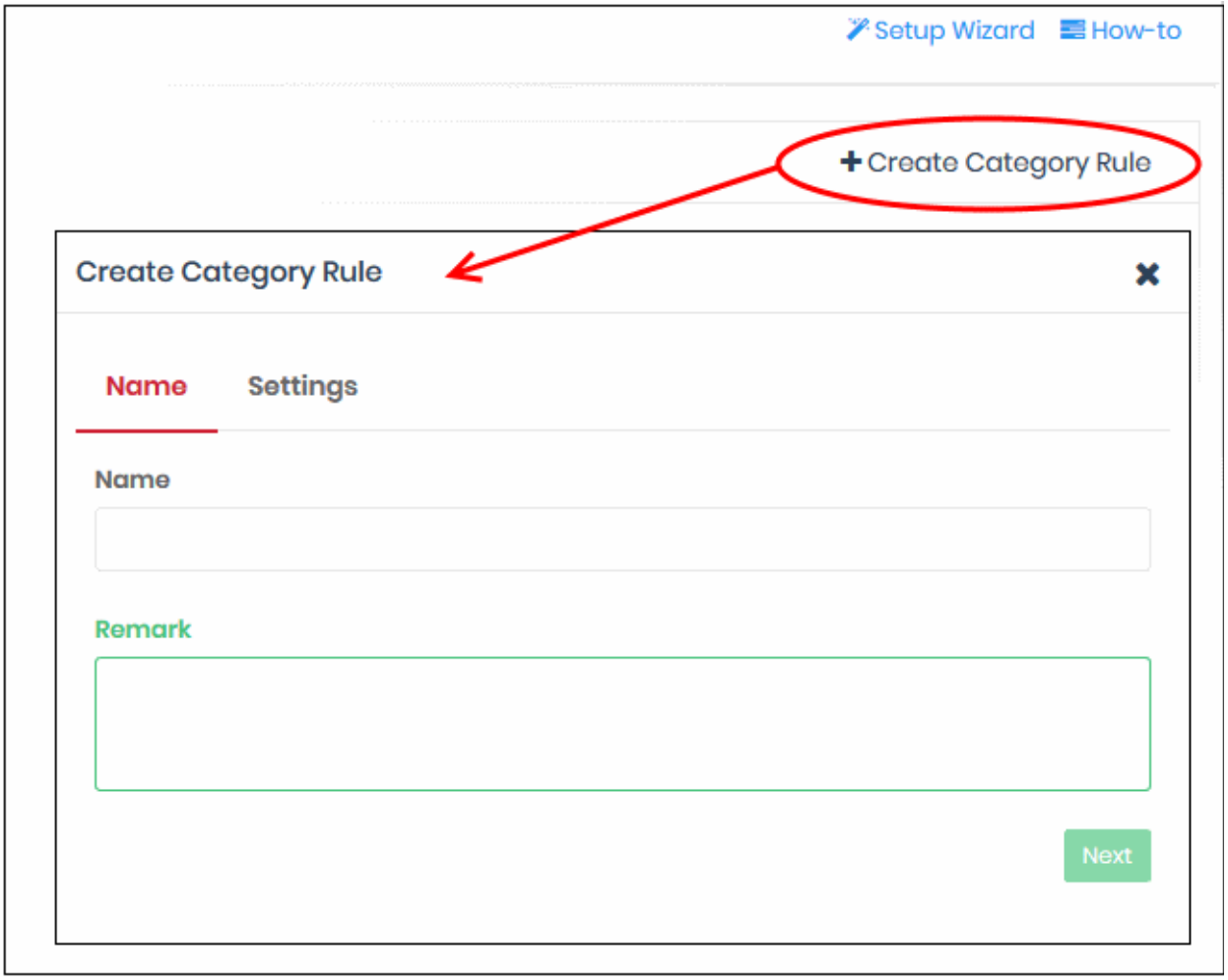
- Use the switches to allow or block sites in a particular threat-category
- Click the 'Create' button to save your rule
- Your new security rule will be available for selection when **creating a policy**.
- Repeat the process to add more security rules

Add 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.

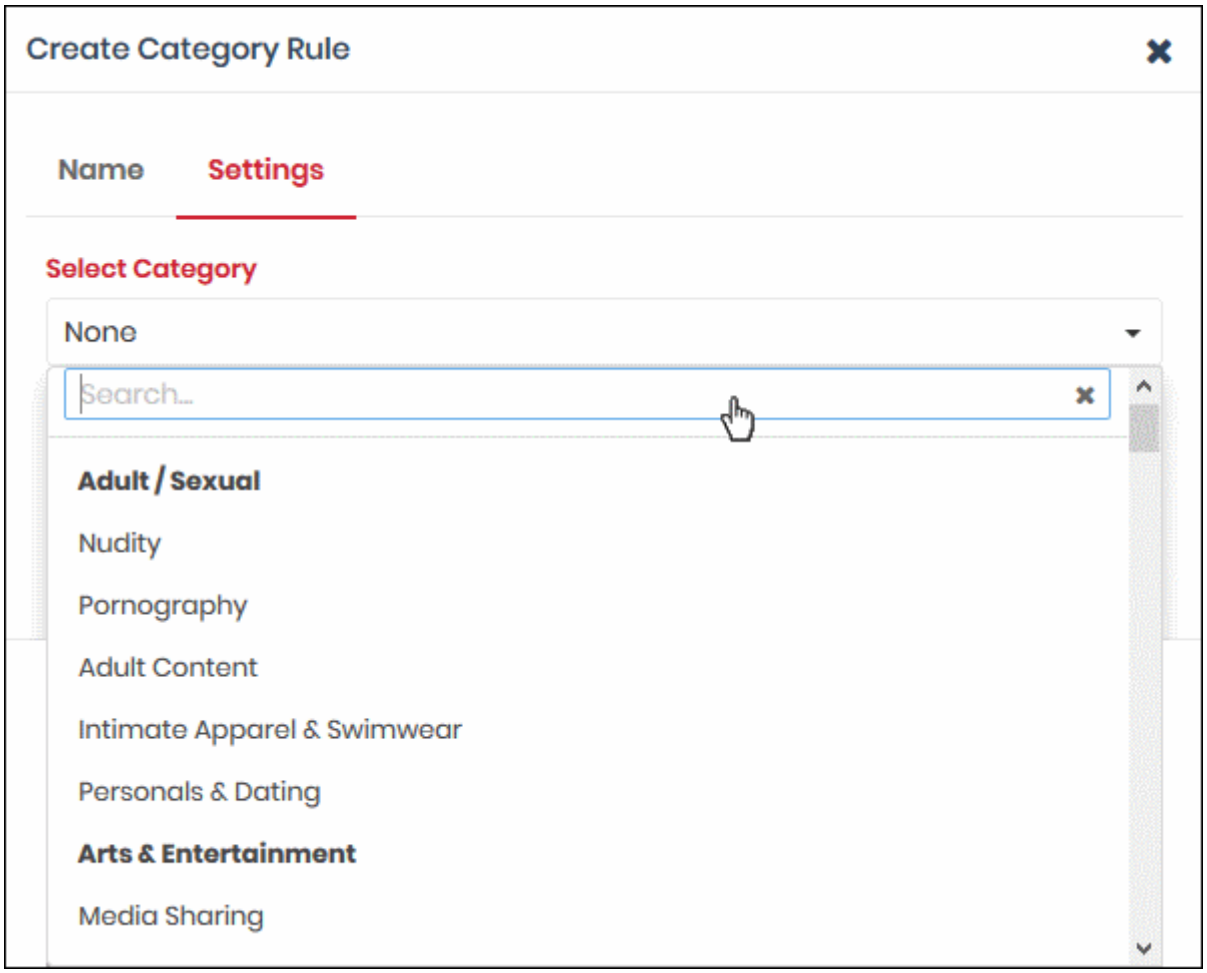
Create a category rule

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

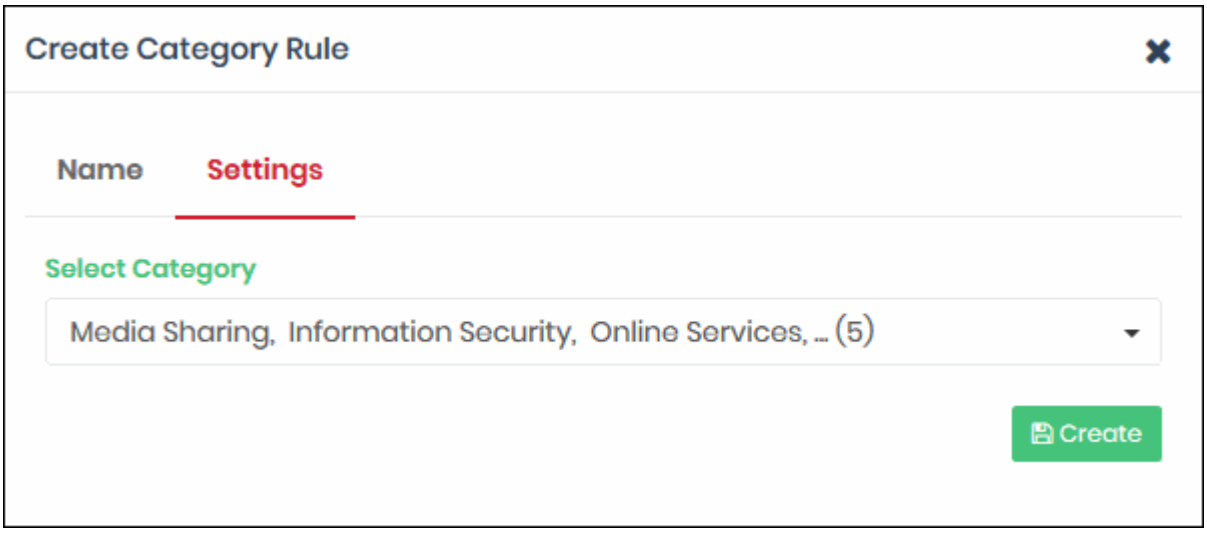


Name and remarks - Create a rule label and comments which will help you and others identify the purpose of the rule.

- Click 'Settings' or 'Next' to choose which categories you want to block/allow:



- **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 are automatically selected. Review and deselect any sub-categories you want to allow.
- You can add multiple categories to your rule. The number of categories you have added are shown at the end of the list:



- Click 'Create' when done.
- The category rule is now available to **add to a policy**.

- Repeat the process to add more category rules

Add Domain Blacklists and Whitelists

Blacklists allow you to block access to specific websites, while whitelists let you grant access to specific sites. These lists are often used to create exceptions to the blanket protection provided by a security or category rule.

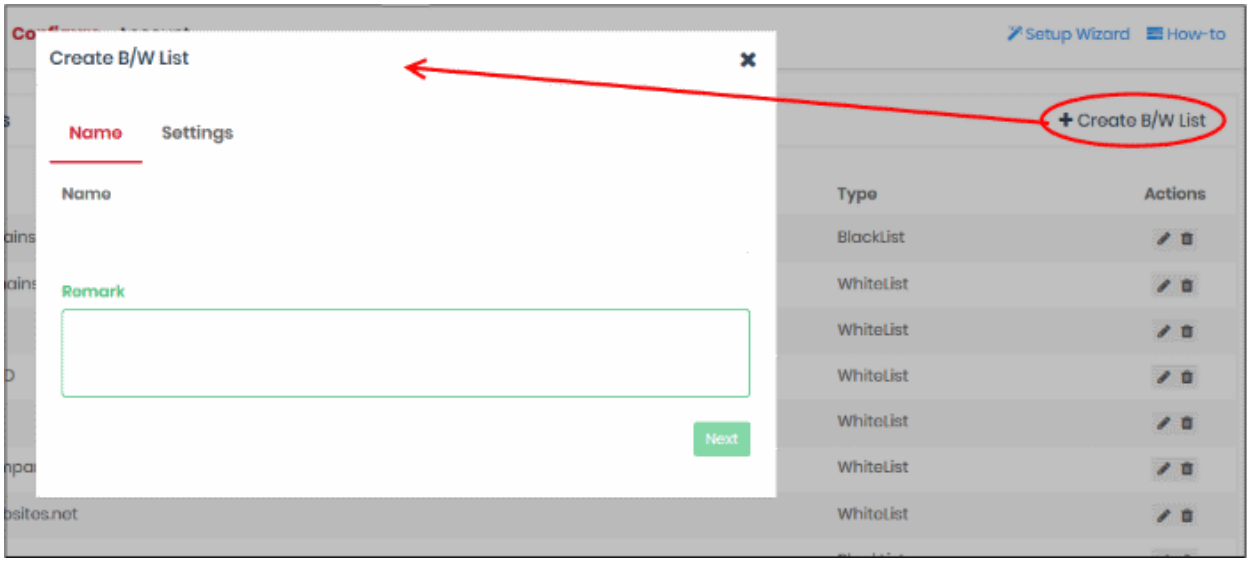
Example – Suppose your category rule blocks the 'Social Media' category, but you want to allow access to LinkedIn because it helps with careers. You would add 'www.linkedin.com' to the whitelist in your policy.

- Blacklists and whitelists over-rule category and security rules.
- Whitelists over-rule blacklists
- For example - If you block the 'Shopping' category, but add 'shop.com' to the whitelist, then 'shop.com' is allowed.

'Only B/W Mode' – if enabled, then only the black and white lists are consulted. All security and category rules are ignored.

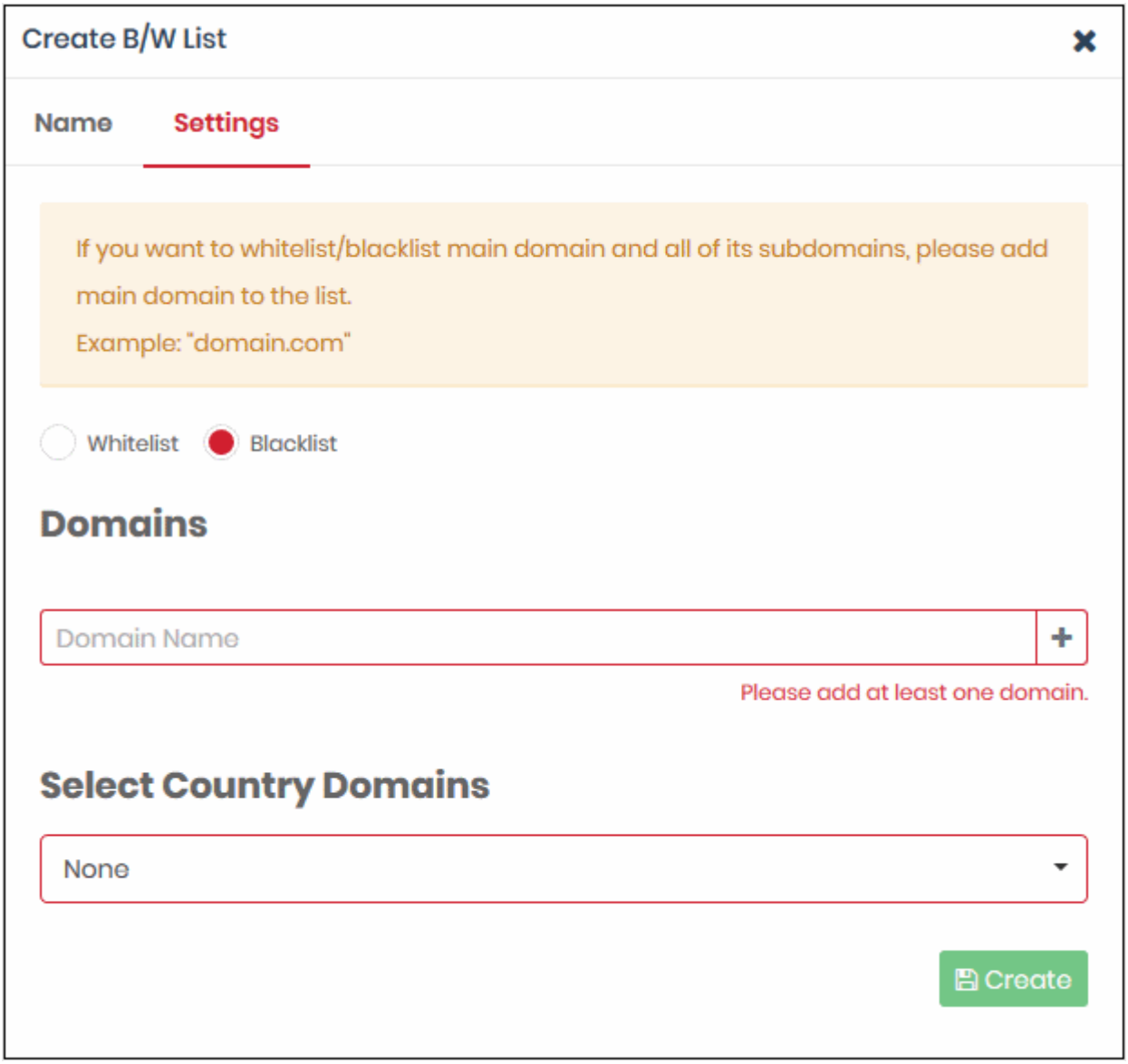
Create a blacklist or whitelist

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

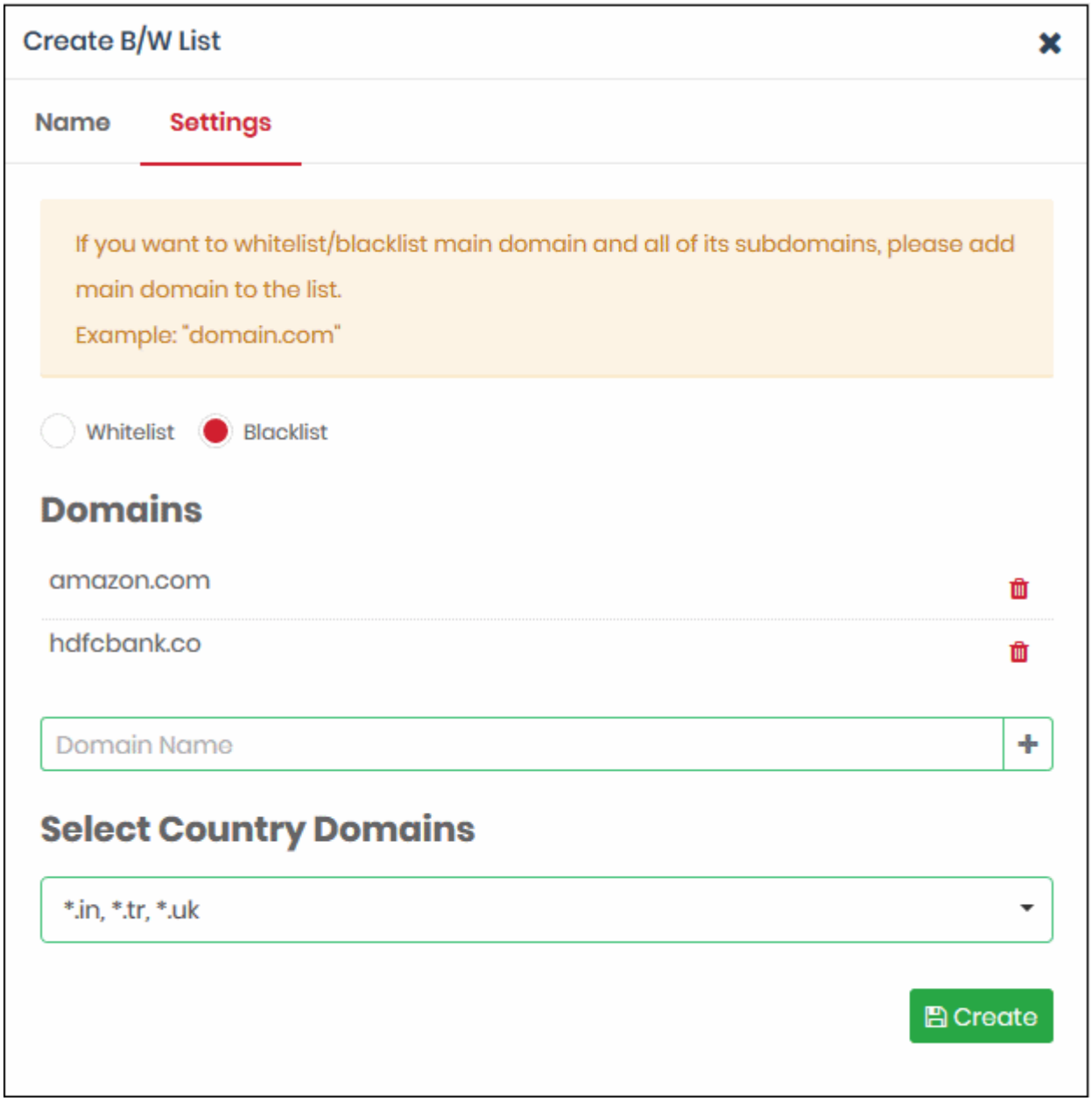


Name and remarks - Create a label and comments which will help you and others identify the purpose of the rule.

- Click 'Next' or 'Settings' to add domains you want to blacklist or whitelist.



- 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.
- Click the '+' button to add the domain to the list. Repeat the process to add more domain names.



- Click the 'Create' button when done

The domains are added to the B/W list. You can select it when **creating a policy**.

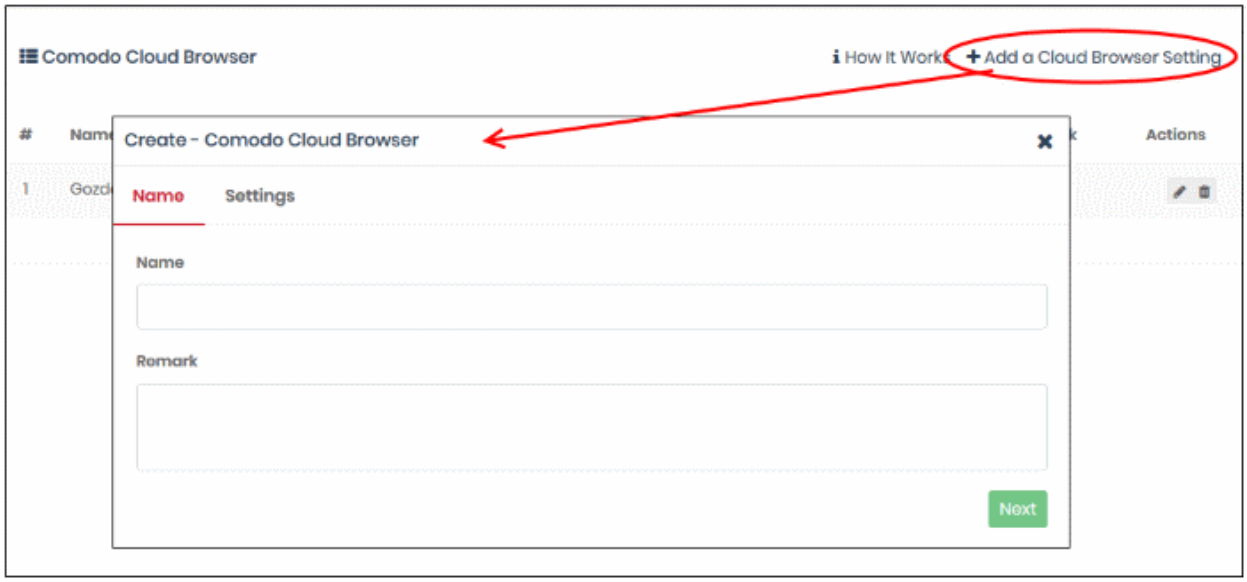
- Repeat the process to add more blacklists and whitelists.

Configure Virtual Browsing

- The cloud browser feature lets you specify that sites blocked by a **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.

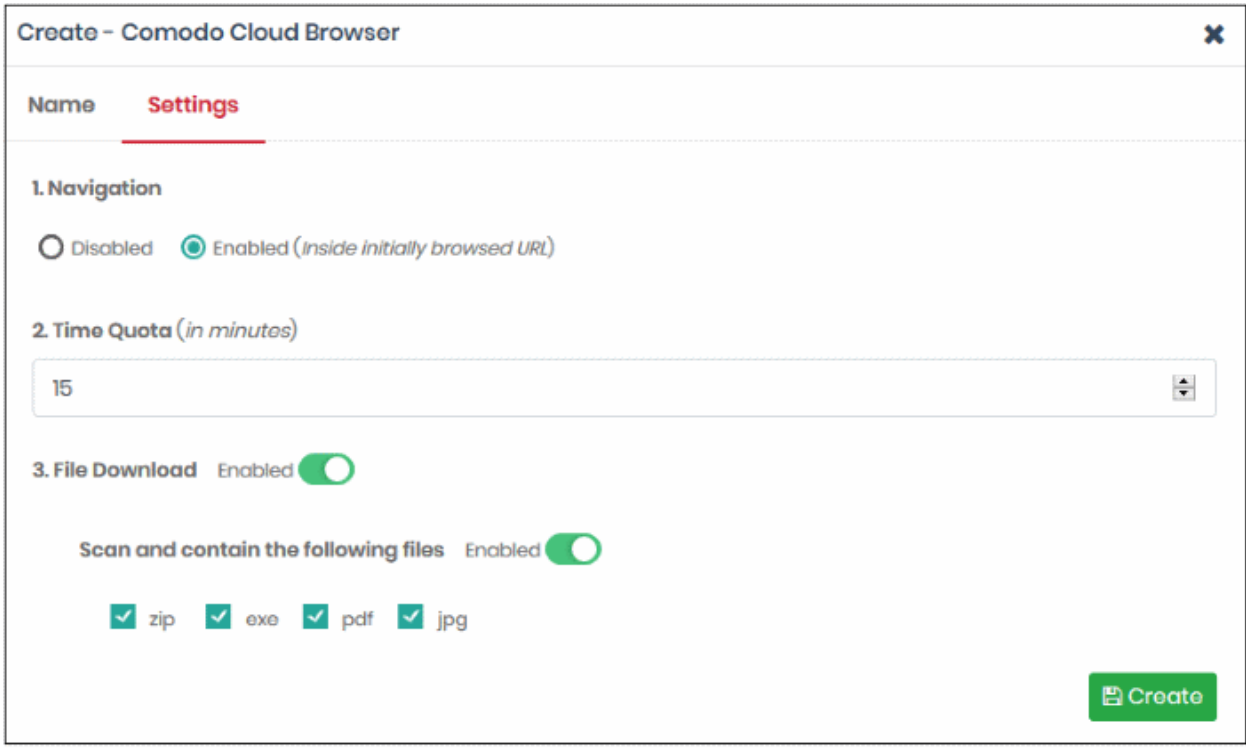
Create a new cloud browser rule

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



Name and remark - Create a rule label and add comments that will help you and others identify the purpose of the rule.

- Click 'Next' or 'Settings' to configure the virtual setting:



Navigation

- **Disabled** - Users can only browse the base-domain of the site 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 for threats. Supported file types are .zip, .exe, .pdf and .jpg.

- Click 'Create' when done

You can now add this rule to the security section when **creating a policy**.

Add Block Pages

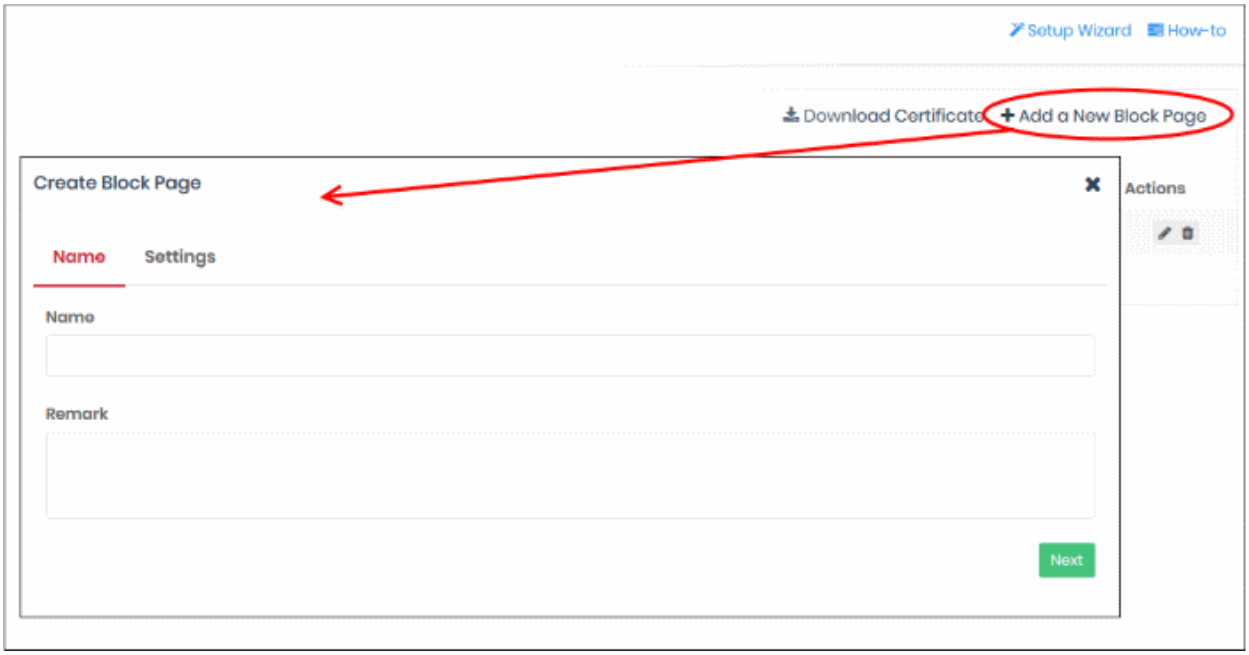
Block pages are shown to end-users when they attempt to visit a site that is banned by one of your policies. This includes users of endpoints in your protected networks, and all roaming endpoints.

- 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 of rule violation
  - Show different block pages for category, security, and blacklist violations
  - Show custom text on block pages, and add your company logos
  - Redirect users to a specific page

You need to install the Secure Internet Gateway SSL certificate on all protected endpoints. This is so the block page loads correctly over HTTPS connections.

Create a block page

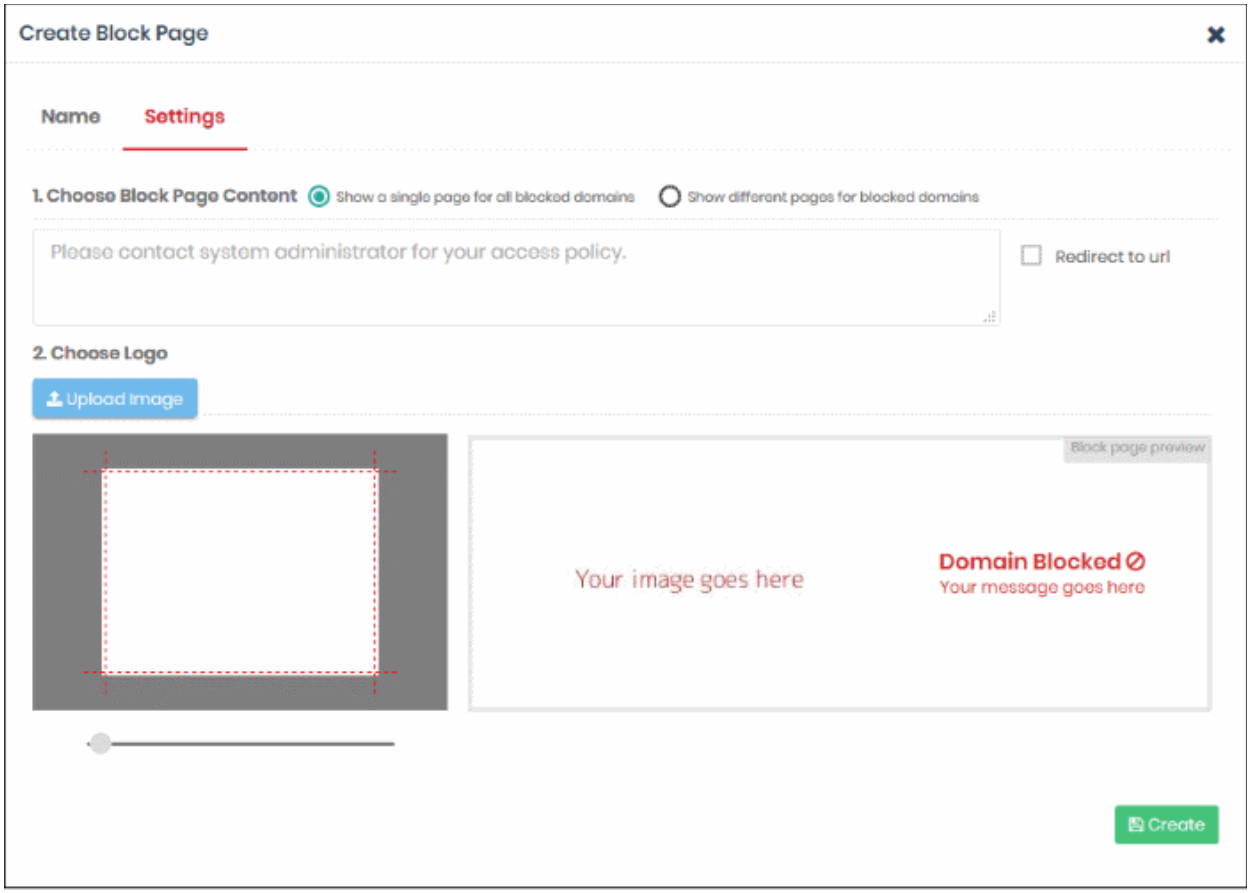
- Click 'Configure' > 'Policy Settings' > 'Block Pages'
- Click 'Add a New Block Page' at top-right



Name - Enter a descriptive label for the block page

Remark - Type internal notes/comments about the page, if required. This text is not shown in the block page itself.

- Click 'Next' or 'Settings' to configure the block page

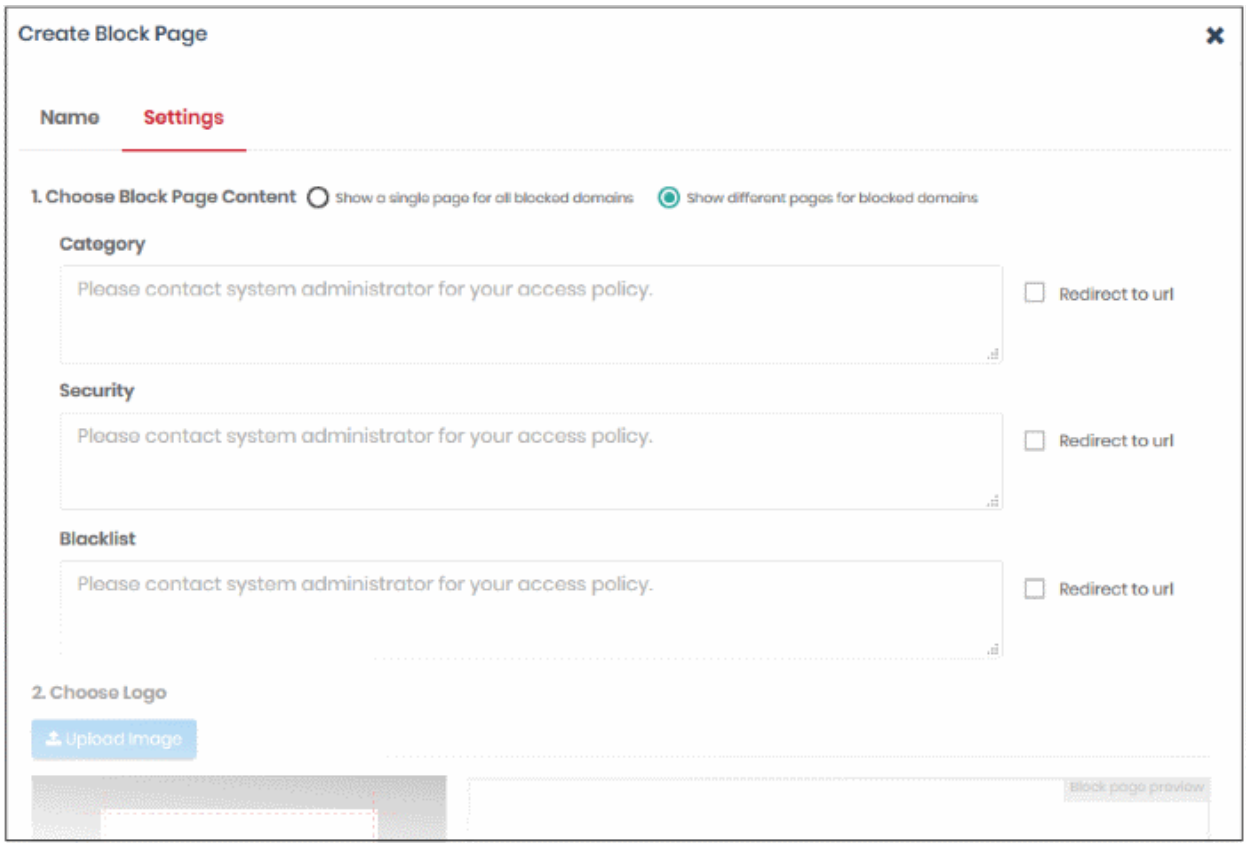


You now need to create your block page content and upload your logo:

1 - Configure Block Page Content

Choose one of the following:

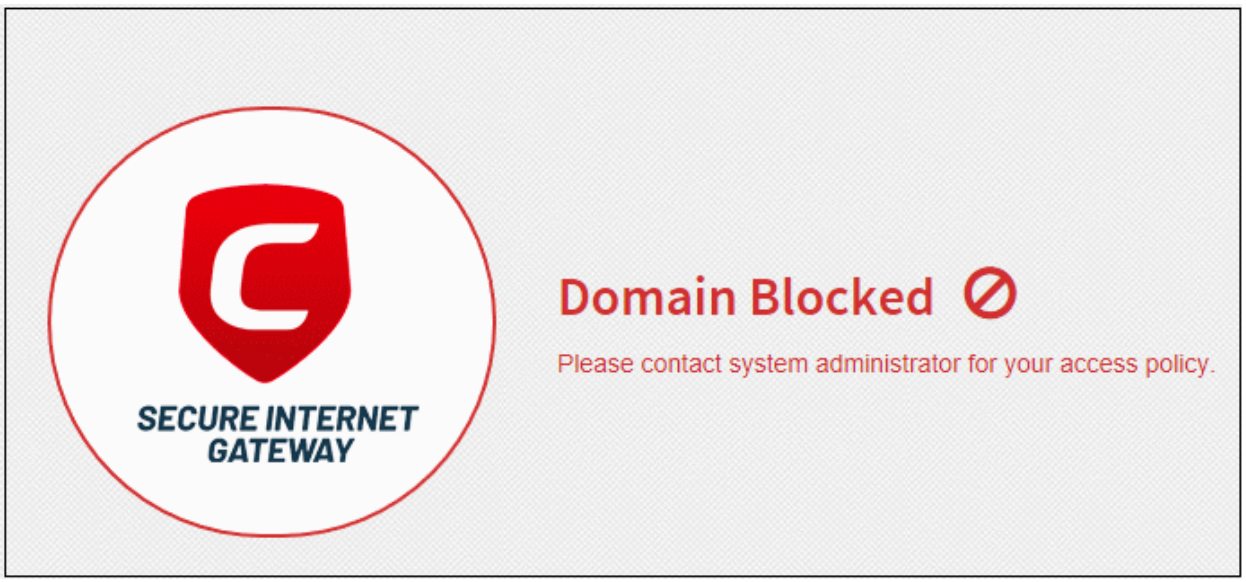
- **Show a single page for all blocked domains** - The same block page is shown regardless of the type of rule violated.
- **Show different pages for blocked domains** - Show specific block pages when a certain type of rule is violated. You can show different pages for category rule breaches, security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



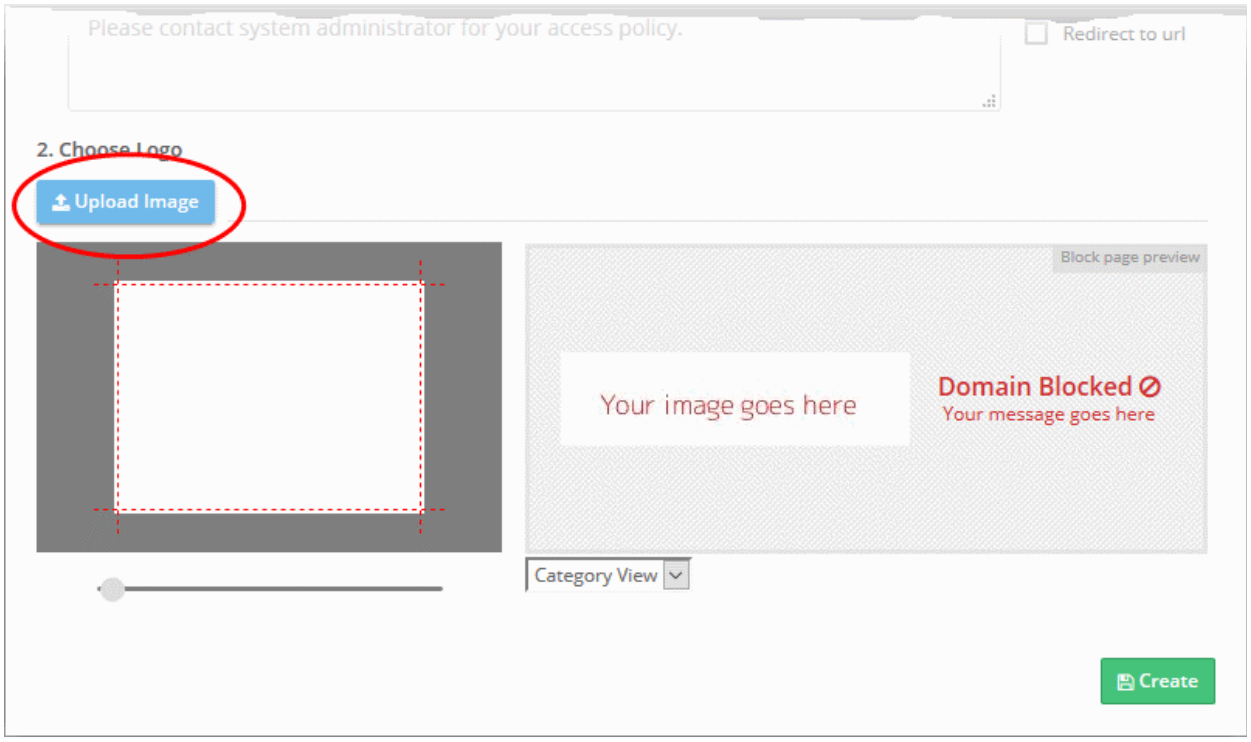
- You can create a custom message for each page if required.
- Alternatively, you can use the default message of 'Please contact your system administrator for your access policy'
- You can also redirect to a different page instead. For example, to the home page of your company website. Please specify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

2 - Upload Your Logo

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

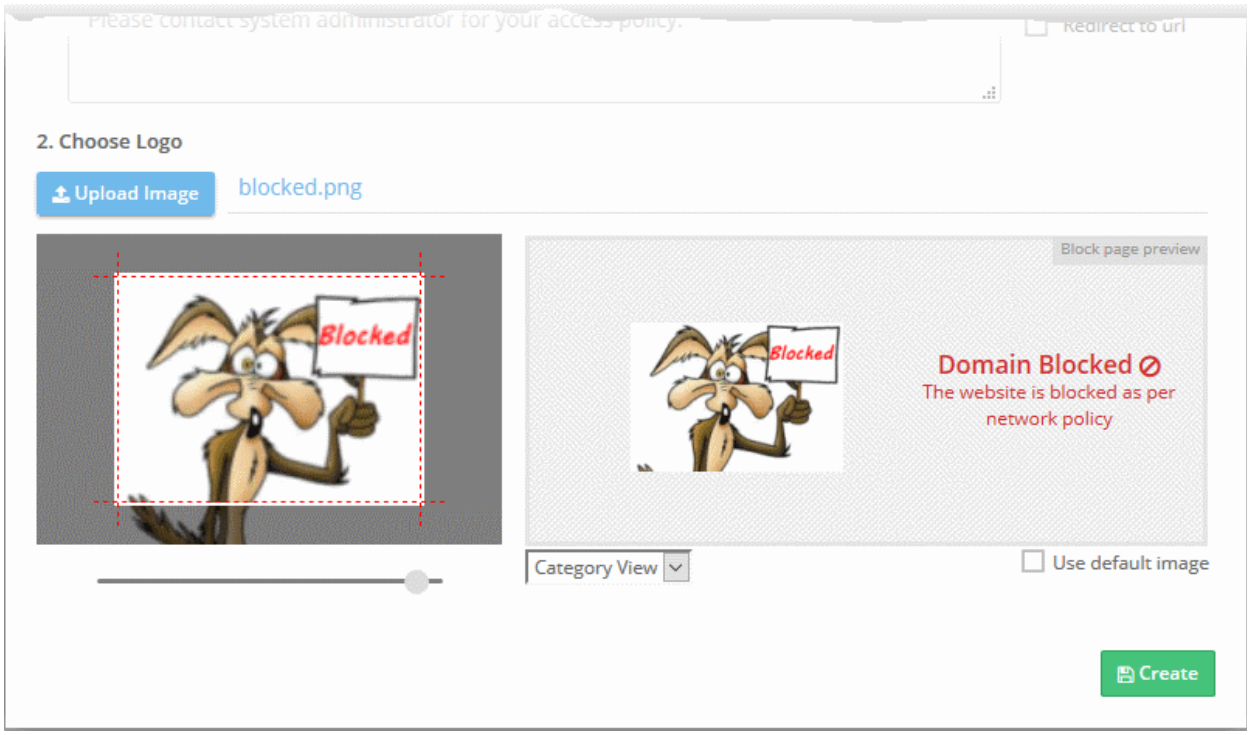


- Click 'Upload Image' under 'Choose Logo'. Browse to the location of your image and click 'Open'



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 on the block page.
- Click 'Create'

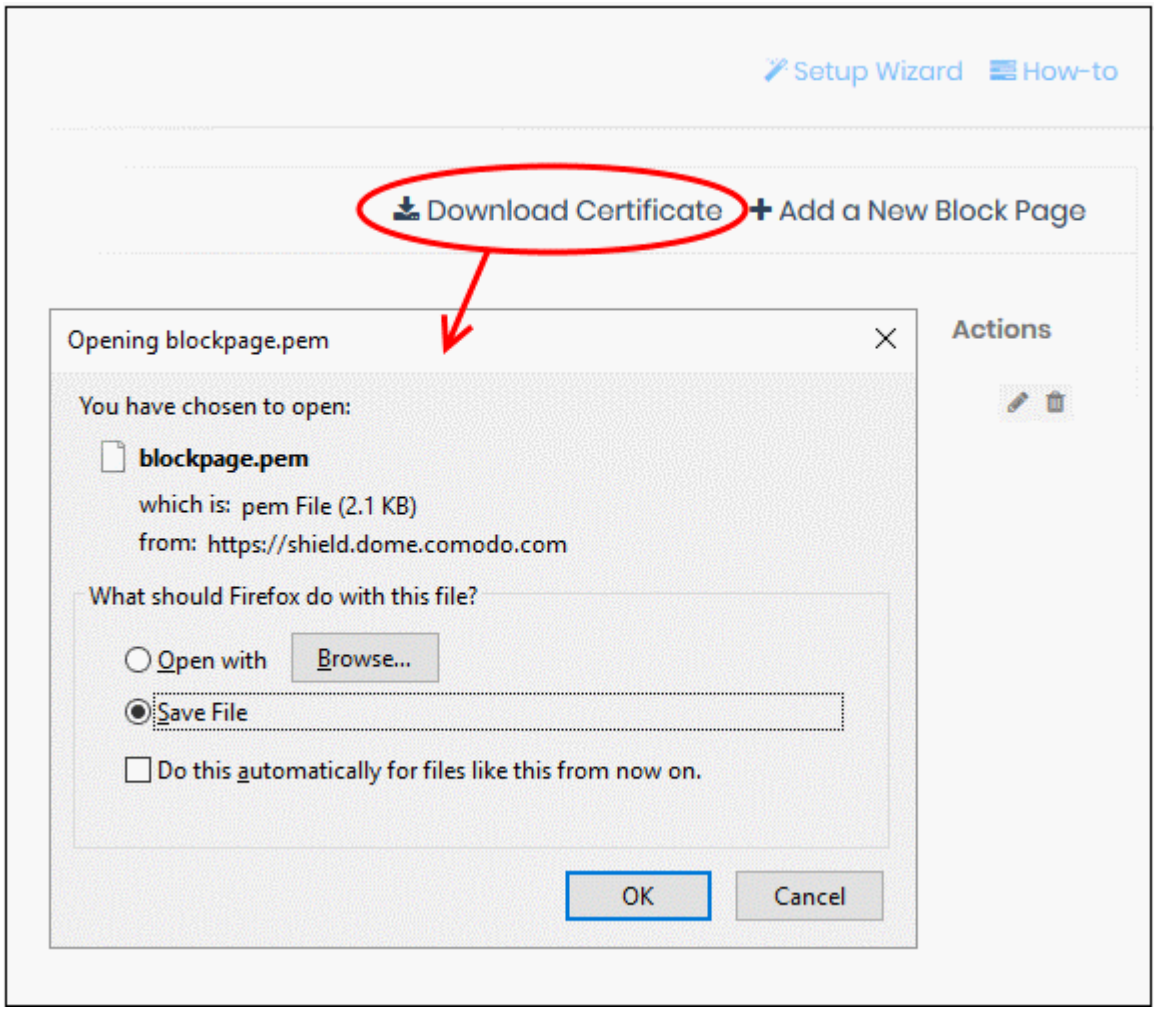
The new block page is available for selection when **creating a policy**.

Install the 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 the certificate

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



The certificate is downloaded in .pem format.

- See **https://help.comodo.com/topic-434-1-840-11971-Manage-Block-Pages.html** for help to install the certificate.

Step 5 – Build and Apply your Policy

- 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 custom block pages and/or virtual browsing settings.

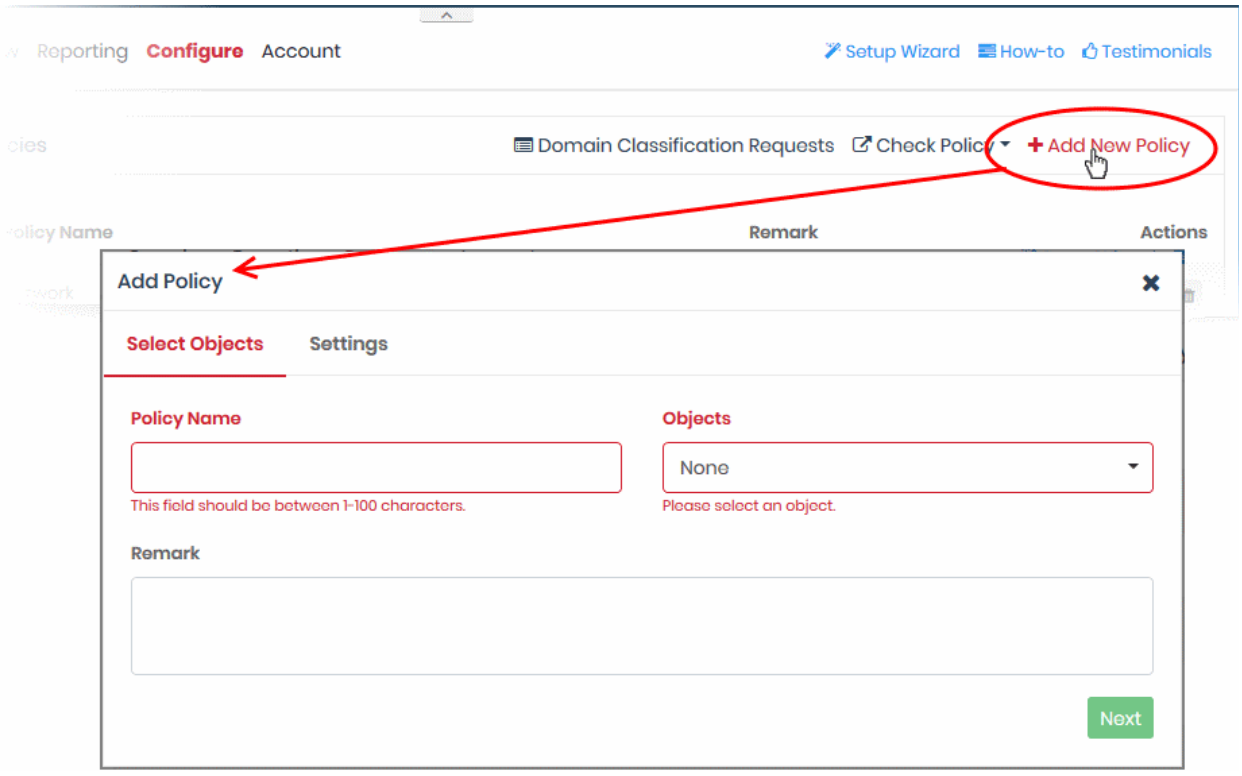
- You must have created at least one rule before you can create a policy.
- You must also have added at least one device or network, or have imported a site using the local resolver.

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 is in a banned category then it is blocked, or virtualized as per your preference.
- If the site isn't in the blacklist or category rules, then it is allowed.

Create a policy

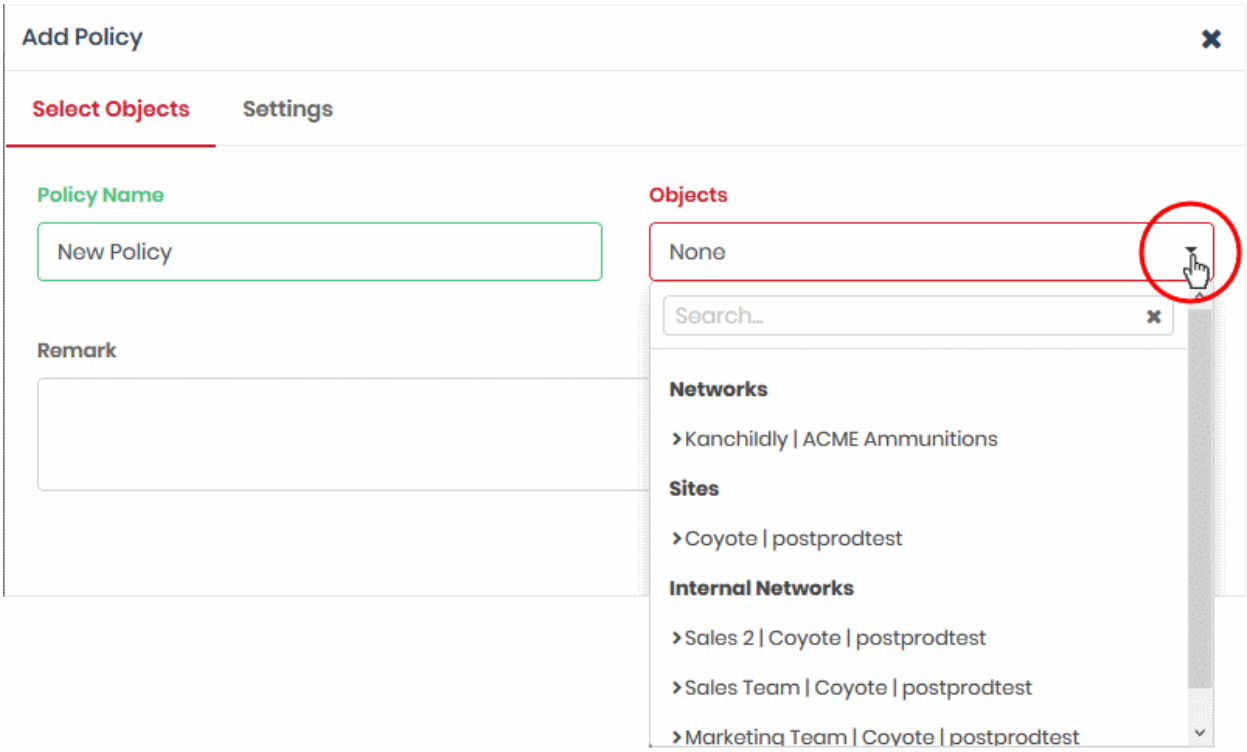
- Click 'Configure' > 'Policy'
- Click 'Add New Policy' at top-right



Policy Name - Enter a label for the policy

Objects - Select the devices/networks to which the policy should apply. This can be a network, roaming device, internal network, site, 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 - Manually added networks.

Agents - Roaming Windows and Mac devices that have the Secure Internet Gateway agent installed.

Mobile Agents - Enrolled Android and iOS devices.

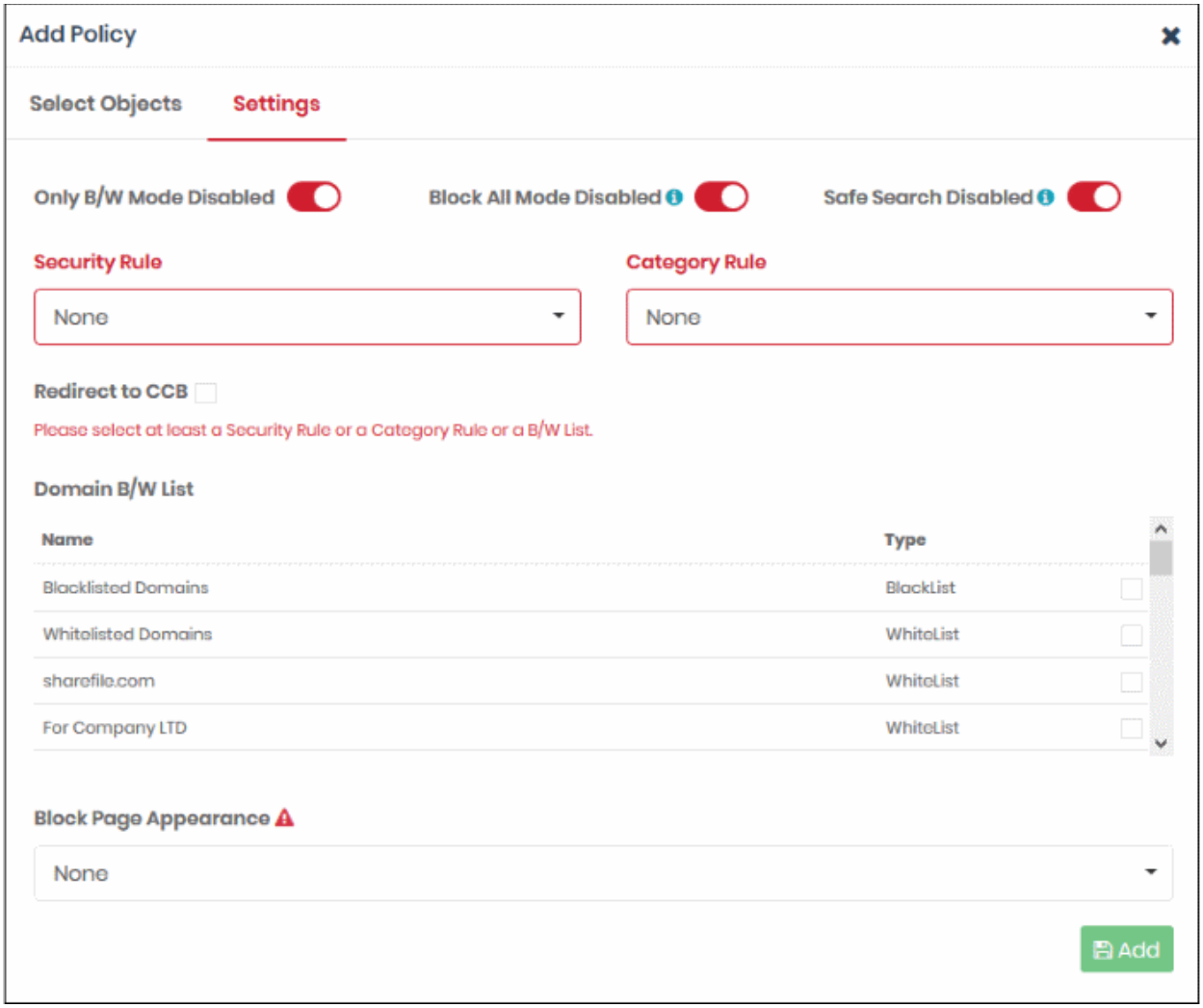
Sites - Network sites imported by deploying the local resolver virtual appliance.

Internal Networks - Internal objects within imported sites. Note - Policies applied to a site will over-rule policies applied to internal 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:



Only B/W Mode - If enabled, you can only add blacklist and/or whitelist rules to the policy. You cannot add security or category rules to the policy.

Block All Mode - If enabled, all domains are blocked EXCEPT domains in the whitelist. 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 '**Add 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 '**Configure Virtual Browsing**' if you need more information on virtual session rules.

Category Rule - Rules which block websites by their content-type. The drop-down lists category rules that have been added to the 'Policy Settings' section. See '**Add Category Rules**' for more details.

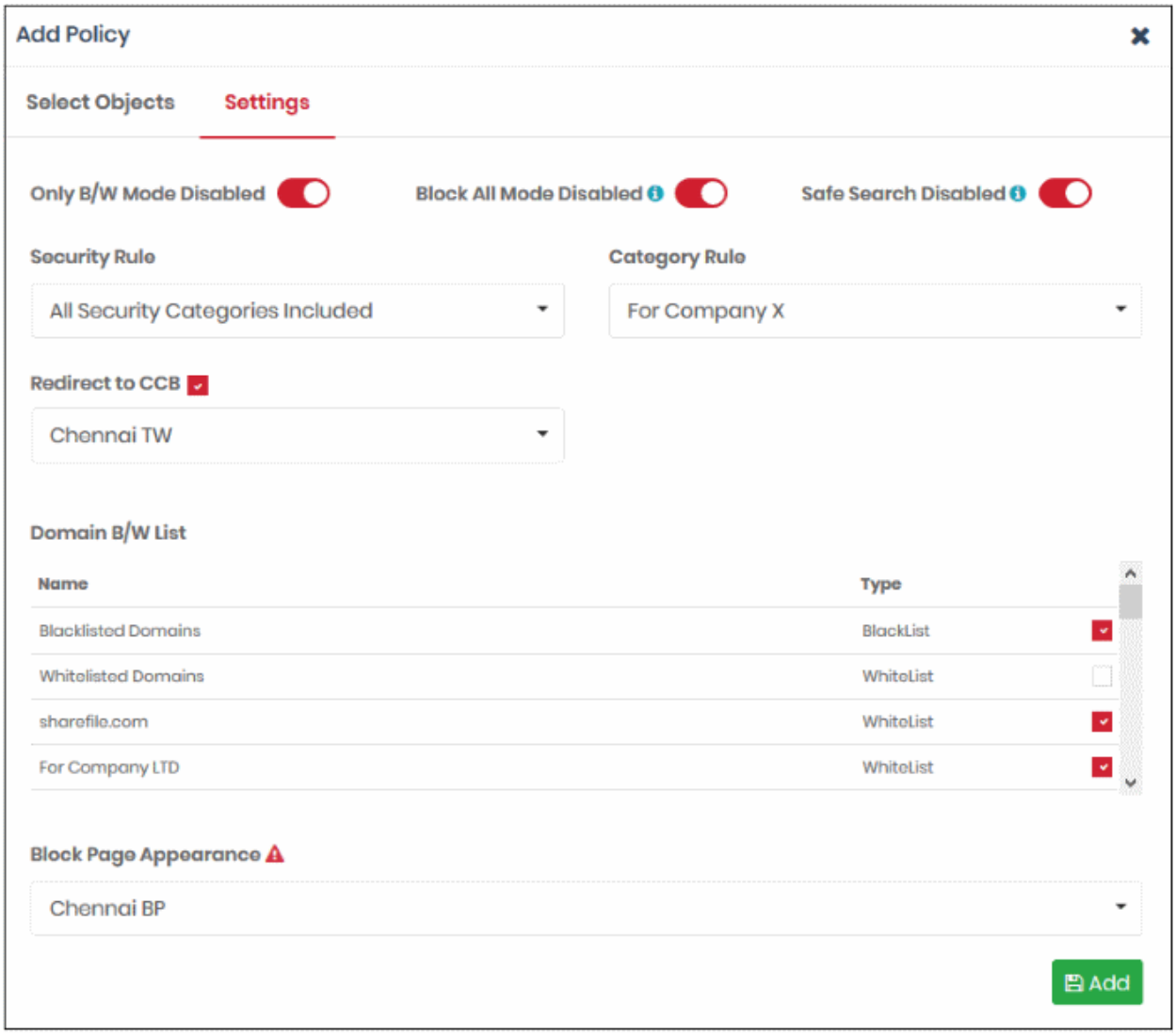
Domain B/W List - Select a list to block or allow specific domains. The dialog shows blacklists and whitelists added to the 'Policy Settings' section. See '**Add Domain Blacklist and Whitelist**' for more details.

Note – Black and white lists over-rule security/category rules in the event of a conflict over a particular domain.

Block Page Appearance - Choose the block page you want to show to users if they try to visit a site prohibited by the policy. The drop-down lists block pages created in the 'Policy Settings' area. See **Add 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.

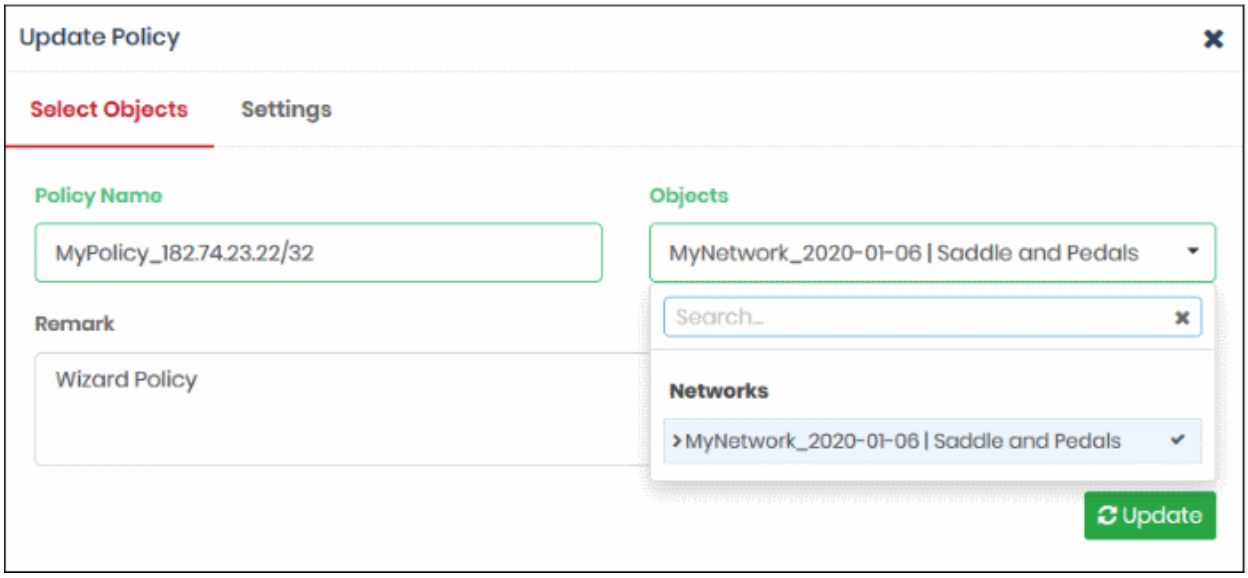
The policy is applied to the chosen networks and devices.

- Repeat the process to add more policies.

Add an existing policy to newly added networks and roaming/mobile devices

- Click 'Configure' > 'Policy'
- Click the 'Edit' icon in the row of the policy

The 'Update Policy' dialog appears.



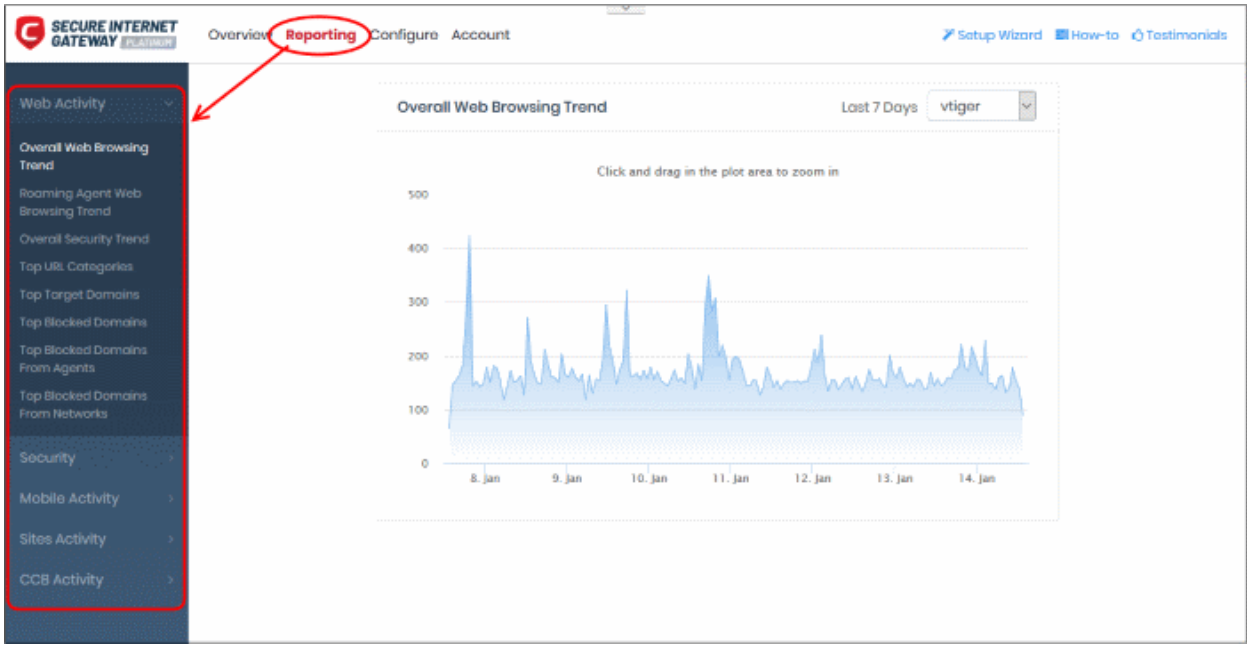
- Select the new network / roaming / mobile device from the 'Objects' drop-down
- Click 'Update'

The policy is applied to the new object.

Step 6 - Generate 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, more interactive, versions of those on the dashboard.
- Use the drop-down at top-right to choose the time period covered by the report.

Web Activity Reports

- **Overall Web Browsing Trend** - The number of domain access requests from all protected networks and endpoints over the selected period.

- **Roaming Agent Web Browsing Trend** - The number of domain access requests by roaming devices over the selected period.
- **Overall Security Trend** - The number of harmful sites blocked by security rules over time.
- **Top URL Categories** - The website categories most often visited by users.
- **Top Target Domains** - The websites most often visited by users in your organization. Results are shown for the top 10 domains.
- **Top Blocked Domains** - The websites that were most often blocked by your security policies. The results show the top 10 blocked domains.
- **Top Blocked Domains From Agents** - The websites that were most often blocked on roaming devices. Results are shown for the top 10 domains.
- **Top Blocked domains From Networks** - The websites that were most often blocked on endpoints in your networks. Results are shown for the top 10 domains.

Security Reports

- **Overall Advanced Threats** - The websites that were most often blocked by your security rules. The results cover both enrolled networks and roaming devices.
- **Roaming Agent Advanced Threats** - The websites that were most often blocked by your security policies after requests from roaming devices.
- **Most Blocked Mobile Threats** - The number of website categories that were blocked on mobile devices over time.
- **Sites - Most Blocked Threats** - The website categories most often blocked on endpoints imported by a local resolver.
- **Overall Security Incidents** - Number of incidents where harmful sites were blocked across all networks and roaming devices.
- **Roaming Agent Security Incidents** - The number of incidents in which harmful sites were blocked on roaming devices over time.

Mobile Activity Reports

- **Top Target Domains of Mobile Users** - The websites which were most often visited by mobile users. Results are available for the top 10 domains.
- **Web Traffic of Mobile Users** - The total number of domain access requests from all mobile devices over the selected period.
- **Top Blocked Categories of Mobile Users** - The website categories most often blocked by your security policies for mobile users.

Sites Activity Reports

- **Sites - Top Target Domains** - The websites most often visited by users in sites imported by a local resolver. Results are shown for the top 10 domains.
- **Sites - Overall Web Browsing Trend** - The number of domain access requests from all endpoints imported by a local resolver.
- **Sites - Top Blocked Domains** - The websites most often blocked by your security policies in networks imported by a local resolver. The results show the top 10 blocked domains

CCB Activity Report

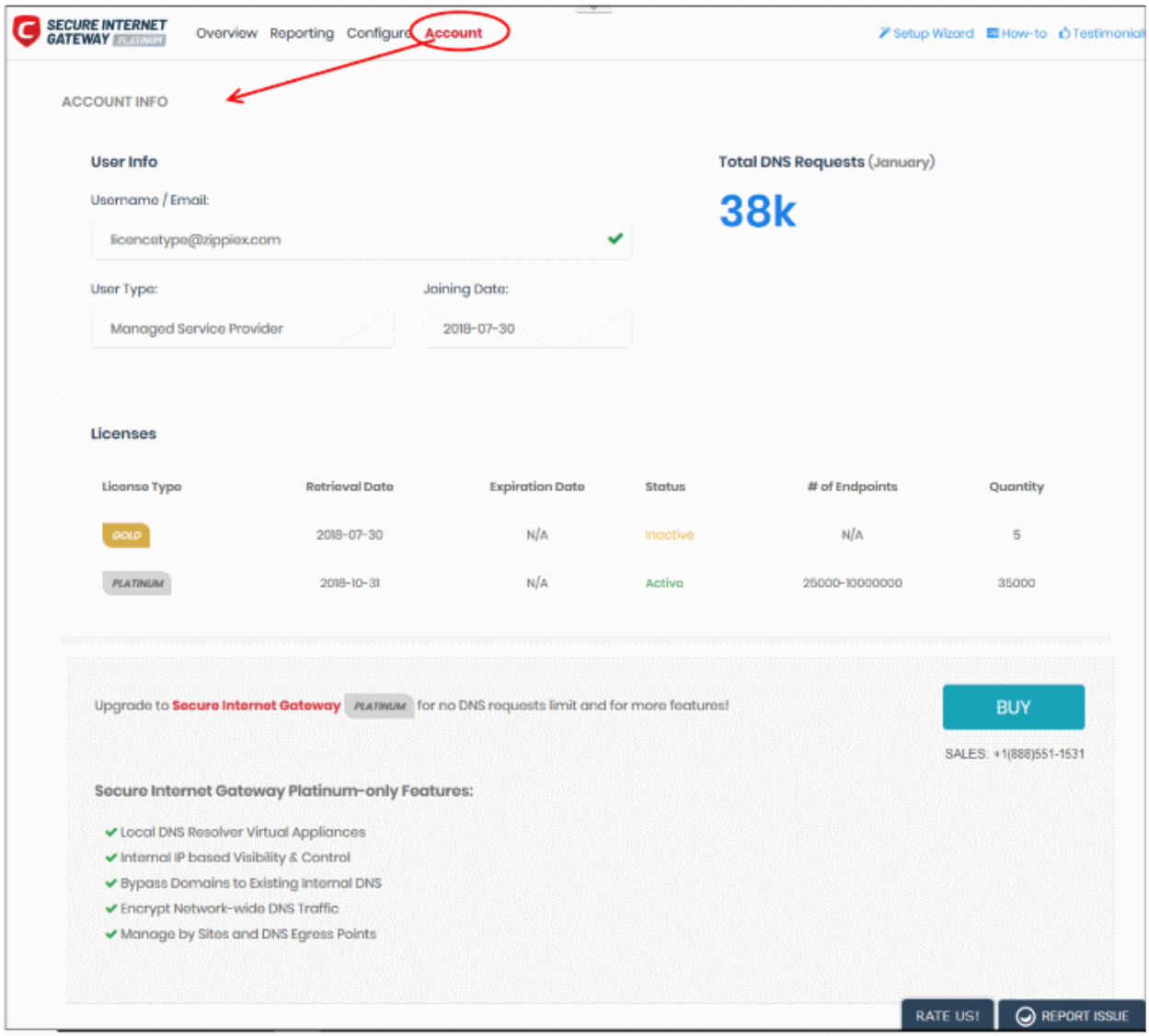
- **Top Visited Sites –** The websites that were most visited in virtual sessions by your users. The results show the top 10 visited domains.
- **Top Opened Sessions –** Devices that most often visited sites in virtual sessions. The results show the top 10 devices that used the virtual sessions.
- **File Status** – A summary of files downloaded from virtual sessions. Details include files that were allowed (files scanned and found safe) and files contained (unknown / malicious files that were placed in the

container).

See **https://help.comodo.com/topic-434-1-840-10759-The-Dashboard.html** for more details on report types.

Step 7 - 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 your free license to a Platinum license.
  - **Click here** to compare packages.
- Click 'Account' to open the account info page:



User Info

- **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.
    - 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.

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 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**